Journal of the Korea Academia-Industrial cooperation Society
Vol. 16, No. 7 pp. 4863-4870, 2015

http://dx.doi.org/10.5762/KAIS.2015.16.7.4863
ISSN 1975-4701 / eISSN 2288-4688

정량적 안전성 분석을 통한 Vital 데이터 처리장치의 안전무결성 요구사항 검증

최진우[1*], 박재영[1]
[1]우송대학교 철도시스템학과

Verification of safety integrity for vital data processing device through quantitative safety analysis

Jin-Woo Choi[1*], Jae-Young Park[1]
[1]**Division of Railroad System Engineering, Woosong University**

요 약 현재 철도신호 시스템/제품(Generic Product)에 대한 안전성 확보가 최우선시 되면서 그에 대한 정량적인 척도로 안전무결성 요구사항(SIR) 만족에 대한 검증은 필수사항으로 요구되고 있다. 안전무결성 요구사항(SIR) 검증은 시스템 안전성 분석을 기반으로 수행되지만 아직까지는 국내에서 수행한 경험이 없기 때문에 시스템 안전성 분석을 위한 기본 데이터의 확보율이 현저하게 떨어졌다. 따라서 지금까지는 정성적인 시스템/제품 안전성 분석에 의존할 수밖에 없었다. 정성적 분석은 리스크 매트릭스, 리스크 그래프와 같은 방법으로 사고의 폭은 넓지만 결과의 신뢰성이 떨어진다는 단점을 가지고 있다. 따라서 정성적 분석의 단점을 보완하기 위해서는 시스템/제품에 대한 정량적인 안전성 분석이 병행되어져야 한다. 본 논문에서는 정성적 분석의 단점을 극복하기 위해 정량적인 안전성 분석방법을 제시하고 신뢰성이 향상된 안전무결성 요구사항(SIR)의 검증방안을 제시한다. 검증 결과, Vital 데이터 처리장치에 대한 위험고장 발생 빈도는 1.172279×10^{-9}으로 산출되었으며, 이 수치는 요구된 안전무결성 목표보다 상회하는 것으로 검증되었다.

Abstract Currently, as a priority to secure the safety of the railway signalling system, verification for satisfy of the safety integrity requirements(SIR) is required to the essential elements. Safety Integrity Requirements(SIR) verification is performed based on the system safety analysis. But the probability of securing basic data for system safety analysis significantly dropped because there is no experience yet performed in the country. Therefore we are had to rely on a qualitative analysis. There are methods such as qualitative risk analysis matrix, and risk graphs. The qualitative analysis is wide, the width of the accident. However, the reliability of the result is significantly less has a disadvantage. Therefore, it should be parallel quantitative safety analysis of the system/products in order to compensate for the disadvantages of the qualitative analysis. This paper presents a quantitative safety analysis method to overcome the disadvantages of the qualitative analysis. And through a result, highly reliable Safety Integrity Requirements(SIR) verification measures proposed. Verification results, the dangerous failure incidence for vital data processing device was calculated to be 1.172279×10^{-9}. The result was verified to exceed the required safety integrity targets more.

Keywords : Safety, SIR, PFH, SIL, Quantity Analysis

1. 서론

최근 열차의 속도는 급속하게 고속화되고 있으며 이를 이용하는 승객의 수 또한 매년 상당한 증가 추세를 보이고 있다. 따라서 열차의 속도 향상에 핵심 역할을 하는 철도신호시스템의 안전성 확보는 최우선적인 요구조

*Corresponding Author : Jin-Woo Choi(Woosong univ.) Tel: +82-11-238-4363 email: jwchoi@daeati.co.kr
Received June 5, 2015 Revised (1st July 1, 2015, 2nd July 7, 2015)
Accepted July 16, 2015 Published July 31, 2015

건이 되고 있으며, 이에 대한 수행과 검증이 반드시 이루어 져야 한다.

유럽표준 및 국제표준에서 철도신호시스템의 안전성 확보를 위한 조건이 제시되어 있지만, 대부분 정성적인 접근 방법이 권고되고 있으며

정성적인 접근 방법이 권고되고 있으며 이에 대한 평가는 각 국가별로 상이한 방법으로 평가되고 있다.

이러한 정성적인 파라미터에 의한 분석(리스크 매트리스 또는 리스크 그래프 등)은 적용하기가 쉽고 그 범위도 광범위하여 일반적인 위험(Hazard)분석에 적용할 수 있는 반면 그에 대한 정량적인 접근과 검증이 불명확하고 어려운 문제가 발생하고 있다. 따라서 정성적인 분석의 취약점을 보완하기 위해서는 신뢰할 수 있는 정량적인 데이터가 적용되어야 하며 이에 대한 검증이 반드시 이루어져야 한다.

본 논문에서는 Vital 데이터처리장치에 대한 정략적 분석방법을 적용하여 목표된 SIL3의 만족여부를 확인할 수 있는 상세한 방법을 제시하였다. 여기서 제시되는 방법은 신뢰성 데이터를 기반으로 다양한 파라미터가 적용되고 그 결과 산출되는 '시간당 고장확률'로 SIL3 만족여부를 결정하게 된다. 만약 SIL3에 해당되는 범위를 벗어나서 만족하지 못한다면 시스템의 설계 및 구조를 변경하여야 하기 때문에 본 논문에서 제시되는 내용은 시스템의 안전성뿐만 아니라 신뢰성까지 모두 만족시켜야 하는 복합적인 방법이라 할 수 있다.

국내 철도신호시스템의 Vital 데이터처리장치에 대한 SIL인증(Generic Product)은 지금까지 수행된 사례가 없는 관계로 처리장치의 정량적 분석 데이터가 매우 빈약한 실정이다. 방대한 정량적 분석 데이터는 국내 철도신호시스템의 지속적인 발전과 개발에 큰 영향을 줄 수 있을 것으로 판단되며 다양한 방법에 의한 전략적인 접근이 가능할 것이다.

2. 본론

2.1 정성적 SIL 할당 방법

철도 신호시스템에서 일반적으로 적용된 정성적 SIL 할당 방법은 EN50129(IEC62425)의 Appendix에 명시된 바와 같이 적합한 SIL을 결정하기 위해서는 Systematic Failure Integrity와 Random Failure Integrity에 대한 분석이 수행되어야 한다. 하지만 Systematic Failure는 시스템 수명주기 단계에서 발생할 수 있는 다양한 Human Error에 의하기 때문에 정성적인 접근이 필요하며 THR(Tolerable Hazard Rates)에 따라 SIL이 결정된다. IEC62425에 따르면 "THR은 Random Failure Integrity는 정량화 될 수 있으나, Systematic Failure Integrity를 판단하는 근거는 단지 정성적 방법으로 가능하며 이것이 SIL에 의해 판단된다." 라고 명시되어 있다. 이에 따라 지금까지 다양한 분석(PHA, SHA, IHA 등)에 의해 Systematic Failure Integrity의 목표치가 결정되었으며, Random Failure Integrity는 정량적으로 수치적인 고장률 형태로 표현되었다. 이에 해당되는 시스템의 명확한 SIL 목표치를 산출하고 이를 검증하기에 모호한 부분이 존재하였다.

본 논문에서는 정량적인 측정과 분석을 통한 SIL 결정 및 검증에 주안점을 두고 기술하였다.

2.2 Vital 데이터 처리장치 구성

2.2.1 하드웨어 구조

Vital 데이터 처리장치의 기본 구조는 1oo2구조로 설계되며 각 채널이 Safety 기능을 처리할 수 있도록 병렬된 두 개의 채널로 구성된다.[3, 4]

Vital 데이터 처리장치는 양 채널 간 Diagnostic을 수행하고 결과가 Fail일 경우 안전 측으로 전환한다.Vital 데이터 처리장치에 대한 신뢰성 블록 다이어그램은 Fig. 2와 같다.[1, 2]

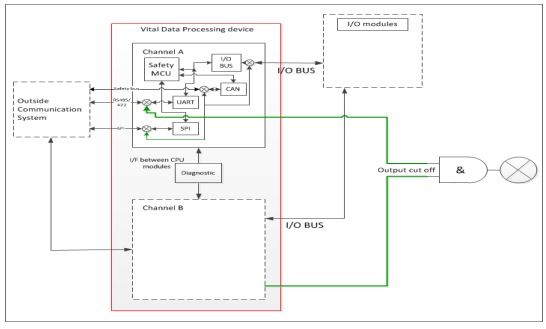

Fig. 1. architecture of the vital data processing device

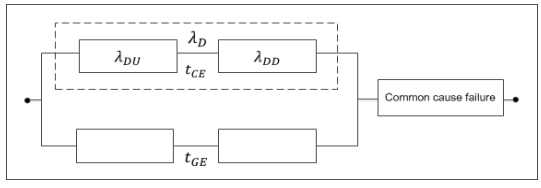

Fig. 2. Reliability Block Diagram(IEC 61508-6)

2.2.2 Vital 데이터 처리장치 기능

Table 1 은 Vital 데이터 처리장치가 수행할 가능한 기능을 보여준다. 아래의 기능 설명은 Vital 데이터 처리장치에 대한 시스템 범위의 기능이며 소프트웨어 요구사항 단계에서 상세하게 기능이 정의된다.

Table 1. Function of vital data processing device

Function No.	Function block	Function Description
01	Processing function	Input/output processing for the respective functions Entering the safe state after fault detection
02	Power supply function	Power supply circuits When detecting the output power and maintaining power off
03	I/O bus interface function	Interface function with the external module
04	Communication function	Serial communication capabilities with external systems
05	Temperature Detection function	Internal temperature monitoring
06	Local Time function	Provides local time and calendar functions
07	Indication function	Revealed function for to the operating state and error codes
08	User Interface functions	Application download/upload function Safety flag clear
09	Digital Input/Output function	Digital input/output interface with external device

2.3 Life-cycle 단계 별 안전성 분석 수행

2.3.1 적용규격

안전성 보장을 위한 Vital 데이터 처리장치 개발에 적용할 규격은 모든 전기/전자 분야에서 적용이 가능한 국제규격 IEC 61508(2010)에서 요구하는 모든 요구사항을 준수한다.[5]

2.3.2 분석 프로세스

규격 IEC 61508에서 제시하는 안전성 Life-cycle에 따라 프로세스가 수립된다. 프로세스는 Plan부터 Validation 단계까지 11개의 프로세스로 구성되며 본 논문에서는 Vital 데이터 처리장치 개발에 따른 정량적 안전성 분석에 대한 내용이 설명된다. 따라서 정량적 안전성 분석의 결과에 따라 HW 설계가 변경되며 HW 설계 이후의 과정은 본 논문 범위에서 제외된다.

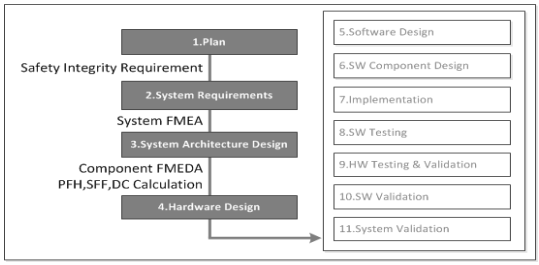

Fig. 3. Life-cycle of task

2.4 System Requirements 단계

2.4.1 System 요구사항

System 요구사항 단계 이전의 Plan 단계는 안전성 보장을 위한 활동 계획이 수립되며 본 논문에서 설명되는 안전성 분석방법 등이 포함된다. Vital 데이터 처리장치에 대한 요구사항은 아래의 내용이 모두 포함되어 도출되며, 본 논문에서는 Safety Integrity 요구사항 만족 여부를 확인하는 방법이 제시되고 그 분석 결과가 정량적으로 산출된다.

· Safety Functional Requirements
· Safety Integrity Requirements
· Interface Requirements
· Life time and Environmental Requirements

2.4.2 Safety Integrity 요구사항

IEC 61508은 안전관련 기능의 사용빈도에 따라 Low Demand Mode와 High Demand Mode로 구분하고 있으며, 각 모드의 구분은 IEC 61508-4의 3.5.12항에서 안전기능의 사용빈도가 1년 이하인 기능은 Low Demand Mode의 SIL 기준을 적용하고, 사용빈도가 1년에 1회를 초과하는 경우 High Demand Mode의 SIL 기준을 적용하도록 하고 있다.[6]

Vital 정보처리 범용장치는 High Demand Mode에 해당하며 도출된 Safety Integrity 요구사항은 아래 Table 2와 같으며, Vital 데이터 처리장치에 대한 기존 기능 분석과 해외제품 사례, 경험 등을 고려하여 가장 보수적인 수준으로 도출된 결과를 보여준다.

Table 2. Safety Integrity Requirement

Safety Function	Required Risk Reduction	Explanation of HW architecture	SFF (Safety Failure Fraction)
Safe output cut off when device is failed	PFH: SIL3	1oo2	95%

Vital 데이터 처리장치는 기본적으로 모든 Safety 기능에 대하여 고장 또는 기능 실패 시 안전 측으로 동작해야하며 이것은 시스템 FMEA(Failure Mode and Effect Analysis)와 Component FMEDA(Failure Mode and Effect Diagnostic Analysis)를 통해 분석된다.[8] 시스템 FMEA는 정성적인 분석을 통해 시스템 범위에서 안전성을 분석하는 방법으로 Safety Integrity 요구사항과는 관계가 없기 때문에 본 논문에서는 Component FMEDA 분석 과정만 제시된다.

2.5 System Architecture and Design 단계

2.5.1 시간당 고장확률(SIL 기준 값)

Safety Integrity 등급을 산정하는 정량적인 척도로 시간당 고장확률 계산 결과에 따라 아래의 기준에 의해 SIL등급이 정해진다. 여기에서 말하는 시간당 고장확률은 Vital 데이터 처리장치의 위험 측 고장에 대한 평균 빈도수를 의미한다.

Table 3. Safety Integrity Level(IEC61508-1 Table 3)

SIL	Average frequency of a dangerous failure of the safety function
4	≥10^-9 to <10^-8
3	≥10^-8 to <10^-7
2	≥10^-7 to <10^-6
1	≥10^-6 to <10^-5

앞서 Table 2 의 도출된 요구사항에서 보였듯이 Vital 데이터 처리장치에 대한 Safety Integrity 목표는 SIL3 이다. 따라서 시간당 고장확률에 대한 계산 결과는 $\geq 1\times10^{-8}$or $< 1\times10^{-7}$ 범위 이내여야 하며, 시간당 고장확률(PFH)은 아래의 공식에 의해 구해진다. 시간당 고장확률(PFH)은 IEC61508-6에서 제시된 공식이 사용된다.[1]

$$PFH = 2((1-\beta_D))\lambda_{DD} + (1-\beta)\lambda_{DU}(1-\beta)\lambda_{DU}t_{CE} + \beta\lambda_{DU}$$

λ_{DD} : Dangerous/Detectable 고장률

λ_{DU} : Dangerous/Undetectable 고장률

$\beta-factor$: 공통원인고장

t_{CE} : 채널 간 등가평균 정지시간

시간당 고장확률 계산을 위해서는 위 공식에서 보여지는 모든 파라미터 값을 구해야 한다. 이것은 Table 4 에서 제시된 방법을 통해 산출된다.

Table 4. Parameter

Parameter	Calculation Method	Equation	Section
λ_{DD}	Component FMEDA	-	2.4.1.1
λ_{DU}	Component FMEDA	-	2.4.1.1
β-factor	Assessment Table of βD	$-\lambda_{DU}\beta+\lambda_{DD}\beta_D$	2.4.1.2
	Z calculation	$-\beta_D : S_D = X(Z+1)+Y$	
	Assessment Table of β	$-\beta : S = X+Y$	
t_{CE}	MRT Process	$t_{CE}=\frac{\lambda_{DU}}{\lambda_D}(\frac{T_1}{2}+MRT)+$	2.4.1.3
	MTTR Process	$\frac{\lambda_{DD}}{\lambda_D}MTTF$	

2.5.1.1 Component FMEDA

시스템 설계가 시작되고 BOM(Bill of Material)이 생성되면 각 컴포넌트별로 고장모드에 대한 분석이 이루어진다. Component FMEDA의 목적은 각각의 컴포넌트가 해당 블록 또는 범용장치 전체에 어떠한 영향을 미치는지 분석하고 위험 및 검지 여부에 대한 영향을 파악한다.[7]

각 컴포넌트의 정량적 입력 데이터는 각 소자의 기본 고장률이 사용된다. 기본 고장률은 각 공급사에서 제공되는 고장률과 그렇지 않을 경우, 고장률 예측을 통해 산출된다. 고장률 예측은 IEC TR 62380을 기반으로 예측되었다.

기본 고장률이 산출되면 각 기본고장률은 해당 컴포넌트 고장의 위험 상관성 및 고장검지 가능여부를 파악하는 등 안전성을 분석한다. 안전성을 분석할 Vital 데이터 처리장치를 구성하는 전체의 컴포넌트의 수는 Table 5와 같으며 본 논문에서는 그 중 하나의 분석에 대한 일부분을 보여준다.

Table 5. Component configuration

Component Name	Quantity
Capacitor	296
Resistor	198
Diode	42
Fuse	2
Connector	28
Bead	4
Inductor	6
MOSFET	6
Switch	6
Temperature sensor	4
Integrated Circuit	92
DC/DC Convertor	12
Photo coupler	12
Dot Matrix	2
Crystal	5
Socket	2
Total	717

Component FMEDA는 Table 6.과 같은 방법으로 수

행 되며 본 논문에서는 특정 디바이스의 분석 내용만 제시된다.

Component FMEDA는 Table 5의 모든 컴포넌트에 대해 동일한 방법으로 수행되며 분석 결과 값은 각각의 고장률의 합으로 결정된다. 여기서 도출된 결과 값은 시간당 고장확률을 구하기 위한 입력 데이터로 활용된다. Table 5에서와 같이 17종의 모든 컴포넌트에 대한 FMEDA를 수행한 결과는 아래와 같다.

- $\lambda_{basic} = 8.682350 \times 10^{-6}$: 기본고장률(신뢰성 예측 데이터)
- $\lambda_{safe} = 3.833027 \times 10^{-6}$: 안전한 고장률
- $\lambda_{dangerous} = 2.806476 \times 10^{-6}$: 위험한 고장률
- $\lambda_{don't\,care} = 2.040847 \times 10^{-6}$: 무시할만한 고장률
- $\lambda_{SD} = 9.902678 \times 10^{-7}$: Safe/Detectable 고장률
- $\lambda_{SU} = 2.452921 \times 10^{-6}$: Safe/Undetectable 고장률
- $\lambda_{DD} = 2.807977 \times 10^{-6}$: Dangerous/Detectable 고장률
- $\lambda_{DU} = 3.000303 \times 10^{-8}$: Dangerous/Undetectable 고장률

2.5.1.2 β-factor(공통원인고장)

시간당 고장확률을 구하기 위해서는 시스템 내에 내

Table 6. Component FMEDA

Func Block ID	Sub block ID	Component ID	Qnt.	Component Name	Part Number	Basic Failure (Windchill) (10^-9)	Failure Mode	Failure Causes	Failure effects 1.block 2.module
Block-01	Block-01-01	L100	1	EMI Filter (Inductor)	BLM18PG600SN1D	7.132255	Open-circuit	component fault, overcurrent	1. 1.2 V power to U100 MCU's PLL monitoring circuit is cut off. Operating clock supply to MCU internal circuit is cut off. 2. Dangerous as U100 MCU can stop operating and maintain incorrect output.
						7.132255	Short-circuit	component fault	1. Upon U100 MCU's PLL operation, power high-frequency noise cannot be eliminated. 2. U100 MCU's PLL malfunctions and can cause the internal circuit operation clock to fail.

Dectection method	System Operation after appling failure dection	Safe/ dangerous	Failure Ratio(%)	λ_safe	λ_dangerous	λ_don't care	DC	λ_SD	λ_SU	λ_DD	λ_DU
Visual check, Watch-dog with time-window(IEC 61508-2 Table A.11: Watch-dog with separate time base and time-window), Independent 2-channel Architecture (IEC 61508-2 Table A.7, Input comparsion/ voting(1oo2, 2oo3 or better redundancy)	If MCU operation is stopped, A-ALIVE_OUT signal is cut off and Safey Relay can no longer be run. Block enters Safe state and block is safe. The independent Channel B detects link-fail from Channel A through Block-12 inter-communication SPI and switches to Safe state.	Safe	50%	0	3.5661×10^-9	0	99%	0	0	3.5304×10^-9	3.5661×10^-11
Redundancy	Use multiple capacitor (BC112 to BC121) to eliminate high-frequency noise for the 1.2 V power and thus allow safe operation.	Safe	50%	0	3.5661×10^-9	0	99%	0	0	3.5304×10^-9	3.5661×10^-11

포된 공통원인고장을 발견해야 한다. 공통원인고장 β-factor는 다음 공식에 의해 도출된다.

$$\lambda_{DU}\beta+\lambda_{DD}\beta_D$$

각각의 공통원인 β는 IEC 61508-6에서 제시된 점수 산정 방법이 적용되었으며 Vital 정보처리 범용장치 하드웨어 내의 공통원인 고장으로 제한된다. 공통원인 고장은 IEC601508-6 table D.1에서 보여지는 항목에 대한 점수를 산정하고 아래 계산식에 의해 구해진다.

$$\beta \rightarrow S = X + Y$$

$$\beta_D \rightarrow S_D = X(Z+1) + Y$$

공통원인고장에 대한 결과는 아래와 같다.

· Total X: 26.00
· Total Y: 24.80
· Score S: 50.80
· β: 2.0%
· Score SD: 50.80
· βD: 2.0%

2.5.1.2.1 Z Value

진단 범위와 진단시험 간격에 따른 공통원인 βD값을 구하기 위한 또 하나의 변수가 산출되어야 한다.

변수 Z는 다음 기준에 의해 산출된다.

Table 7. Value of Z

DC	Diagnostic test interval		
	Less than 1 min	Between 1 min 5 min	Greater than 5 min
≥99%	2.0	1.0	0
≥90%	1.5	0.5	0
≥60%	2.0	0	0

Z의 산출결과는 아래와 같다.

· Diagnostic: 90% 이상
· Diagnostic test interval: 1~5분
· Result: 0.5

2.5.1.3 등가평균 정지시간 계산(t_{CE})

시간당 고장확률 값을 구하기 위해 각각의 위험 측 고장률, 공통원인 고장 이외에 또 필요한 정보로 Vital 데이터 처리장치 구조(1oo2)에 대한 채널 등가 평균 정지시간을 구해야 한다. 채널의 고장 확률에 대하여 각 컴포넌트의 기여 정도에 정비례하는 두 컴포넌트에서 얻어진 개별적인 정지시간 t_{c1}과 t_{c2}를 더하여 채널 등가 평균정지 시간을 계산할 수 있고 계산공식은 다음과 같다.

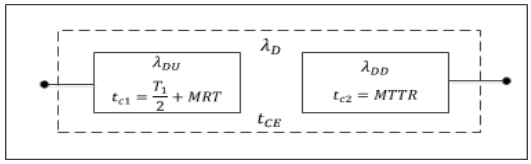

Fig. 4. t_{CE} Calculation

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

t_{CE}의 계산 결과는 다음과 같다.

· $\lambda_{dangerous} = 2.80848 \times 10^{-6}$
· $\lambda_{DU} = 3.0003 \times 10^{-8}$
· $\lambda_{DD} = 2.80797 \times 10^{-6}$
· $MRT/MTTR = 0.55$

Vital 데이터 처리장치 특성상 MRT(평균 수리시간)와 MTTR(평균 복구 시간)은 동일하며 다음과 같은 프로세스의 의해 산출된다.

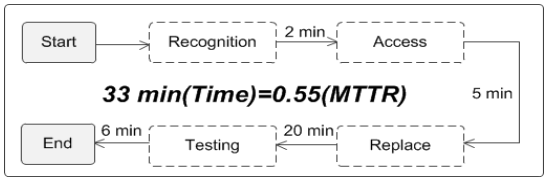

Fig. 5. Maintenance procedure

2.5.2 시간당 고장확률 계산 결과

시간당 고장확률을 구하기 위해 산출된 각 파라미터의 산출 결과는 아래 Table 8과 같다.

Table 8. Result of calculation

Classification	Analysis Method	Parameter	Rusult
Basic FR	Windchill	λ	8.68235×10^-6
Safety FR	Component FMEDA	λ_safe	3.88303×10^-6
Dangerous FR		λ_dangerous	2.80848×10^-6
No Safety		λ_don't care	2.04084×10^-6
Diagnostic Coverage		DC	98.94%
Safe/Detectable FR		λ_SD	9.90267×10^-7
Safe/Undetectable FR		λ_SU	2.45292×10^-6
Dangerous/Detectable FR		λ_DD	2.80797×10^-6
Dangerous/Undetectable FR		λ_DU	3.00030×10^-8
Common Cause Failure	β-table	β	2.00%
		βD	2.00%
Channel equivalent mean down time	Equation	tCE	1603.01

위 파라미터 들을 시간당 고장확률 구하는 수식(2.5.1

절)에 대입하여 계산하면 최종적으로 다음과 같은 결과 값이 도출된다.

· **시간당 고장확률(위험 측 고장에 대한 평균 빈도수):** 1.172279×10^{-9}

위 결과 값은 모든 컴포넌트(17종, 717개)에 대한 분석결과이며 Table 3의 기준에 의하면 SIL3 수준보다 더욱 낮은 위험고장확률로 나타난 것을 알 수 있다.

3. 결론

Vital 데이터 처리장치의 안전성을 확보하기 위해 Safety Integrity 요구사항을 도출하고 그에 따른 정량적 안전성분석을 수행하였다. 안전성 분석을 위해 우선적으로 각 공급사에서 제공받은 고장률과 신뢰성 Tool을 이용한 고장률 예측 결과를 통해 정량적 분석에 이용될 기본 데이터를 확보하였다. 그리고 시간당 고장확률 계산에 필요한 파라미터를 산출하기 위해 Component FMEDA를 수행하였다. 그 외에 시간당 고장확률 계산을 위한 파라미터인 공통원인 고장 및 등가평균 정지시간은 IEC 61508에서 제시한 방법을 통해 산출하였다.

결과적으로, Vital 데이터 처리장치의 위험노출에 대한 시간당 고장확률은 산출된 각각의 파라미터를 IEC 61508에서 제시한 공식에 대입하여 계산하였다. 계산결과, Vital 데이터 처리장치의 위험관련 고장에 대한 평균 빈도수는 1.172279×10^{-9}로 계산되었으며 계산된 이 수치는 목표한 SIL3의 수준(IEC 61508 기준)보다 훨씬 더 낮은 발생 확률을 보이는 것으로 확인되었다.

위 결과로 보아 정량적인 안전성 분석은 정성적 안전성분석에 비해 수치적으로 확인이 가능하여 명확하게 목표 값에 만족하는지의 평가가 가능하기 때문에 보다 신뢰성 높은 결과라 평가받을 수 있다.그리고 추후 보드단위 Vital 데이터 처리장치의 정량적 안전성분석의 결과가 Generic Application, 또는 그 이후의 Specific Application 범위 안전성분석의 기본 데이터로 활용된다면 FTA, ETA 등과 같은 다양한 안전성 분석방법 등을 통해 보다 신뢰성 높은 안전성활동 수행이 가능할 것으로 예상된다.

References

[1] "IEC 61508-6 Functional safety of electrical/ electronic/programmable electronic safety-related systems-Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3", p.27-94, 2010.

[2] Tieling Zhang, Wei Long, Yoshinobu Sato, "Availability of systems with self-diagnostic components-applying Markov model to IEC 61508-6", Reliability Engineering & System Safety, Volume 80, Issue2, p.133-141, May 2003.
DOI: http://dx.doi.org/10.1016/S0951-8320(03)00004-8

[3] Haitao Guo, Xianhui Yang, "A simple reliability block diagram method for safety integrity verification." Reliability Engineering & System Safety, Volume 92, Issue9, p.1267-1273, September 2007.
DOI: http://dx.doi.org/10.1016/j.ress.2006.08.002

[4] Israel Koren, C. Mani Krishna, "Fault-Tolerant Systems." p.11-41, MORGAN KAUFMANN PUBLISHERS, 2007.

[5] K. A. L. van Heel, "Safety life-cycle management. A flowchart presentation of the IEC 61508 overall safety life-cycle model", Quality and Reliability Engineering International, Volume 15, Issue 6, pages 493-500, November/December 1999.
DOI: http://dx.doi.org/10.1002/(SICI)1099-1638(199911/12)15:6<493::AID-QRE299>3.0.CO;2-X

[6] S. Brown, "Overview of IEC 61508. Design of electrical/electronic/programmable electronic safety-related systems", Computing & Control Engineering Journal, Volume 11, Issue 1, pages 6-12, February 1999.
DOI: http://dx.doi.org/10.1049/cce:20000101

[7] Vinod Chandra, "Reliability and safety analysis of fault tolerant and fail safe node for use in a railway signalling system", Reliability Engineering & System Safety, Volume 57, Issue 2, pages 177-183, August 1997.
DOI: http://dx.doi.org/10.1016/S0951-8320(97)00020-3

[8] Koji IWATA, "Risk Evaluation Method for Improvement of Railway Signalling Systems", Quarterly Report of RTRI, Volume 51, pages 205-213, December 2010.
DOI: http://dx.doi.org/10.2219/rtriqr.51.205

최 진 우(Jin-Woo Choi) **[정회원]**

- 1985년 2월 : 중앙대학교 전기공학과 졸업
- 2013년 2월 : 우송대학교 철도대학원 철도전기정보통신공학과 졸업
- 2013년 3월 ~ 현재 : 우송대학교 박사과정 재학
- 1990년 1월 ~ 1999년 12월 : LG 산전
- 2000년 1월 ~ 현재 : 대아티아이(주) 대표이사
- 2004년 6월 ~ 현재 : 한국철도대학 산학협력단 산학협의회 위원
- 2004년 7월 ~ 현재 : (사)한국도시철도협회 이사
- 2012년 2월 ~ 현재 : SW공제조합 이사

<관심분야>
RAMS, CBTC, 안전관제

박 재 영(Jae-Young Park) **[정회원]**

- 1996년 8월 : 고려대학교 산업대학원 전기공학과 (공학석사)
- 2007년 2월 : 서울산업대학교 철도전문대학원 철도전기신호공학과 (공학박사)
- 1970년 2월 ~ 2004년 12월 : 철도청 서울신호제어사무소장
- 2005년 1월 ~ 2007년 2월 : 한국철도공사 오송고속철도전기사무소장
- 2007년 3월 ~ 2015년 5월 현재 : 우송대학교 철도전기시스템학과 교수

<관심분야>
자동제어, 지능형시스템, 제어계측