ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 66, No. 9, pp. 1373~1378, 2017
http://doi.org/10.5370/KIEE.2017.66.9.1373

차량 내 네트워크 통신의 기능안전성을 위한 하드웨어 기본 설계

Basic Design of ECU Hardware for the Functional Safety of In-Vehicle Network Communication

곽 현 철* · 안 현 식†
(Hyun Chul Koag · Hyun-Sik Ahn)

Abstract - This paper presents a basic ECU(Electronic Control Unit) hardware development procedure for the functional safety of in-vehicle network systems. We consider complete hardware redundancy as a safety mechanism for in-vehicle communication network under the assumption of the wired network failure such as disconnection of a CAN bus. An ESC (Electronic Stability Control) system is selected as an item and the required ASIL(Automotive Safety Integrity Level) for this item is assigned by performing the HARA(Hazard Analysis and Risk Assessment). The basic hardware architecture of the ESC system is designed with a microcontroller, passive components, and communication transceivers. The required ASIL for ESC system is shown to be satisfied with the designed safety mechanism by calculation of hardware architecture metrics such as the SPFM(Single Point Fault Metric) and the LFM(Latent Fault Metric).

Key Words : ISO26262, ESC(Electronic Stability Control), CAN(Controller Area Network), Functional safety, ASIL(Automotive Safety Integrity Level), HARA(Hazard Analysis and Risk Assessment)

1. 서 론

최근 차량 내 다양한 제어 시스템이 기존의 유압 및 기계 장치를 이용한 시스템에서 전자 장치를 이용한 시스템으로 대체되고, 운전자의 편의 및 안전과 관련된 다양한 기술이 적용됨으로써 차량 내 전자 부품의 수가 크게 증가하고 있다. 이에 따라 차량 내 전자 장치의 고장으로 인해 발생할 수 있는 잠재적 위험 상황을 인식하고 이에 대한 대책 수립을 통해 위험을 제거하거나 회피하며, 시스템의 신뢰성을 높이기 위한 기능 안전(Functional Safety)의 중요성이 높아지고 있다[1][2]. 이러한 요구에 맞추어 유럽의 OEM 및 주요 부품 업체를 중심으로 제품의 개발, 생산, 폐기에 이르는 전체 생명 주기에서 안전 요구사항을 정의하여 차량의 기능 안전을 확보하기 위한 차량 기능 안전성 국제 표준인 ISO 26262가 제정되었으며, 국내 부품업체에도 이 표준안에 따른 제품 개발이 요구되고 있다[3].

또한, 차량 내 전자 부품이 증가함에 따라 전자 부품들 간 또는 이를 제어하기 위한 ECU(Electronic Control Unit) 간 배선의 수가 증가하여 무게와 생산 비용이 늘어나고, 차량의 정비성이 떨어지게 되었다[4][5]. 이러한 문제를 해결하기 위해 다수의 전자부품과 ECU를 하나의 버스로 연결하여 배선 수를 줄인 CAN, FlexRay 와 같은 차량 내 네트워크 시스템이 등장하였다[6]. 그러나 유선 네트워크 시스템은 단선, 발화 등의 고장이 발생할 수 있으며, 이는 운전자의 안전에 치명적이므로 높은 고장 허용 능력이 요구된다. 이러한 고장에 대처하기 위해 CAN 컨트롤러의 다중화, 추가적인 CAN 버스 구현 등의 방법이 연구되었지만, 단선과 같은 유선 네트워크의 고장을 본질적으로 해결하기는 어렵다. 따라서 차량 내 유선 네트워크를 무선 네트워크로 보조하거나 대체하기 위한 관련 연구가 시도되고 있으며, 특히 ZigBee는 낮은 전송속도에도 불구하고 메쉬 네트워크 형성 기능, 낮은 전력 소모 등의 장점을 가지고 있어 차량 내 유선 네트워크를 대체하기에 적합한 무선 네트워크 프로토콜로 평가되고 있다[7][8].

본 논문에서는 대표적인 차량 네트워크인 CAN 노드의 단선과 같은 고장으로부터 차량의 기능 안전을 확보하기 위하여 기존의 유선 네트워크에 ZigBee 무선 네트워크를 병용하는 네트워크 시스템을 제안하고 ISO 26262 표준안에 따른 ECU간 통신 시스템의 하드웨어 설계 절차를 제시한다. 이를 위한 대상 아이템으로 ESC(Electronic Stability Control) 시스템을 선정하며 정상 동작 중인 ESC 시스템에서 발생할 수 있는 하나의 위험원으로 CAN 노드의 단선을 가정한다. 이에 대한 리스크 평가를 통해 목표 ASIL (Automotive Safety Integrity Level) 등급을 결정하고 안전 목표(Safety Goal)를 설정하며, 도출된 안전 관련 요구사항을 바탕으로 기본 하드웨어를 설계한다. CAN 노드가 단선되었을 경우, 무선 네트워크 프로토콜을 이용하여 통신을 지속할 수 있는 안전 메커니즘을 설계하며, 이러한 안전 메커니즘이 적용된 하드웨어를 정량적으로 평가하여 할당된 ASIL 등급에서 요구하는 기

† Corresponding Author : School of Electrical Engineering, Kookmin University, Korea.
E-mail: ahs@kookmin.ac.kr
* Dept. of Secured-Smart Electric Vehicle, Kookmin University, Korea.
Received : July 18, 2017; Accepted : August 1, 2017

준의 만족 여부를 확인한다.

2. ESC 시스템의 제어 체계

최근 차량의 안전한 자세제어를 위하여 필수적으로 요구되는 ESC 시스템은 일반적으로 그림 1과 같이 ESC 제어기와 차량 모델을 이용하여 설명할 수 있다[9]. 사용자로부터의 조향 입력이 ESC 제어기와 차량 모델로 전달되며, 이 조향각과 차량 모델로부터 출력되는 차속을 입력으로 하는 2-자유도 참조 모델로부터 기준 요 속도(Reference yaw rate)를 계산한다. ESC 제어기는 기준 요 속도와 차량의 실제 요 속도를 비교하여 이를 기반으로 각 바퀴의 기준 제동 토크(Reference brake torque)를 계산하며, 이는 CAN 네트워크를 통해 차량 모델로 전달된다. 또한 차량 모델로부터 휠 각속도, 실제 요 속도, 차속 등의 정보들이 CAN 네트워크를 통해 ESC 시스템으로 피드백 되어 활용되므로, CAN 네트워크의 고장 발생 시 ESC 시스템의 정상적인 동작이 불가능하다. 따라서 본 논문에서는 차량 내 네트워크의 고장으로 인한 ESC 시스템에서의 영향을 분석하고 이에 기초하여 기능 안전성이 적용된 차량 내 ECU 간 통신 시스템의 하드웨어를 설계한다.

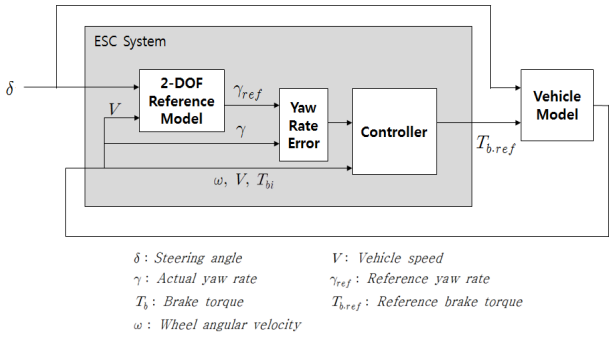

그림 1 ESC 시스템의 제어 체계
Fig. 1 Block diagram of ESC system

3. ISO 26262 표준안 핵심단계에 따른 ESC 제어기 하드웨어 설계

차량의 기능안전성 표준안인 ISO 26262는 10개의 Part와 43개의 요구 사항(Requirements) 또는 권고 사항(Recommendations)으로 구성되어 있으며, 제품 개발 초기부터 생산, 폐기에 이르는 전체 생명 주기에서의 안전 관련 요구사항을 제시하고 있다. 또한 각 Part 별 상호 관련성에 따른 V 모델 개념을 기반으로 제품 개발 프로세스가 진행되고, 전체 프로세스 중 핵심 프로세스는 개념단계(Part 3), 시스템 레벨 제품개발 단계(Part 4), 하드웨어 레벨 제품개발 단계(Part 5), 그리고 소프트웨어 레벨 제품개발 단계(Part 6)이다[10]. 본 논문에서는 ESC 시스템을 대상으로 ISO 26262 표준안의 핵심 절차를 따라 설계하는 절차를 제안하고 하드웨어 메트릭 연산을 통하여 요구되는 ASIL 등급이 만족됨을 보이기로 한다.

3.1 개념 단계

개념 단계(Part 3 : Concept phase)에서는 아이템 정의를 통하여 기본적인 기능을 정의하고 아이템에서 발생할 수 있는 위험원에 대한 리스크 평가를 통하여 안전 목표를 도출한다. ESC 제어시스템에 대한 아이템 정의의 예는 표 1과 같다.

표 1 ESC 시스템의 아이템 정의 예
Table 1 Item definition of ESC system

Item Function	Yaw stability control of a vehicle
Item Description	When the intended direction is not the same as the driving direction, the direction of vehicle is controlled to follow the intended direction by braking individual wheels based on measurement of steering angle and yaw rate.
Item Malfunction	Unintended operation Late operation No operation

표 2 심각성(S), 노출성(E), 가제어성(C)에 따른 ASIL 등급 할당
Table 2 ASIL determination based on S, E and C ratings

Severity class	Probability class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

또한, 선정한 아이템에서 발생 가능한 하나의 위험원으로 CAN 노드의 단선을 가정하고 이에 대한 위험원 분석과 리스크 평가(Hazard Analysis and Risk Assessment, HARA)를 수행하여 아이템의 목표 ASIL 등급을 결정한다. ASIL 등급은 대상 아이템이 달성하고자 하는 기능 안전성의 수준을 나타내는 것으로, ASIL D 등급에 가까울수록 기능 안전성을 달성하기 위해 더 높은 수준의 요구사항을 만족해야 한다. 일반적으로 위험원의 심각성(Severity: S), 노출성(Exposure: E) 및 가제어성(Controllability: C) 정도에 따른 ASIL 등급 결정은 표 2와 같이 정의되어 있으며[11], 본 논문에서 정의한 아이템의 경우 표 3과 같이 고려될 수 있으므로(S3, E3, C3), ASIL 등급은 C 등급으로 결정된다. 또한 위험원 분석 및 리스크 평가 수행을 통해 위험

표 3 ESC 시스템의 HARA 수행 결과
Table 3 HARA result for ESC system

Level	Vehicle
Request	CAN communication request in ESC system
Hazard description	Disconnection of CAN node
Scenario	Highway
Hazard effect	Unintended operating of ESC system
Severity	S3
Exposure	E3
Controllability	C3
ASIL	C
Safety Goal	Maintenance of ESC system function

사건의 방지 혹은 완화에 관련된 안전 목표를 설정하며, 이에 따라 안전 상태를 유지하기 위한 아이템 수준의 기능 안전 요구사항(Functional Safety Requirement)을 명시한다. 위험원 분석 및 리스크 평가를 통해 도출된 안전 목표는 ESC 시스템의 기능이 유지될 수 있도록 하는 것이며, 이에 따른 기능 안전 요구사항은 위험 사건인 CAN 노드의 단선이 발생한 경우에도 네트워크 통신이 지속될 수 있도록 하는 것이다.

3.2 시스템 레벨의 제품 개발

시스템 레벨의 제품 개발 단계(Part 4 : Product development at the system level)에서는 개념 단계에서 명시한 기능 안전 요구사항을 시스템 레벨에서 실제로 구현할 수 있도록 기술 안전 요구사항(Technical Safety Requirement)을 명시한다[12]. 여기서 기술 안전 요구사항은 CAN 노드의 단선 발생 시 이를 감지하고 고장이 발생한 노드의 통신을 무선 통신 방식으로 전환하여 ECU 간의 통신이 지속되도록 하는 것이며, 본 논문에서는 이 추가 통신 채널로서 무선통신 프로토콜인 ZigBee의 사용을 제안한다. 이와 같이 아이템의 기능을 유지하기 위해 독립적인 하드웨어를 추가적으로 사용하는 하드웨어 이중화 구조는 추후 하드웨어 설계 시 고려되는 안전 메커니즘 중 Complete hardware redundancy에 해당하며, 이는 표 4에 나타낸 바와 같이 높은 수준의 결함 진단 범위(Diagnostic Coverage)를 갖는다[13]. 또한 기술 안전 요구사항을 적용하여 설계한 ESC 시스템의 예비 아키텍처 모델은 그림 2와 같다.

표 4 ISO 26262 part 5 Annex D – Table D.8 : Communication Bus
Table 4 ISO 26262 part 5 Annex D – Table D.8 : Communication Bus

Safety mechanism/measure	See overview of techniques	Diagnostic Coverage
One-bit hardware redundancy	D.2.7.1	Low(60%)
Timeout monitoring	D.2.7.8	Medium(90%)
Complete hardware redundancy	D.2.7.3	High(99%)

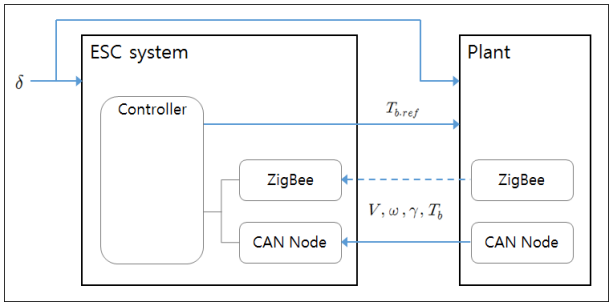

그림 2 ESC 시스템의 예비 아키텍처 모델
Fig. 2 Preliminary architecture model of ESC system

표 5 ESC 시스템의 FMEA 수행 예
Table 5 FMEA of ESC system

Potential Failures	Potential Effect(s) of Failure	SEV	Potential Cause(s) / Mechanism(s) of Failure	OCC	Detection Measure	DET	RPN
Unintended operating of ESC system	Rear-end collision due to emergent braking by driver	6	Corrupted CAN node Corrupted ESC system micro-controller Corrupted yaw sensor node	5	Hardware redundancy (ex. Redundant CAN bus, dual-core ESC MCU, TMR for yaw sensor node, etc.)	9	270
No operating of ESC system	Collision accident due to over yaw motion of vehicle	9	Disconnected CAN node Corrupted ESC system micro-controller Corrupted yaw sensor node	4	Hardware redundancy (ex. Redundant CAN bus, dual-core ESC MCU, TMR for yaw sensor node, etc.)	9	324

시스템 설계 분석 기법인 FMEA(Failure Mode and Effect Analysis)는 제품 개발 초기 단계에서부터 제품에 발생할 수 있는 잠재적 고장을 식별하고, 이에 대한 원인 및 영향을 분석함으로써 이를 제거 또는 완화시킬 수 있도록 하는 정성적 고장 분석 기법이다[14]. FMEA를 실시하기 위해서는 제품에 발생할 수 있는 잠재적 고장의 심각도(Severity: SEV), 발생 빈도(Occurrence: OCC), 검출도(Detection: DET)를 분석해야 하며, 이를 기반으로 해당 고장의 리스크에 따른 우선순위(Risk Priority Number: RPN)를 결정한다. 이와 같이 ESC 시스템에 대한 FMEA를 간략히 수행한 예시는 표 5에 나타낸 바와 같다. ESC 시스템이 동작하지 않는 것이 안전과 관련하여 더 높은 우선순위를 갖는 고장 모드이므로, 이에 따라 본 논문에서는 해당 고장의 발생원인 중, CAN 노드의 단선에 대한 안전 메커니즘을 적용하여 하드웨어를 설계하기로 한다.

3.3 하드웨어 레벨의 제품 개발

하드웨어 레벨의 제품 개발 단계(Part 5 : Product development at the hardware level)에서는 도출된 기술 안전 요구사항으로부터 하드웨어 안전 요구사항(Hardware Safety Requirement)을 명시하며, 이를 적용하여 하드웨어를 설계한다. 또한 설계한 하드웨어를 정량적으로 평가하여 아이템에 할당된 ASIL 등급에서 요구하는 기준을 만족하는지 확인한다. 본 논문에서의 하드웨어 안전 요구사항은 기존의 CAN 네트워크 이외에 ZigBee 모듈을 추가함으로써 ECU간 통신 채널의 이중화 설계를 통해 고장에

대한 강인성을 가지는 것을 목표로 하며, 이를 기반으로 설계한 하드웨어의 회로도는 그림 3과 같다.

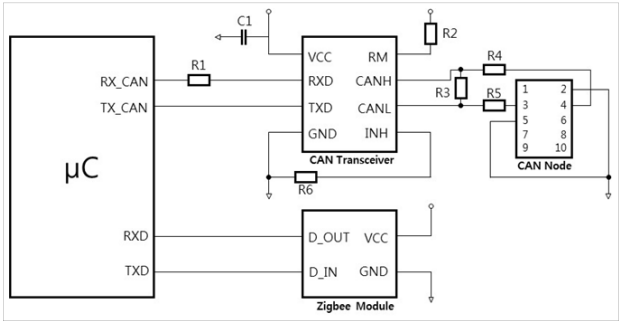

그림 3 안전 메커니즘이 적용된 ESC 시스템 회로도
Fig. 3 ESC system circuit diagram applied safety mechanism

설계한 하드웨어를 정량적으로 평가하기 위해서는 하드웨어에서 발생 가능한 고장 형태 중, 안전 목표와 관련된 고장 형태를 우선 분류하여야 한다. 하드웨어에 대한 일반적인 정량적 평가는 발생 즉시 안전 목표를 위배할 수 있는 단일점 결함(Single Point Fault), 결함에 대한 안전 메커니즘이 존재하나 안전 메커니즘에 의해 보호되지 않는 잔존 결함(Residual Fault), 그리고 안전 메커니즘에 의해 검출되거나 운전자에 의해 인지되지 않아 잠재적으로 안전 목표를 위배할 수 있는 잠재 결함(Latent Fault)만을 대상으로 한다.

또한, 하드웨어 아키텍처 메트릭은 설계된 하드웨어의 안전 관련 적합성을 평가하기 위한 안전 분석(Safety Analysis)의 한 방법으로, 단일점 결함 메트릭(SPFM)과 잠재 결함 메트릭(LFM)으로 구분된다[15]. SPFM은 하드웨어에 존재하는 모든 안전 관련 결함 중 단일점 결함과 잔존 결함을 제외한 결함의 비율을 의미하며, 식 (1)과 같이 계산할 수 있다. 또한 LFM은 단일점 결함과 잔존 결함을 제외한 안전 관련 결함 중 잠재 결함을 제외한 결함의 비율을 의미하며, 식 (2)와 같이 계산할 수 있다. 설계된 회로(하드웨어)에 대한 메트릭 계산을 통해 ASIL 등급 목표치(표 6 참조)가 만족되는지 확인할 수 있다.

$$SPFM = 1 - \frac{\sum_{SR}(\lambda_{SPF}+\lambda_{RF})}{\sum_{SR}(\lambda)} = \frac{\sum_{SR}(\lambda_{MPF}+\lambda_{S})}{\sum_{SR}(\lambda)} \quad (1)$$

$$LFM = 1 - \frac{\sum_{SR}(\lambda_{MPFLatent})}{\sum_{SR}(\lambda_{F}-\lambda_{SPF}-\lambda_{RF})} = \frac{\sum_{SR}(\lambda_{MPFP/D}+\lambda_{S})}{\sum_{SR}(\lambda_{F}-\lambda_{SPF}-\lambda_{RF})} \quad (2)$$

λ_{SPF} : 단일점 결함 고장률, λ_{RF} : 잔존결함 고장률,
λ_{MPF} : 다중결함 고장률, $\lambda_{MPFP/D}$: 감지 및 인지 결함 고장률,
λ_{S} : 안전 결함 고장률, λ_{F} : 전체 결함 고장률

표 6 ASIL 등급에 따른 SPFM 및 LFM 목표치
Table 6 Targets for SPFM and LFM according to ASIL

	ASIL B	ASIL C	ASIL D
SPFM	≥ 90%	≥ 97%	≥ 99%
LFM	≥ 60%	≥ 80%	≥ 90%

표 7 설계한 하드웨어의 SPFM 및 LFM 계산
Table 7 SPFM and LFM for designed hardware

C	F	FM	FD	SR	SM	DC	λSPF	λRF	λMPF_Latent
R1	0.3	Open	40%	O	O	99%		0.001	
		Short	40%	O	X				0.12
		Drift0.5	10%						
		Drift2.0	10%						
R2	0.3	Open	40%	O	O	99%		0.001	
		Short	40%						
		Drift0.5	10%						
		Drift2.0	10%						
R3	0.3	Open	40%	O	O	99%		0.001	
		Short	40%	O	X		0.12		
		Drift0.5	10%	O	X		0.03		
		Drift2.0	10%	O	X		0.03		
R4	0.3	Open	40%	O	O	99%		0.001	
		Short	40%	O	X				0.12
		Drift0.5	10%						
		Drift2.0	10%						
R5	0.3	Open	40%	O	O	99%		0.001	
		Short	40%	O	X				0.12
		Drift0.5	10%						
		Drift2.0	10%						
R6	0.3	Open	40%	O	O	99%		0.001	
		Short	40%						
		Drift0.5	10%						
		Drift2.0	10%						
C1	10.0	Open	40%						
		Short	40%	O	O	99%		0.04	
		Drift0.5	10%						
		Drift2.0	10%						
uC	3.29			O	O		0.66		2.63
XBee	15.0			O	O	99%		0.15	
CAN Trans	20.0			O	O	99%		0.2	
Total	50.09			43.55			0.84	0.396	2.99

C: Component Name, F: Failure Rate, FM: Failure Mode,
FD: Failure rate Distribution, SR: Safety Related,
SM: Safety Mechanism, DC: Diagnostic Coverage

4. 하드웨어 설계 검증

위와 같이 설계된 차량 내 통신시스템 하드웨어의 ASIL 등급을 확인하기 위하여 회로내 저항과 전해 커패시터 등 수동 소자, MCU, CAN Transceiver 및 ZigBee 모듈 등을 대상으로 SPFM 및 LFM의 결과값 산출 과정을 표 7에 나타내었다. 하드웨어 아키텍처 메트릭 계산은 IEC62380 또는 SN29500 등의 규격을 참조하여 각 소자의 고장률을 이용하여 계산한다. 메트릭을 수행한 결과, 표 8에 나타낸 바와 같이 SPFM은 97.16%, LFM은 92.93%로 아이템에 할당된 ASIL C 등급 목표치를 만족하는 것

표 8 SPFM 및 LFM 계산 결과
Table 8 Result of SPFM and LFM

Safety Goal		ASIL	SPFM Target Value		>97%
Maintenance of ESC system function		C	LFM Target Value		>80%
Total		Single-Point		Latent	
Failure Rate (in FIT)	50.09	Total Failure Rate (in FIT)	1.236	Total Failure Rate (in FIT)	2.99
Safety Related (in FIT)	43.55				
Not Safety Related (in FIT)	6.54	Fault Metric	97.16%	Fault Metric	92.93%

표 9 ASIL 등급에 따른 PMHF 평가 기준
Table 9 Evaluation Criteria of PMHF according to ASIL

ASIL	Random hardware failure target values
D	$< 10^{-8} h^{-1}$ (10FIT)
C	$< 10^{-7} h^{-1}$ (100FIT)
B	$< 10^{-7} h^{-1}$ (100FIT)

을 확인할 수 있다.

또한, 안전 목표를 위배할 수 있는 하드웨어의 우발적인 고장에 대하여도 잔존 리스크가 충분히 낮다는 것을 보이기 위해 하드웨어 우발 고장률(Probability Metric of Random Hardware Failure, PMHF) 평가를 수행한다. PMHF 평가를 수행하기 위해서는 FTA 등을 이용하여 정량화된 안전 목표의 위배 가능성을 평가하며, 이를 표 9에 나타낸 안전 목표의 ASIL 등급에 따른 목표치와 비교한다. 여기서, SPFM 및 LFM을 수행한 경우 PMHF의 정량적 수치는 식 (3)과 같이 나타낼 수 있으며, 설계된 하드웨어에 대한 PMHF는 4.226 FIT로써 역시 ASIL C 등급에서의 목표치를 만족하는 것을 확인할 수 있다[16].

$$PMHF = \sum \lambda_{SPF} + \sum \lambda_{RF} + \sum \lambda_{MPF} \quad (3)$$

5. 결 론

본 논문에서는 급격히 증가하고 있는 차량 내 전자제어장치 또는 전자부품 간 네트워크 시스템의 기능 안전을 위하여 차량 기능안전성 관련 국제 표준인 ISO 26262에서 제시하는 개발 절차 중 개념 단계부터 하드웨어 개발 단계까지의 표준안을 따라 실제 하드웨어 설계 및 검증 방법을 제시한다. 위험원 분석 등을 통하여 적절한 목표 ASIL 등급을 설정하고 이 목표 등급을 달성하기 위한 안전 메커니즘으로서 ZigBee 무선통신 네트워크를 병용하는 차량내 통신 시스템을 제안하였다. ESC 시스템을 하나의 아이템으로 선정하고 발생 가능한 위험원으로 CAN 노드의 고장을 가정하였으며, HARA를 수행하여 요구되는 기능 안전성 등급이 ASIL C 등급으로 결정되었다. 실제 설계된 하드웨어에 대하여 하드웨어 메트릭, SPFM과 LFM의 계산을 수행한 결과 목표 등급인 ASIL C 등급 기준이 만족되는 것을 확인하였다.

감사의 글

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 육성지원사업(IITP-2017-2012-0-00628)의 연구결과로 수행되었습니다.

References

[1] K. L. Leu, H. Huang, Y. Y. Chen, L. R. Huang and K. M. Ji, "An Intelligent Brake-By-Wire System Design and Analysis in Accordance with ISO-26262 Functional Safety Standard." International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2015.

[2] S. H. Jeon, J. H. Cho, Y. J. Jung, S. C. Park and T. M. Han, "Automotive Hardware Development According to ISO 26262.", International Conference on Advanced Communication Technology (ICACT), IEEE, 2011.

[3] C. Tao, "Functional Safety Concept Design of Hybrid Electric Vehicle following ISO 26262." Transportation Electrification Asia-Pacific (ITEC Asia-Pacific), IEEE Conference and Expo. IEEE, 2014.

[4] H. Schubotz, "Hazard Analysis and Risk Assessment for Complex EE-Architecture," SAE Technical Paper 2010-01-0029, 2010.

[5] S. M. Mahmud and S. Alles, "In-Vehicle Network Architecture for the Next-Generation Vehicles," SAE Technical Paper 2005-01-1531, 2005.

[6] S. M. Yang, S. Y. Kim, Y. H. Ki and H. S. Ahn, "ECU-In-the-Loop Simulation for ESC Performance Analysis on the Selection of in-Vehicle Networks." Transactions of the Korean Society of Automotive Engineers, Vol. 21, No. 5, pp. 87-96, 2013.

[7] A. D. G. Reddy and B. Ramkumar, "Simulation Studies on ZigBee Network for in-Vehicle Wireless Communications.", International Conference on Computer Communication and Informatics (ICCCI), IEEE, pp. 1-6, 2014.

[8] AC. Ai, F. Zhang and R. Liu, "Research on Wireless Backup for CAN in Process Control System.", 1st Annual RFID Eurasia, pp. 1-6, 2007.

[9] Y. Ying, L. Weiguo and I. S. Tukur, "Performance Analysis and Simulation of Vehicle Electronic Stability Control System.", Computing and Applications for Business Engineering and Science (DCABES), 14th International Symposium on IEEE, pp. 415-418, 2015.

[10] P. Srivastava, M. Karle, U. S. Karle, and A. A. Deshpande, "Development of Electrical Power Assisted Steering (EPAS) Considering Safety and Reliability

Aspects as per ISO 26262.", SAE Technical Paper 2015-26-0086, 2015.
[11] ISO 26262 Road vehicles - Functional safety - Part 3: Concept phase, 2011.
[12] ISO 26262 Road vehicles - Functional safety - Part 4: Product development at the system level, 2011.
[13] ISO 26262 Road vehicles - Functional safety - Part 5: Product development at the hardware level, 2011.
[14] M. Hillenbrand, M. Heinz, N. Adler, J. Matheis and K. D. Müller-Glaser, "Failure Mode and Effect Analysis based on Electric and Electronic Architectures of Vehicles to Support the Safety Lifecycle ISO/DIS 26262.", Proceedings of 21st IEEE International Symposium on Rapid System Protyping. IEEE, 2010.
[15] N. Adler, S. Otten, P. Cuenot and K. Adler, N., Otten, S., Cuenot, P., & Müller-Glaser, "Performing Safety Evaluation on Detailed Hardware Level According to ISO 26262.", SAE Technical Paper 2013-01-0182, 2013.
[16] Y. C. Chang, L. R. Huang, H. C. Liu, C. J. Yang and C. T. Chiu, "Assessing Automotive Functional Safety Micro-processor with ISO 26262 Hardware Requirements.", International Symposium on VLSI Design, Automation and Test (VLSI-DAT), IEEE, pp. 1-4, 2014.

저 자 소 개

곽 현 철 (Hyun Chul Koag)

2016년 8월 : 국민대학교 전자공학과(학사)
2016년 9월~현재 : 국민대학교 보안-스마트 전기자동차학과 석사과정
관심분야 : 차량전자제어시스템, 임베디드 시스템

안 현 식 (Hyun-Sik Ahn)

1992년 2월 : 서울대학교 제어계측공학과 (공학박사)
1993년~현재 : 국민대학교 전자공학부 교수
관심분야 : 차량전자제어시스템, 지능제어, 임베디드시스템