

< 응용 논문 >

반도체 수준의 FMEDA 수행 방안

박 병 규* · 주 백 수 · 이 승 환

에스피아이디 엔지니어링 사업본부

The Method to Perform Semiconductor Level FMEDA

Byoungkyu Park* · Baegsu Joo · Seunghwan Lee

Engineering Division, SPID Co. Ltd., 145 Gasan Digital1-ro, Geumcheon-gu, Seoul 08506, Korea

(Received 15 July 2020 / Revised 28 September 2020 / Accepted 5 October 2020)

Abstract : Quantitative evaluation of random failure for semiconductor elements is essential in the development of automotive semiconductors that comply with the ASIL B or higher functional safety ISO 26262 standard. The most preferred method for performing these quantitative assessments is the FMEDA analysis technique. FMEDA, along with the introduction of ISO 26262, is a quantitative safety analysis that has been used in the overall automotive industry for many years. However, the domestic semiconductor industry has little practical experience with FMEDA, perhaps because it is in the early process of introducing the functional safety ISO 26262. Moreover, since there are few FMEDA-related data suitable for the semiconductor level, it is difficult to understand and apply to semiconductor analysis. The aim of this paper is to gain a better understanding of the quantitative safety analysis at the semiconductor level by presenting a method of performing the FMEDA at the semiconductor level from a practical point of view.

Key words : Functional safety(기능안전) ISO 26262(자동차 기능 안전성 국제 표준), Random hardware failure(하드웨어 우발 고장), Base failure rate(기본 고장률), Failure modes effects and diagnostics analysis(고장모드 영향 및 진단 분석), Quantitative safety analysis of semiconductor level(반도체 수준의 정량적 안전분석), Semiconductor(반도체)

Nomenclature

ADS	: automated driving system
ASIL	: automotive safety integrity level
BFR	: base failure rate
DC	: diagnostic coverage
E/E System	: electric/electronic system
EOS	: electric over stress
FIT	: failure in time
FMEDA	: failure modes effects and diagnostics analysis
FSR	: functional safety requirement
HW	: hardware
IP	: intellectual property
SG	: safety goal
SPI	: serial peripheral interface
SW	: software
TSR	: technical safety requirement

1. 서론

자동차 산업은 기존 기계류 중심의 개발 환경에서, E/E System 즉, 전기전자 시스템으로 개발 패러다임이 급격하게 변화하고 있다. 요즘 자동차 산업에서의 최신 트렌드는 당연 ADS(자율 주행 시스템)¹⁾ 일 것이다. 자율 주행 시스템은 움직이는 컴퓨터와 다름이 없다고 해도 과언이 아니다. 이러한 변화 속에서 E/E System의 근간이 되는 반도체의 중요성은 논란의 여지가 없다. 그러하기 때문에, 2018년 12월에 발표된 기능안전 ISO 26262 2nd에서는 새로이 반도체 부분을 추가하였다. “ISO 26262 Part 11: Guidelines on application of ISO 26262 to semiconductors”²⁾가 그것이다.

ISO 26262 Part 11²⁾은 반도체에 대한 기능안전 ISO 26262:2018 적용 가이드라인으로서 Part 3, 4, 5, 6, 7과 같

*Corresponding author, E-mail: pbk@espid.com

¹⁾This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

은 핵심 파트와 달리 요구사항은 아니나, 기능안전 반도체 적용에 있어서 참고할 만한 지침을 제공한다. 이 지침에는 기능안전을 준수하는 반도체의 개발은 기본적으로 Part 5 하드웨어 개발 요구사항³⁾을 준수할 것을 권고하고 있으며, 필요에 따라서는 Part 4 시스템 개발 요구사항⁴⁾이나 Part 6 소프트웨어 개발 요구사항⁵⁾ 역시 적절히 테일러링 하여 수행할 것을 권고한다. 어찌 됐든 Part 5의 하드웨어 개발 요구 사항³⁾들을 준수해야 하므로 반도체에 대한 우발 고장을 정량적으로 평가하여야 한다.

본 논문은 이러한 정량적 평가에 있어서 일반적으로 사용되는 FMEDA 기법을 반도체 수준에 맞춰 소개하고, 이에 대한 작성 절차를 ISO 26262-11:2018 4.6.2.1.1²⁾에서 적용된 IEC TR 62380:2004⁶⁾를 기반으로 설명한다.

2. 반도체 분석의 세분화 수준

정성적이든 정량적이든 간에 안전 분석을 위한 주요 측면 중 하나는 분석을 기반으로 하는 계층 구조의 수준을 적절하게 식별하는 것이다. 대개의 경우, 분석의 세분화 수준을 낮추는 것이 고장 모드 및 고장 모드 분포를 더 잘 이해하는 것으로 볼 수 있다.²⁾ 하지만, 그렇다고 필요 이상으로 분석의 수준을 깊게 할 경우, 개발 과정에서 너무 많은 리소스가 요구되어 개발 비용 및 제품 출시 일정 등에 영향을 줄 수 있으므로 주의가 요구된다.

2.1 제어기/반도체의 구성 분류 및 ‘Part’에 대한 고찰

아래 Fig. 1은 제어기 및 반도체의 구성 분류를 보여주는 그림으로서, ISO26262-10:2011 Fig. 3,⁷⁾ ISO2626-10:2018 Fig. 3, Fig. 4,⁸⁾ ISO26262-11 Fig. 2²⁾를 참조하였다.

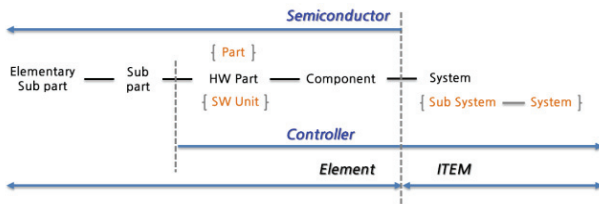


Fig. 1 Classification for composition of controller and semiconductor

Fig. 1에서 보듯이 Controller 수준에서의 최하위 구성 단위는 ‘HW Part’이다. ISO 26262:2011 1st는 주로 Controller 중심으로 기술하였기 때문에, ‘Part’를 ‘소자’(Passive 부품류: 저항, 캐패시터, 인덕터 / Discrete 부품류: 다이오드, 트랜지스터, FET류)라고 번역될 수 있었으나,⁹⁾ ISO 26262:2018 2nd에서 반도체 부분이 추가됨으로써, ‘Part’를 ‘소자’라고 딱히 번역하기 어려운 상황이

되었다. 이 경우의 ‘Part’는 반도체 내부를 구성하는 엘리먼트들인 CPU, ADC, PWM, TIMER 등을 지칭하는 것이기 때문이다. 그러므로 본문에서는 ‘Part’를 ‘소자’ 또는 ‘부품’이라 하지 않고 ‘Part’ 또는 ‘파트’라고 기술한다.

2.2 반도체 구성 엘리먼트에 대한 분류

아래 Fig. 2는 ISO 26262-11:2018에서 보여준 반도체 컴포넌트의 일반적인 구성이다.²⁾

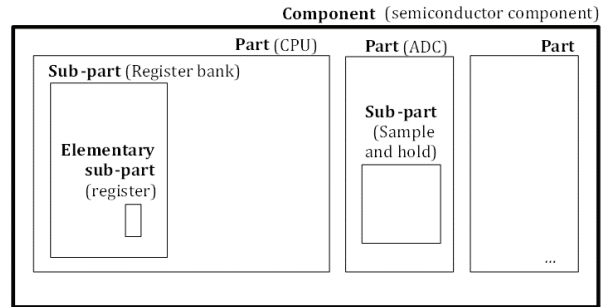


Fig. 2 A semiconductor, its parts and sub-parts²⁾

Fig. 2를 보듯이 반도체 컴포넌트는 다음과 같은 구성 요소로 분해될 수 있다.²⁾ 참고로, IP(지적 재산)에는 Fig. 2에 표현된 Part, Sub-part, Elementary sub-part를 포함한다.

- 1) Component: 논리적/기술적으로 분리가 가능하고 하나 이상의 Part로 구성된 엘리먼트
- 2) Part: 반도체 내부의 CPU, ADC, PWM, Timer 등을 가리키는 구성 엘리먼트
- 3) Sub-part: Part의 하위 수준으로서, Part를 구성하는 구성 엘리먼트
- 4) Elementary sub-part: 레지스터와 같은 기초 하위 엘리먼트

분석의 세분화 수준은 반도체 아키텍처가 반도체 구성 요소의 어느 부분까지 표현하고 있는지에 따라 달라질 수 있겠으나, 적어도 반도체 수준의 정량적 분석의 최소 깊이는 Sub-part일 것을 권장한다.

3. 반도체 수준의 FMEDA 수행

다음은 반도체 수준의 FMEDA 수행 방안을 기술한 내용이다. 참고로 본문의 3.1~3.7항은 작업 순서를 의미하는 것이 아니기 때문에, 한 단계가 끝나야만 다음 단계로 진행할 수 있는 구조가 아니다. 즉, FMEDA 수행 과정에서 각 항은 언제나 반복 및 갱신될 수 있다. 그리고 3.1~3.6항은 3.7항을 수행하기 위한 준비 과정으로 볼 수 있으며, 사용된 모든 예시는 이해를 돕기 위해 작성된 것이다.

3.1 최상위 안전 요구사항의 할당

3.1.1 목적

- 1) 분석 대상 반도체에 할당된 안전 요구사항과 관련된 반도체 안전 관련 엘리먼트들을 식별하고,
- 2) 식별된 안전 관련 엘리먼트들의 고장을 분석하여 안전 고장, 단일점 고장, 잔존 고장, 다중점 잠재 고장과 같은, 고장 모드를 분류하기 위함이다.

3.1.2 수행 방안

- 1) 하나의 안전 목표로부터 파생된 안전 요구사항들만을 기술한다.
- 2) 다른 안전 목표로부터 파생된 안전 요구사항들은 별도의 FMEDA 분석에서 다룬다. 이는 안전 목표로부터 파생된 최상위 안전 요구사항에 따른 반도체 엘리먼트의 고장 모드 분류를 정확하게 하기 위함이며, 또한 정량적 목표값을 하나로 가지기 위함이다.
- 3) 되도록 하위 안전 요구 사항들을 포괄할 수 있는 상위 요구 사항을 기술한다.
- 4) 필요시 안전목표(SG) 및/또는 ASIL 등급을 병행하여 기입한다.

3.1.3 수행 예시

- 1) TSR1: 두 입력을 비교하여 차이 값이 허용치 이상일 경우, High side와 Low side의 출력 신호를 100 ms 이내로 차단시켜야 한다(ASIL B).

- 2) TSR2: 칩 내부의 에러를 검출하면, 진단 코드를 100 ms 이내로 출력해야 한다.(ASIL B)

3.2 구조 분석(Structure Analysis)

3.2.1 목적

- 1) 반도체 아키텍처를 상세 분석하여 분석 대상의 이해를 돕고,
- 2) 반도체를 구성하는 엘리먼트들에 대한 기본 고장률 (BFR) 계산 시 필요한 정보를 제공하기 위함이다.

3.2.2 수행 방안

위의 목적을 위해 반도체 아키텍처로부터 Table 1과 같은 반도체구조 분석 테이블을 작성한다. 다음은 Table 1에 기술할 내용을 설명한다.

- 1) Part/Sub-part name: 분석 대상 반도체 엘리먼트의 이름이다. 일관성을 위해 아래 Fig. 3 반도체 아키텍처에 기술된 블록 이름과 같아야 한다.
- 2) Volt: 반도체 엘리먼트에서 사용되는 전압을 기술한다. 사용 전압에 따라 Transient fault(일시적인 결함) 값이 달라짐으로, 이 값은 일시적 결함률을 구할 때 사용한다.
- 3) Description: 분석 대상 반도체 엘리먼트에 대한 기능을 기술한다.

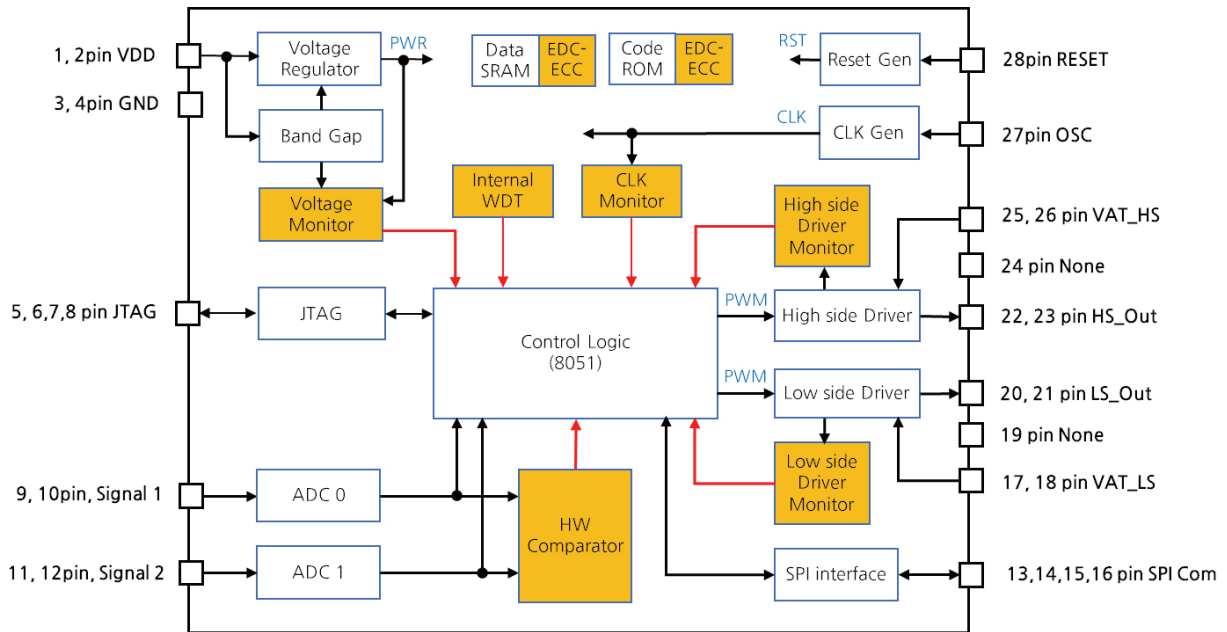


Fig. 3 Example of the semiconductor architecture

Table 1 Example of semiconductor structure analysis result

No	Part/Sub-part name	Volt	Description	Parts type	Semiconductor technology		Number of gate	Number of transistor
1	Voltage regulator	5.0 V	After generating a constant voltage of 3.3 V (± 0.2 V) from the 5 V input power, it is supply power to all IPs in the chip.	Analog part	Silicon: MOS : Standard circuits	Linear circuits	1,075.44	4,301.75
2	Voltage monitor	3.3 V	It monitors the case where the output voltage value of the voltage regulator exceeds 3.6 V and when it is less than 3.0 V. When an error occurs, an error signal is generated.	Analog part	Silicon: MOS : Standard circuits	Linear circuits	80.97	323.88
3	Bandgap reference	3.3 V	Generate a reference voltage for the ADC. The voltage fluctuation according to the temperature difference is suppressed by using the threshold voltage of the forward direction of the PN channel. It has a temperature coefficient of -2.3 mV / °C.	Analog part	Silicon: MOS : Standard circuits	Linear circuits	108.08	432.32
4	Data SRAM	3.3 V	It is a volatile memory for temporarily storing data. It has a size of 4 kBy.	Digital part	Silicon: MOS : Standard circuits	Low consumption SRAM	49,152.00	196,608.00
5	Code flash ROM	3.3 V	It is a non-volatile memory for permanently storing data. It has a size of 16 Kbyte.	Digital part	Silicon: MOS : Standard circuits	ROM	196,608.00	786,432.00
6	EDC-ECC	3.3 V	Error detection-correction logic to RAM that corrects all single bit fault (single error correction, SEC) and detects all double bit fault (double error detection, DEC)	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	3,235.56	12,942.26
7	SPI	3.3 V	SPI communication interface. It outputs an error message by communicating with the Master MCU.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	5,443.76	21,775.04
8	Internal WDT	3.3 V	Internal watchdog timer	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	235.56	942.26
9	HW comparator	3.3 V	Compare input values received from input logic channel 0 and input logic channel 1 as a Hardware-based. If the difference value is more than the allowable value, an error signal is generated.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	20,363.23	81,452.94
10	ADC 0	3.3 V	Analog-to-digital converter 0	Mixed part	Silicon: MOS : Standard circuits	Digital/linear circuits(Telecom, CAN, CAN, RAMDAC, ...)	13,075.39	52,301.54
11	ADC 1	3.3 V	Analog-to-digital converter 1	Mixed part	Silicon: MOS : Standard circuits	Digital/linear circuits(Telecom, CAN, CAN, RAMDAC, ...)	13,078.03	52,312.12
12	High-side driver	40 V	The output signal according to the control logic (High side) is sent out.	Analog part	Silicon: Bipolar and MOS circuits (BICMOS)	Linear / digital circuits, high voltage(≥ 6 V) and Smart Power	1,908.64	7,634.54

Table 1 Example of semiconductor structure analysis result

No	Part/Sub-part name	Volt	Description	Parts type	Semiconductor technology		Number of gate	Number of transistor
13	Low-side driver	40 V	The output signal according to the control logic (Low side) is sent out.	Analog part	Silicon: Bipolar and MOS circuits (BICMOS)	Linear / digital circuits, high voltage (≥ 6 V) and Smart Power	1,883.64	7,534.55
14	High side driver monitor	3.3 V	It monitors the operation for High-side driver.	Analog part	Silicon: MOS : Standard circuits	Linear circuits	311.63	1,246.53
15	Low side driver monitor	3.3 V	It monitors the operation for Low-side driver.	Analog part	Silicon: MOS : Standard circuits	Linear circuits	309.06	1,236.24
16	CLK Gen	3.3 V	Supplies a clock for each IP logic.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	1,132.33	4,529.32
17	CLK monitor	3.3 V	Always monitor CLK Gen IP to detect clock errors.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	832.20	3,328.80
18	Reset Gen	3.3 V	When reset ON, the reset signal is active, then supplied to all IPs in the chip. When reset OFF, the reset signal is disable.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	1,965.24	7,860.94
19	Control logic	3.3 V	8051 core is built in, and is in charge of arithmetic operation and control. The output of the high side driver and low side driver is controlled by PWM method according to the ADC input value. Error signals are collected from each monitoring IP and transmitted to the Master ECU through SPI communication.	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	252,386.43	1,009,545.73
20	JTAG	3.3 V	JTAG interface. (For executable file loading and debugger.)	Digital part	Silicon: MOS : Standard circuits	Digital circuits, Micros, DSP	1,156.98	4,627.92

- 4) Parts type: 분석 대상 반도체 엘리먼트의 Type을 기술한다. Type은 ‘Digital part’, ‘Analog part’, ‘Mixed part’가 있다.
- 5) Semiconductor technology: 분석 대상 반도체 엘리먼트 별로 적용된 반도체 기술 유형(Semiconductor technology)을 기술한다. 예를 들어, Fig. 3과 같은 반도체 Architecture가 주어진 경우, IEC TR 62380 Table 16⁶⁾의 분류에 따라 Digital parts는 Digital circuits에 해당되며, Analog low voltage Parts는 Linear circuits low voltage (<6 V)에 해당되고, Analog high voltage parts는 Linear circuits high voltage (≥ 6 V)에 해당된다.
- 6) Number of gate: 분석 대상 반도체 엘리먼트에 대한 등가 게이트 개수를 기술한다.
- 7) Number of transistor: 분석 대상 반도체 엘리먼트에 대한 등가 트랜지스터 개수를 기술한다.

3.2.3 수행 예시

Fig. 3은 반도체 아키텍처에 대한 예시이며, Table 1은 반도체 구조 분석 결과에 대한 예시이다. Fig. 3을 참조하여 Table 1을 작성한다.

3.3 안전 메커니즘 및 진단 커버리지

3.3.1 목적

- 1) 안전 요구사항을 위배할 가능성이 있는 반도체 엘리먼트의 고장 모드를 방지하거나 회피하기 위한 기술적 수단인 안전 메커니즘에 대한 기능 및 속성을 명세하고,
- 2) 안전 메커니즘의 진단 커버리지 값을 도출하기 위함이다.

3.3.2 작성 방안

위의 목적을 위해 아래의 Table 2를 작성한다. 다음은 Table 2에 기술할 내용을 설명한다.

- 1) Define of safety status at IC level : 반도체 수준의 안전 상태를 정의한다.
- 2) SM No : 안전 메커니즘의 ID를 기입한다.
- 3) SM Name : 안전 메커니즘 이름이다.
- 4) Detailed description : 안전 메커니즘에 대한 설명이다. 되도록 기능을 포함하는 작동 원리를 기술한다. 단일 점 결함을 방지하는 안전 메커니즘 또는 잠재 결함을 방지하는 안전 메커니즘이 있으나, 설계 방식에 따라서 하나의 안전 메커니즘이 둘 모두를 방지할 수도 있다. 참고로 “효과적인 FMEDA 수행을 위한 안전 메커니즘의 작성 방안과 진단 커버리지의 산정 방안”¹⁰⁾에서는 안전 메커니즘 기술 및 진단 커버리지 산정에 관한 참고할 만한 정보를 제공한다.
- 5) Timing : 안전 메커니즘이 동작하는 주기를 기술한다. 안전 메커니즘은 하드웨어 방식의 상시 동작 방식, 클럭 주기 방식, 소프트웨어 의한 일정 시간 주기 방식, 하드웨어 또는 소프트웨어 인터럽트에 의한 이벤트 방식, Power on/off시마다 한 번씩 동작하는 방식 등이

있다.

- 6) Type : 안전 메커니즘이 반도체 내부(Internal)에서 동작하는지 또는 반도체 외부(External)에서 동작하는지를 기술한다.
- 7) DC : 산정된 안전 메커니즘의 진단 커버리지 값을 ‘Avoidance of single point fault’ 및/또는 ‘Avoidance of latent fault’에 기술한다.
- 8) Rationale of evaluation : DC를 산출한 근거를 ‘Avoidance of single point fault’ 및/또는 ‘Avoidance of latent fault’에 기술한다. 해당 되는 경우, 결함 주입 시험에 의한 시험 결과를 포함한다.

3.3.3 작성 예시

아래 Table 2는 안전 메커니즘 및 진단 커버리지에 대한 내용을 기술한 예시이다. 참고로, SM-01, SM-03, SM-05, SM-06, SM-07, SM-08, SM-09, SM-011과 같은 안전 메커니즘에 대한 DC 산출에 있어서, 그 근거의 정당성을 증명해 줄 수 있는 세부적인 논리적 근거나 결함 주입 시험 결과는 본 예시에서 생략하였다. 이러한 세부적인 근거는 필요시 별도로 기술한다.

Table 2 Example of description of safety mechanism for semiconductor

Define of safety status at IC level		When an error is detected by the safety mechanism, the output signals of the High side and Low side are blocked within 100 ms, then an error signal is sent to Master ECU.							
SM No.	SM name	Detailed description	Property						
			Timing	Type	Avoidance of single point fault		Avoidance of latent fault		
					DC	Rationale of evaluation	DC	Rationale of evaluation	
SM-01	Voltage Monitoring	It monitors the case where the output voltage value of the voltage regulator exceeds 3.6 V and when it is less than 3.0 V. When an error occurs, an error signal is generated.	Always	Internal	99.0 %	Hardware-based monitoring. It claim to DC 99.0% for voltages exceeding (above 3.6 V) the allowed voltage range.	-	-	
			Always	Internal	99.0 %	Hardware-based monitoring. It claims to DC 99.0 % for voltages below (less 3.0 V) the allowed voltage range.	-	-	
SM-02	Clock Monitoring	Detection to clock error by at all time clock status monitoring. It has an error rate of ± 0.02 %.	-	Internal	96.0 %	In the case of ‘Jitter’ DC(%) = 1 - 0.04 = 96 %	-	-	
			20 clock cycle	Internal	99.0 %	In the case of ‘Stuck at fault’ DC(%) = 99 %	-	-	

Table 2 Example of description of safety mechanism for semiconductor

SM No.	SM name	Detailed description	Property					
			Timing	Type	Avoidance of single point fault		Avoidance of latent fault	
					DC	Rationale of evaluation	DC	Rationale of evaluation
SM-03	Built In Self Test	BIST(Built-in self-test) performs a self test on the monitoring logic inside the chip once after start-up.	One time	Internal	-	-	60.0 %	It claims to DC 60.0 % for BIST.
SM-04	HW Comparator	Compare input values received from ADC 0 channel and ADC 1 channel as a Hardware-based. If the difference value is more than the allowable value, an error signal is generated. It has an error rate of ± 0.1 %.	Event	Internal	99.8 %	$DC(\%) = 1 - 0.002 = 99.8 \%$	-	-
SM-05	EDC-ECC	Error detection-correction logic circuit to RAM that corrects all single bit fault (single error correction, SEC) and detects all double bit fault (double error detection, DEC)	Event	External	99.9 %	It claim to DC 99.9 % for the single bit fault.	-	-
			Event	External	60.0 %	It claim to DC 60.0 % for the double bit fault.	-	-
SM-06	ADC input check	After comparing the difference between the two values, check the validity of the input values received from ADC 0 and ADC 1 channels.	Event	Internal	99.0 %	It claim to DC 99.0 % for ADC input value validity.	-	-
			Event	Internal	-	-	99.0 %	The difference value comparison mechanism for ADC0 and ADC1 claim DC 99.0 %.
SM-07	Internal WDT	Built-in internal watchdog timer. It monitors stuck status of Control Logic.	200 ms	Internal	60.0 %	It claim to DC 60.0 % for 'control logic stuck'.	-	-
SM-08	High side driver monitor	It monitors the operation status of the High-side driver.	20 ms	Internal	99.0 %	It claim to DC 99.0 % regarding short/open failure of High-side drive.	-	-
SM-09	Low side driver monitor	It monitors the operation status of the Low-side driver.	20 ms	Internal	99.0 %	It claim to DC 99.0 % regarding short/open failure of Low-side drive.	-	-
SM-10	SPI COM monitoring	Monitors errors for messages received from the Master ECU. (8 bit CRC check)	Event	External	99.0 %	As it is an 8-bit check, $1-(1/2^8) = DC 99.0 \%$	-	-
SM-11	Control logic monitoring	The control logic is monitored by the master MCU. It is interfaced by SPI communication, and Control Logic returns the results within 10 ms when the Master MCU requests a specific arithmetic operation. The master MCU determines the error status of the Control Logic according to the results of the arithmetic operation received from the Control Logic.	20 ms	External	-	-	80.0 %	It claim to DC 80.0 % regarding SPI communication inability.
			20 ms	External	99.0 %	It claim to DC 99.0 % regarding computation fault for Control Logic.	-	-

3.4 미션 프로파일

3.4.1 목적

- 반도체에 대한 현장 사용 환경과 조건에 관한 설정으로서, 반도체가 사용되는 환경의 온도, 반도체 사용 패턴 등을 정하고,
- 이것을 반도체 엘리먼트 별 영구적인 기본 고장률 계산에 반영하기 위함이다.

3.4.2 작성 방안

- 고객으로부터 전달받은 Mission profile을 우선적으로 사용해야 하나, 그렇지 않은 경우, 신뢰할 만한 고장률 데이터 북을 활용하여 적용한다. ISO 26262:2018에서 제시되고 현업에서 Mission profile을 참고할 수 있는 신뢰할 만한 고장률 데이터 북에는 IEC 61709,¹¹⁾ ISO 26262-11:2018 4.6.2.1.1 (IEC TR 62380:2004),^{2,6)} FIDES 2009 EdA¹²⁾ 등이 있다.
- 아래 Table 3은 ISO 26262-11:2018 4.6.2.1.1(IEC TR 62380:2004)에서 제시된 자동차에 대한 Mission profile로서 다음은 이에 대한 설명이다.^{2,6)}

Table 3 Mission profiles for automotive^{2,6)}

Mission profile phases	Temp. 1	Temp. 2	Temp. 3	Ratio on/off	2 night starts	4 day light starts	Non used vehicle							
Application types	$(t_{ac})_1$ °C	r_1	$(t_{ac})_2$ °C	r_2	$(t_{ac})_3$ °C	r_3	r_{on}	r_{off}	n_1	ΔT_1 °C/cycle	n_2	ΔT_2 °C/cycle	n_3	ΔT_3 °C/cycle
Motor control	32	0.02 0	60	0.01 5	85	0.02 3	0.05 8	0.94 2	670	$\frac{\Delta T_1}{3} + 55$	1340	$\frac{\Delta T_2}{7} + 45$	30	10
Passenger compartment	27	0.00 6	30	0.04 6	85	0.00 6	0.05 8	0.94 2	670	$\frac{\Delta T_1}{3} + 30$	1340	$\frac{\Delta T_2}{7} + 20$	30	10

① IEC TR 62380의 Mission Profile은 연간 운용 사이클을 기반으로 하여 몇 가지 동질적인 동작 단계로 분해된다.

- 장비가 노출되는 다양한 평균 외부 온도에서 동작하는 On/Off working phases.
- 장비가 노출되는 다양한 평균 외부 온도에서 지속적으로 동작하는 Permanent working phases
- 장비가 노출되는 다양한 평균 외부 온도에서 저장 또는 휴면하는 Storage or dormant phases

② 필요한 Parameters는 아래와 같다.

$(t_{ac})_i$: 장비(제어기)의 i번째 phase에서 장비(제어기)를 둘러싼 평균 외부 대기 온도. 프랑스 기후의 경우는 11 °C이며, 전 세계적인 기후에 대해 14 °C를 유지

$(t_{ac})_i$: i 번째 phase에서(가장 중요한 것으로 간주되는) 컴포넌트(반도체) 주변 PCB의 평균 주변 온도.
 t_{ac} = average temperature increases of the PCB near components + t_{ac}

τ_i : $(t_{ac})_i$ 온도시 동작하는 시간의 연간 비율

τ_{on} : 전원이 공급되어 동작하는 전체 시간의 연간 비율

τ_{off} : 동작하지 않거나 저장/휴면 모드 상태로 있는 전체 연간 시간 비율

n_i : 평균 온도 변동 ΔT_i 를 동반한 i번째 Phase에 일치하는 PCB의 컴포넌트에 의해 보이는 온도 사이클 수량

ΔT_i : i 번째 단계에서 PCB의 구성 요소에서 볼 수 있는 열 변동의 평균 편차

On/Off working phases인 경우:

$$\Delta T_i = \left[\frac{\Delta T_j}{3} + (t_{ac})_j \right] - (t_{ac})_i$$

집적 회로 또는 discrete 소자인 경우라면, 접합 온도 상승이고, 수동 소자인 경우라면, 표면 온도 상승이다. 그 값의 3분의 1만이 ΔT_i 계산에 고려된다. 따라서 고려해야 할 온도는 내부 온도에 대한 절충안이며, 일부 열 시뮬레이션은 이 값의 1/3이 적절하다는 것을 보여준다.

Storage or Permanent working phase인 경우:

만일 이 값이 3 °C보다 낮으면, 이 값의 열 기계적 응력은 COFFIN-MANSON 방정식에서 열적으로 독립적이라는 조건을 고려하여 $\Delta T_i = 0$ 이 된다. 대부분의 적용에서 하루는 한주기에 해당하며, ΔT_i 는 고려된 기후에서 장비가 놓인 장소에서 보이는 밤과 낮의 온도 차이의 일일 평균에 해당.

프랑스의 기후는 $\Delta T_i = 8$ °C,

World-wide인 경우, $\Delta T_i = 10$ °C.

3.4.3 작성 예시

위 Table 3은 다음 사항이 고려되었다.

- 장비의 3가지 내부 작동 온도를 고려하고 각 온도에 대한 연간 작동 시간을 고려. 전체 운용 시간을 500시간으로 산정함.
- 아래와 같은 자동차의 열 순환을 고려함.

① Phase 1: 2 night starts

② Phase 2: 4 day light starts

③ Phase 3: non-used vehicle, dormant mode 30 days per year

위 Table 3을 보다시피 ISO 26262-11:2018 4.6.2.1.1 (IEC TR 62380:2004)에서 제시된 자동차에 대한 Mission profile에는 ‘Motor control’과 ‘Passenger compartment’라는 두 가지 파라미터들이 존재한다. 선택은 반도체가 적

용될 위치에 따라 달라진다. ‘Motor control’은 차량의 엔진 룸 또는 Chassis 부분이며, ‘Passenger compartment’는 승객 룸을 포함하는 차량의 Body 부분이다. ‘Motor control’이 Passenger compartment’보다 환경 조건이 열악하기 때문에, 장착 위치와 상관없이 보수적으로 계산하기 위해서 ‘Motor control’을 선택할 수 있다. 다음은 ‘Passenger compartment’에서 사용되는 파라미터 값을 설명한다.

$(t_{ac})_1$: 27 °C, 온도 사이클 3개 중 첫 번째 반도체 주변 PCB의 평균 주변 온도

τ_1 : 0.006, 27 °C 에서 동작하는 시간의 연간 비율

$(t_{ac})_2$: 30 °C, 온도 사이클 3개 중 두 번째 반도체 주변 PCB의 평균 주변 온도

τ_2 : 0.046, 30 °C에서 동작하는 시간의 연간 비율

$(t_{ac})_3$: 85 °C, 온도 사이클 3개 중 세 번째 반도체 주변 PCB의 평균 주변 온도

τ_3 : 0.006, 85 °C에서 동작하는 시간의 연간 비율

τ_{on} : 0.058, 전원이 공급되어 동작하는 전체 시간의 연간 비율로서, $\tau_1 + \tau_2 + \tau_3 = 0.006 + 0.046 + 0.006 = 0.058$ 또는 $500 / (365 \times 24) = 0.058$ 이다.

τ_{off} : 0.942, 동작하지 않거나 저장/휴면 모드 상태로 있는 전체 연간 시간 비율로서, $1 - \tau_{on} = 1 - 0.058 = 0.942$ 이다.

n_1 : 670, 평균 온도 변동 ΔT_1 을 동반한 첫 번째 Phase에 일치하는 PCB의 컴포넌트에 의해 보이는 온도 사이클 수량(2 night starts)으로서, $(365-30) \times 2 = 670$ cycles/year이다.

ΔT_1 : 첫 번째 단계에서 PCB의 구성 요소에서 볼 수 있는 열 변동의 평균 편차.

$(t_{ac})_1$ working phases 동안의 평균 온도 : $(0.006 \times 27 + 0.046 \times 30 + 0.006 \times 85) / 0.058 = 35$ °C

$(t_{ac})_1$: night starts phase에서 장비(제어기)를 둘러싼 평균 외부 대기 온도, world wide night 평균 온도 5 °C 적용. $(t_{ac})_1 - (t_{ac})_1 = 35$ °C- 5 °C = 30 °C

n_2 : 1340, 평균 온도 변동 ΔT_2 를 동반한 두 번째 Phase에 일치하는 PCB의 컴포넌트에 의해 보이는 온도 사이클 수량(4 day light starts)으로서, $(365-30) \times 4 = 1340$ cycles/year이다.

ΔT_2 : 두 번째 단계에서 PCB의 구성 요소에서 볼 수 있는 열 변동의 평균 편차

$(t_{ac})_2$ working phases 동안의 평균 온도 : $(0.006 \times 27 + 0.046 \times 30 + 0.006 \times 85) / 0.058 = 35$ °C

$(t_{ac})_2$: day light starts에서 장비(제어기)를 둘러

싼 평균 외부 대기 온도, world wide day 평균 온도 15 °C 적용. $(t_{ac})_2 - (t_{ac})_2 = 35$ °C - 15 °C = 20 °C

n_3 : 30, 평균 온도 변동 ΔT_3 을 동반한 세 번째 Phase에 일치하는 PCB의 컴포넌트에 의해 보이는 온도 사이클 수량(non-used vehicle)으로서, 30 cycles/ year (dormant mode 30 days per year)이다.

ΔT_3 : 세 번째 단계에서 PCB의 구성 요소에서 볼 수 있는 열 변동의 평균 편차.

Permanent working phase, storage or dormant에서는 장비가 본 사이클 당 최대 및 최소 온도 차이의 평균을 적용하기 위해 world wide $\Delta T_3 = 10$ °C 적용한다.

3.5 기본 고장률(BFR) 산정

3.5.1 목적

1) 안전 메커니즘을 전혀 반영하지 않는 상태에서 반도체 엘리먼트에 대한 기본 고장률을 산정하기 위함이다.

3.5.2 작성 방안

기본 고장률에는 영구적인 것과 일시적인 것이 있으며, 서로 별도로 다루어지는 고장률이다. 다음은 이에 대한 작성 방안을 설명한다.

1) 영구적인 고장률(Permanent failure rate) 산정:

‘3.2 구조 분석’으로 부터 얻은 자료를 기반으로 반도체 엘리먼트에 대한 영구적인 고장률을 산정한다. Fig. 4는 엑셀 매크로를 활용한 반도체 엘리먼트에 대한 영구적인 고장률 산정을 보여준다. 참고로 “하드웨어 우발 고장 평가를 위한 기본 고장률 산정 및 고장 모드, 고장 모드 분포율 도출 방안”¹³⁾에서는 반도체 엘리먼트에 대한 영구적인 기본 고장률 계산에 대한 참고할 만한 정보를 제공해 준다. 다음은 Fig. 4에 대한 간략한 설명이다.

① Common factor:

- Select the mission profile: ‘Motor control’ 또는 ‘Passenger compartment’ 둘 중 하나를 선택한다.
- Manufacturing year: 반도체 제조 연도를 입력한다.
- Package information: 반도체 Package에 대한 정보를 입력한다.
- Dissipated power by the component: 반도체 소비 전력을 입력한다.

1. Common Factor

Select the Mission Profile : Passenger compartment

Manufacturing year : 2018 year
 a [year of manufacturing]-1998 : 20

Package Information :
 Which is table 17a or table 17b ? And package type : Table 17b : Two rows connections packages
 Package category (for RTH_{ja}): SOI
 Package type: SSOP
 S (number of pins) : 28
 Pin pitch : 1.27 mm
 Package Width : 7.65 mm
 Package Length : 17.70 mm
 Package Diagonal : - mm

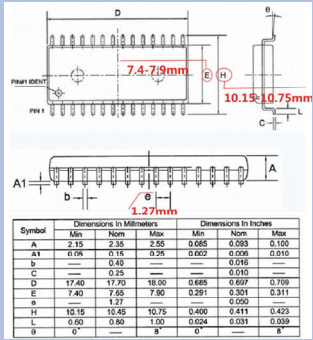
Dissipated power by the component : 0.30 W

K (air flow factor) : 1.4 : Natural Convection(자연 대류) 0.15m/s

RTH_{ja} (°C/W) : 86.01

ΔT_j = 25.80 °C

Junction Temperature
 (t_j)₁ = 52.80 °C
 (t_j)₂ = 55.80 °C
 (t_j)₃ = 110.80 °C



Symbol	Dimensions in Millimeters			Dimensions in Inches		
	Min	Nom	Max	Min	Nom	Max
A	2.15	2.35	2.55	0.085	0.093	0.100
A1	0.08	0.18	0.25	0.003	0.006	0.010
b	—	0.40	—	—	0.016	—
C	—	0.25	—	—	0.010	—
D	17.40	17.90	18.90	0.685	0.697	0.709
E	7.40	7.65	7.90	0.291	0.301	0.311
e	—	1.27	—	—	0.050	—
H	10.15	10.45	10.75	0.400	0.411	0.423
L	0.60	0.80	1.00	0.024	0.031	0.039
g	0	—	0	0	—	0

increase of the internal temperature of the component as compared to t_{sc} during a τ_{on} phase. (This is the junction temperature increase for an integrated circuit or a discrete device; this is the surface temperature increase for a passive device.)

2. Die:

Assignment of failure rate by Parts

Part of Semiconductor Die	Effective failure rate of sub part divided by number of transistors (FIT)
1 Digital circuits, Micros, DSP	24.217
2 Low consumption SRAM	4.151
3 FLASH	16.604
4 Linear circuits	0.159
5 Linear / digital circuits, high voltage (>=6V) and Smart	0.320
6 Digital/linear circuits(Telecom, CAN, CAN, RAMDAC, ...)	2.209
7 None	0.000
8 None	0.000
9 None	0.000
10 None	0.000
Total Die Effective failure rate (FIT)	47.660

3. Package :

α_s = 16.000 : Epoxy Glass(FR4 / G-10)
 α_c = 21.500 : Epoxy (Plastic package)
 |α_s - α_c| = 5.500
 π_{cs} = 0.06 × (|α_s - α_c|)^{1.68} = 1.052

(π_{cs})₁ = 140.545
 (π_{cs})₂ = 238.012
 (π_{cs})₃ = 13.262

(t_{sc})_{AVG} = 35.379 : average temperature during the working phase for (t_{sc})_{1,2,3}

ΔT₁ = 38.601
 ΔT₂ = 28.601
 ΔT₃ = 10.000

λ₃ value by Table 17a (manual input) : - FIT
 λ₃ value by Table 17b (It is calculated automatically) : 3.140 FIT

λ_{package with solder joints} = 37.032 FIT : Package failure rate including solder joints between package and board
 λ_{package without solder joints} = 29.625 FIT : Total package failure rate without solder joints between package and board (80 % of package failure rate with solder)
 λ_{total} = 1.058 FIT : The package failure rate is assumed to be equally distributed among the pins

4. EOS (Electric Over Stress) :

λ_{EOS} = 20 FIT
 π₁ = 0 Non Interfaces

5. Results of BFR(Base Failure Rate) value.

Total Effective Base Failure Rate (FIT) without package : 47.660 FIT
 Total Effective Base Failure Rate (FIT) with package : 77.285 FIT

Fig. 4 Example of calculation for semiconductor permanent failure rate

- K(Air flow factor): 반도체 냉각 방식에 따라 선택된다. 이를 위해 IEC TR 62380 Table 13을 참조한다.
 - RTH ja (°C/W) : Thermal resistance between Junction and Ambient atmosphere. 수식에 의해 자동으로 계산된다.
 - ΔTj : 접합부 온도 증가. 수식에 의해 자동으로 계산된다.
- ② Die: 반도체 Die에 존재하는 반도체 엘리먼트별 고장률(Fit)이다.
 - ③ Package: 반도체 Package에 대한 고장률(Fit)이다.
 - ④ EOS: 반도체가 EOS에 노출될 경우 계산된다.
 - ⑤ Result of BFR(Base Failure Rate) value: 반도체 Die와 package를 포함하는 반도체 기본 고장률 값이다.
- 2) 일시적인 고장률(Transient failure rate) 산정:
 일시적인 결함은 영구적인 결함과는 달리 결함이 한번 발생하여 사라지는 결함으로써, 소프트 에러라고도 한다.²⁾ 소프트 에러는 반도체 내부에서 알파선 혹은 중성자선 등에 의해 야기되는 전하에 의해 집적회로의 논리 노드 혹은 기억 노드의 신호 전위를 일시적으로 변동시키거나 반전시켜 발생하는 오류를 의미한다.^{2,14)} 이러한 일시적인 고장률은 측정된 데이터로 지원되는 확률론적 방법으로만 정량화할 수 있는 우발 고장이다.^{2,14)} 그러므로 일시적인 고장률은 반도체 웨이퍼 및 패키지에 중성자선을 조사(照射)하여 측정된 데이터를 통해 얻게 된다.

3.5.3 작성 예시

- 1) 영구적인 고장률(Permanent failure rate)
 Fig. 4는 IEC TR 62380⁶⁾에 근거한 반도체의 영구적인 고장률 계산 예를 보여준다.
- 2) 일시적인 고장률(Transient failure rate)
 메모리 및 디지털 파트에 대한 일시적인 고장률 값을 Foundry 업체로부터 얻는다. Table 4는 SRAM에 대한 일시적인 고장률 예를 보여준다. 사용 전압에 따라 Mbit 당 일시적인 고장률 값이 달라짐을 볼 수 있다.

Table 4 Example of transient failure rate for SRAM

Condition	Fit / Mbit
3.3V	312
5.0V	578

3.6 기본 고장률 할당(BFR Allocation)

3.6.1 목적

- 1) Die의 경우, 동일 유형을 가진 Part 단위의 고장률을 개

별 하위 Sub-part 단위로 고장률을 분할하여 할당하기 위함이다.

- 2) Package의 경우, Pin 당 고장률을 적용하기 위함이다.

3.6.2 작성 방안

- 1) Die의 경우

- ① 반도체 Die를 구성하는 전체 면적에서 개별 엘리먼트가 차지하는 면적을 나눔으로써 이루어지거나,²⁾
- ② 반도체 Die를 구성하는 전체 등가 게이트 개수 또는 등가 트랜지스터 개수에서 개별 엘리먼트가 소비하는 등가 게이트 개수 또는 등가 트랜지스터 개수를 나눔으로써 얻어질 수 있다.²⁾

- 2) Package의 경우

다음과 같은 방식으로 구해진다.

1/(비 안전 관련 핀 포함하는 전체 Pin 개수)²⁾

3.6.3 작성 예시

- 1) Die의 경우:

- ① 면적에 의한 방법

Table 5 Example of BFR allocation based on area

Part	Sub part	Block area (mm ²)	Part ratio	Failure rate
Part 1 10 FIT	Sub part 1-1	0.12	0.158	1.579
	Sub part 1-2	0.24	0.316	3.158
	Sub part 1-3	0.4	0.526	5.263
Sum		0.76	1.000	10.000
Part 2 15 FIT	Sub part 2-1	0.07	0.171	2.561
	Sub part 2-2	0.05	0.122	1.829
	Sub part 2-3	0.29	0.707	10.610
Sum		0.41	1.000	15.000

- ② 등가 게이트 또는 등가 트랜지스터 개수에 의한 방법

Table 6 Example of BFR allocation based on equivalent gates number or equivalent transistors number

Part	Sub part	Number of transistors	Part ratio	Failure rate
Part 1 10 FIT	Sub part 1-1	10,000	0.222	2.222
	Sub part 1-2	15,000	0.333	3.333
	Sub part 1-3	20,000	0.444	4.444
Sum		45,000	1.000	10.000
Part 2 15 FIT	Sub part 2-1	30,000	0.400	6.000
	Sub part 2-2	25,000	0.333	5.000
	Sub part 2-3	20,000	0.267	4.000
Sum		75,000	1.000	15.000

- 의할 점은, 해당 IP를 방어할 수 있는 안전 메커니즘이 실제로 있더라도 이를 무시해야 한다.
- 13) Fault Type: 고장의 형태를 영구결함 또는 일시적인 결함으로 분류한다. ‘P’(Permanent) 또는 ‘T’(Transient) 둘 중 하나 택일하여 기입한다.
 - 14) (Failure distribution for) Permanent faults: 영구적인 결함에 대한 고장모드 분포율을 할당한다.
 - 15) (Failure distribution for) Transient faults: 일시적인 결함에 대한 고장모드 분포율을 할당한다.
 - 16) Failure rate (FIT): 식별된 IP에 대한 고장 모드별로 고장률을 계산한다.
 - a. 13) Fault Type이 ‘P’일 경우: IP 영구적인 고장률 × 영구적인 고장 모드 분포율
 - b. 13) Fault Type이 ‘T’일 경우: IP 일시적인 고장률 × 일시적인 고장 모드 분포율
 - 17) Amount of Safe Faults: IP 고장 모드별로 안전 결함(Safe Fault)의 비율을 반영한다.
 - 18) Failure mode that has the potential to violate the safety requirement in absence of safety mechanisms? (SPF?): IP에 대한 고장 모드별로 안전 메커니즘이 부재 시 단일점 결함을 초래하는지 판단한다. 주의할 점으로 해당 IP를 방어할 수 있는 안전 메커니즘이 실제로 있더라도 이를 무시해야 한다.
 - 19) Safety Mechanism(s) preventing the violation of the safety requirement: 18)번에서 ‘Y’를 선택한 경우, 이를 방지할 수 있는 안전 메커니즘이 있다면 안전메커니즘의 ID를 기입한다. 만약 ‘N’을 선택했다면, 공란으로 비워 둔다.
 - 20) Failure mode coverage with respect to violation of safety requirement: 19)번에 적용된 안전 메커니즘의 진단 커버리지 값을 기입한다. 만약 19)번에 적용된 안전 메커니즘이 없다면 공란으로 비워 둔다.
 - 21) Residual or Single point fault failure rate / FIT: 단일점 결함(Single point fault) 또는 잔존 결함(Residual fault)의 고장률을 자동으로 계산한다.
 - 22) Failure mode that may lead to the violation of safety goal in combination with an independent failure of another component? (MPF?): 다른 독립적인 결함과 결합하여 안전목표(안전요구사항)을 위배하는 결함인지를 판단한다.
 - 23) Safety mechanism(s) to prevent latent faults: 22)번에서 ‘Y’를 선택한 경우, 이를 방지할 수 있는 안전 메커니즘이 있다면 안전메커니즘의 ID를 기입한다. 만약 ‘N’을 선택했다면, 공란으로 비워 둔다.
 - 24) Failure mode coverage with respect to latent failures: 23)번에 적용된 안전 메커니즘의 진단 커버리지 값을 기입한다. 만약 23)번에 적용된 안전 메커니즘이 없다면 공란으로 비워 둔다.
 - 25) Latent multiple point fault failure rate / FIT: 22)번이 ‘Y’라면, 다중점 잠재 결함률(Latent Failure Rate)을 자동으로 계산한다.
 - 26) Detected dual point faults failure rate / FIT: 22)번이 ‘Y’라면, 감지된 이중점 결함률(Detected dual point faults failure rate)을 자동으로 계산한다.
 - 27) Total Permanent Failure Rate: 영구적인 고장률에 대한 총 합계 값이다.
 - 28) Total safety related permanent failure rate: 안전 관련 고장률 중에서 영구적인 고장률에 대한 총 합계 값이다.
 - 29) Total transient failure rate: 일시적인 고장률에 대한 총 합계 값이다.
 - 30) Total Safety Related Transient Failure Rate: 안전 관련 고장률 중에서 일시적인 고장률에 대한 총 합계 값이다.
 - 31) Sum of permanent single or residual faults: 영구적인 고장률 중에서 단일점 결함률과 잔존 결함률을 합산한 값이다.
 - 32) Sum of transient single or residual faults: 일시적인 고장률 중에서 단일점 결함률과 잔존 결함률을 합산한 값이다.
 - 33) Sum of permanent latent faults: 영구적인 고장률 중에서 잠재 결함률의 총 합계 값이다.
 - 34) Sum of transient latent faults: 일시적인 고장률 중에서 잠재 결함률의 총 합계 값이다.
 - 35) Sum of permanent detected dual point faults: 영구적인 고장률 중에서 감지된 이중점 결함률을 합산한 값이다.
 - 36) Sum of transient detected dual point faults: 일시적인 고장률 중에서 감지된 이중점 결함률을 합산한 값이다.
 - 37) Sum of permanent safe faults: 영구적인 고장률에서의 안전측 결함의 총합이다.
 - 38) Sum of transient safe faults: 일시적인 고장률에서의 안전측 결함의 총합이다.

3.8 FMEDA Results summary

아래 Table 7은 ‘3.7 FMEDA 분석’의 결과를 보여주는 예시이다. Permanent faults(영구적인 결함)와 Transient faults(일시적인 결함)에 대한 각 항목별 계산 결과 값을 확인할 수 있다. 계산 결과에 따라 분석 대상 반도체의 정량적 목표 값 만족 여부를 판단한다.

Table 7 Example of semiconductor level FMEA results

FMEA Results for Semiconductor	Expressions	Permanent Faults (Hard Error)	Transient Faults (Soft Error)
Total Failure Rate (Safe Related)	λ	7.09E+01 FIT	1.02E+01 FIT
Safe Faults	λ_s	1.77E+01 FIT	0.00E+00 FIT
Single Point and Residual Faults	$\lambda_{SPF} + \lambda_{RF}$	7.08E+00 FIT	1.02E-02 FIT
Detected Dual Point Faults	λ_{DPFD}	2.73E+01 FIT	6.13E+00 FIT
Latent Dual Point Faults	λ_{DFPL}	1.88E+01 FIT	4.09E+00 FIT
Total Dual Point Faults	λ_{DPF}	4.61E+01 FIT	1.02E+01 FIT
Single Point Fault Metric	$SPFM = 1 - (\lambda_{SPF} + \lambda_{RF}) / \lambda$	90.01%	99.90%
Latent Fault Metric	$LFM = 1 - \lambda_{DFPL} / (\lambda - \lambda_{RF} - \lambda_{SPF})$	70.46%	60.00%
Lifetime		10000 h	10000 h
PMHF	$\lambda_{SPF} + \lambda_{RF} + \lambda_{DPF} \times \lambda_{DFPL} \times T_{Lifetime}$	7.09E+00 FIT	1.06E-02 FIT

4. 결론

기능안전 ISO 26262:2018에서 요구되는 설계 기법 및 절차들은 기존 반도체 산업에 있어 상당히 낮은 것이 현실이다. 이 중에서도 특히 정량적 평가의 경우가 더욱 그러한데, 불행히도 반도체 수준의 정량적 평가와 관련하여 참고할 만한 문서는 더욱 찾아보기 힘들다. 이에 본문에서는 정량적 평가에서 사용되는 FMEA 기법을 반도체 수준에 맞춰 소개하였고, 이에 대한 작성 절차를 제시하였다. 제시된 반도체 수준의 FMEA 작성 방안을 참고한다면, 기능안전 ISO 26262-5:2018⁴⁾에서 요구되는 정량적 평가 수행을 반도체 수준에 맞춰 진행할 수 있을 것으로 기대한다.

후 기

본 문에서는 반도체 수준의 FMEA 작성 방안 및 절차를 소개하였으나, 정작 반도체 Die와 Package에 대한 FMEA 분석 내용은 보여주지 못했다. 그렇기 때문에 향후 과제로서 실무에 적용할 수 있는 반도체 FMEA 분석 사례에 대한 연구가 필요해 보인다.

References

- 1) U. S. Department of Transportation, NHTSA (National Highway Traffic Safety Administration), A Framework for Automated Driving System Testable Cases and Scenarios, September 2018.
- 2) ISO 26262-11:2018, Road Vehicles Functional Safety Part 11: Guidelines on Application of ISO

- 26262 to Semiconductors, 2nd Edn., 2018.
- 3) ISO 26262-4:2018, Road Vehicles Functional Safety Part 4: Product Development at the System Level, 2nd Edn., 2018.
- 4) ISO 26262-5:2018, Road Vehicles Functional Safety Part 5: Product Development at the Hardware Level, 2nd Edn., 2018.
- 5) ISO 26262-6:2018, Road Vehicles Functional Safety Part 6: Product Development at the Software Level, 2nd Edn., 2018.
- 6) International Electrotechnical Commission, IEC TR 62380 Edition 1.0: Reliability Data Handbook - Universal Model for Reliability Prediction of Electronics Components, PCBs and Equipment, IEC, 2004.
- 7) ISO 26262-10:2011, Road Vehicles Functional Safety Part 10: Guideline on ISO 26262, 1st Edn., 2011.
- 8) ISO 26262-10:2018, Road Vehicles Functional Safety Part 10: Guideline on ISO 26262, 2nd Edn., 2018.
- 9) KS R ISO 26262:2011, Road Vehicles - Functional Safety - Part 1: Vocabulary, 2012.
- 10) B. K. Park and S. H. Lee, "The Methods for Describe the Safety Mechanism and Estimate the Diagnostic Coverage in order to Conduct the Efficient FMEA," Transactions of KSAE, Vol.26, pp.791-798, 2018.
- 11) IEC 61709, Electronic Components - Reliability - Reference Conditions for Failure Rates and Stress Models for Conversion, Edition 3.0, 2017.02.
- 12) FIDES Guide 2009 Edition A, Reliability Methodology for Electronic Systems, 2010.
- 13) B. K. Park and S. H. Lee, "The Method for Estimate of Basic Failure Rate and Derivation of Failure Mode and Failure Mode Distribution Rate in order to Evaluate of Random Hardware Failure," Transactions of KSAE, Vol.28, No.8, pp.551-561, 2020.
- 14) JEDEC JESD89A, Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices, 2006.