**하드웨어 안전 분석 지침서**

목차

[**1.** **ISO 26262 하드웨어 안전 분석 요구사항** 3](#_Toc378328231)

[**1.1.** **하드웨어 설계에 대한 안전 분석** 3](#_Toc378328232)

[**1.2.** **하드웨어 아키텍처 메트릭** 3](#_Toc378328233)

[**1.3.** **하드웨어 우발고장으로 인한 안전목표 위배평가** 4](#_Toc378328234)

[**1.4.** **종속 결함 분석** 4](#_Toc378328235)

[**2.** **하드웨어 안전 분석 방법** 4](#_Toc378328236)

[**2.1.** **하드웨어 설계에 대한 안전 분석** 4](#_Toc378328237)

[**2.2.** **하드웨어 아키텍처 메트릭 분석** 8](#_Toc378328238)

[**2.3.** **하드웨어 우발 결함으로 인한 안전 목표 위배 가능성 평가** 17](#_Toc378328239)

[**2.4.** **종속고장 분석** 19](#_Toc378328240)

1. **ISO 26262 하드웨어 안전 분석 요구사항**

ISO 26262에서 하드웨어와 관련된 안전 분석 요구하는 사항은 다음과 같다.

* ISO 26262-5:2011의 7.3절에 따른 **하드웨어 설계에 대한 안전 분석**
* ISO 26262-5:2011의 8절에 따른 **하드웨어 아키텍처 메트릭**
* ISO 26262-5:2011의 9절에 따른 **하드웨어 우발 결함으로 인한 안전 목표 위배 가능성 평가**
* ISO 26262-9:2011의 7절에 따른 **종속 결함 분석**
  1. **하드웨어 설계에 대한 안전 분석**

ISO 26262-5:2011의 7.3절에 따라 고장의 원인과 결함의 영향을 식별하기 위해 하드웨어 설계에 대한 안전 분석을 목적으로 한다. 고장의 원인과 결함의 영향을 식별하기 위해 하드웨어 설계에 대한 안전 분석은 **표 2**와 **KS R ISO 26262-9**, **8절**에 따라 적용되어야 한다. 하드웨어 설계 안전 분석은 정량적인 안전 분석과 결합하여 수행할 수 있다.

표 2 ― 하드웨어 설계 안전 분석

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **방법** | | **ASIL** | | | |
| **A** | **B** | **C** | **D** |
| 1 | 연역적 분석a | 0 | + | ++ | ++ |
| 2 | 귀납적 분석b | ++ | ++ | ++ | ++ |
| 분석의 상세 수준은 설계의 상세 수준에 비례한다. 특정한 경우에 두 가지 방법이 다른 상세 수준에서 수행될 수 있다. | | | | | |
| a 일반적인 연역적 분석 방법은 FTA이다.  b 일반적인 귀납적 분석 방법은 FMEA이다. | | | | | |

* 1. **하드웨어 아키텍처 메트릭**

ISO 26262-5:2011의 8에 따라 안전목표에 대해 구현된 안전메커니즘의 효과성을 분석해야 한다.

하드웨어 우발고장에 대처하기 위한 아이템의 아키텍처의 효과성을 평가하는 두 가지 하드웨어 아키텍처 메트릭을 기술하고 있다. 이 메트릭 및 관련된 목표 값은 아이템의 전체 하드웨어에 적용되고 9절에 기술된 하드웨어의 우발 고장으로 인한 안전 목표 위배에 대한 평가를 보완하는데 사용된다.

이 메트릭에서 지시하는 하드웨어의 우발고장은 일부 아이템의 안전관련 전기/전자 하드웨어 소자, 즉 안전 목표의 위배를 크게 야기할 수 있는 소자와 이러한 소자들의 단일점 결함, 잔존 결함 또는 잠재 결함으로 제한한다. 전기 기계(electromechanical)의 하드웨어 부품에 대해서는, 단지 전기적인 고장 형태와 고장율만을 고려한다.

하드웨어 아키텍처 메트릭은 하드웨어 아키텍처 설계와 하드웨어 상세 설계 동안 반복적으로 적용될 수 있다.

하드웨어 아키텍처 메트릭은 아이템의 전체 하드웨어에 의존적이다. 하드웨어 아키텍처 메트릭에 대해 규정된 목표 값에 대한 부합은 아이템에 포함된 각 안전 목표에 대해 달성된다.

* 1. **하드웨어 우발고장으로 인한 안전목표 위배평가**

본 추정은 ISO 26262-5:2011의 9절에 따라 하드웨어 우발 결함으로 인한 안전 목표 위배 가능성을 분석해야 한다.

안전 목표 위배에 대한 잔존 리스크가 충분히 낮은지를 평가하기 위해 두 가지 대안 방법이 제안된다.

두 가지 방법은 단일점 결함, 잔존 결함, 개연성(plausibiliby)이 있는 이중점 결함으로 인한 안전 목표 위배의 잔존 리스크를 평가한다. 안전 개념과 관련된 것으로 판단된 경우, 다중점 결함도 물론 고려될 수 있다. 이 분석에서 잔존 및 이중점 결함에 대한 안전 메커니즘의 커버리지가 고려되며, 이중점 결함에 대한 노출 기간 역시 고려된다.

첫 번째 방법은, 고려하고 있는 안전 목표에 대한 위배 가능성을 평가 하기 위해, 예를 들면, 정량적 FTA와 이 정량화된 결과를 목표 값과 비교하는 것과 같은, “우발 하드웨어 고장에 대한 확률 메트릭”(PMHF) 라고 불리는 확률 메트릭의 사용으로 구성된다.

두 번째 방법은, 고려하고 있는 안전 목표에 대한 위배를 일으킬 수 있는, 각 잔존 결함, 단일점 결함 및 이중점 결함에 대한 개별적인 평가로 구성된다. 이 분석 방법 또한 컷셋(cut-set) 분석으로 여겨 질 수 있다.

* 1. **종속 결함 분석**

ISO 26262-9:2011의 7절에 따라 요구된 독립성 또는 주어진 엘리먼트 간에 간섭에 대한 자유성을 간과 또는 무효화 시킬 수 있거나 안전 요구사항이나 안전 목표를 위배할 수 있는 단일 사건 또는 단독 원인을 식별하는 것을 목적으로 한다

1. **하드웨어 안전 분석 방법**
   1. **하드웨어 설계에 대한 안전 분석**
      1. FMEA 분석

상세 설계된 Part 수준에서 FMEA를 수행한다. FMEA 수행에 관련된 일반적인 사항은 차량 FMEA 표준인J1739 또는 일반적인 FMEA 가이드를 참고한다. 단 하드웨어 상세 설계를 기반으로 하드웨어 컴포넌트/파트 수준에서 수행한다. ASIL 등급이 A, (B)인 경우 정성적인 분석만 수행하고 ASIL 등급이 (B), C, D인 경우는 FMEA 분석은 HAM 분석과 결합하여 수행한다. 정성적인 분석인 경우 따로 RPN 값을 산정할 필요는 없다. FMEA 양식과 예시는 부록을 참고한다.

* + 1. FTA 분석

부여된 ASIL이 C,D인 경우, Deductive analysis 방법인 FTA 분석을 추가적으로 실시 한다.

■ Top event 선정

• System의 safety goal, 기능 및 성능상의 최상위 설계 목표를 top event로 선정

• [작성 예]

|  |  |
| --- | --- |
| Top event group | Top event |
| Safety goal | Unintended acceleration  Loss of ability to brake  Unintended vehicle movement when vehicle start requested |

■ Basic event 제한

• Hardware architecture 상 표기된 Hardware block 수준까지 구조적인 관점까지 수행. (해당 Block의 세부 component/part 대한 식별은 수행하지 않음, HAM 결과로 대체함)

■ Top event로 부터 Basic event까지의 derivation 방법 (FTA 수행 방법은 IEC 61025 또는 일반적인 FTA 가이드 문서를 참고한다.)

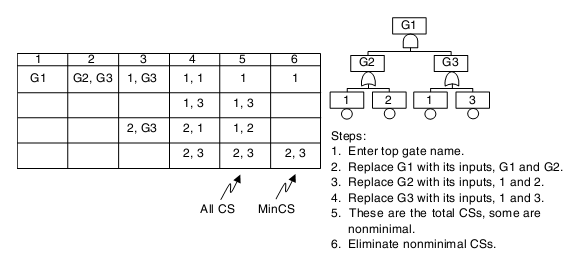
• Step1: top event에서부터 hardware architecture block을 기준으로 fault tree 전개

• Step2: gate(OR gate, AND gate, PRIORITY gate, NOT gate 등)를 고려하여 hardware architecture block 수준까지 fault tree 전개

• Step3: Cut-set analysis를 통한 설계 개선, architecture 상 기능적 dependencies 파악, PMHF 값 산출 등의 분석 수행

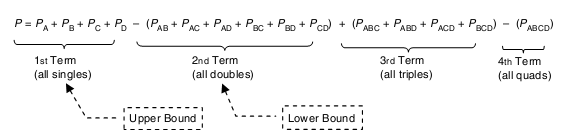
참고) MOCUS Algorithm (Cut-set analysis 방법)

AND 게이트는 어떤 CS의 엘리먼트 개수를 증가 시키고, OR 게이트는 CS의 개수를 증가 하는 원리를 이용한 minimal cut-set 생성



<MOCUS Algorithm을 이용한 Cut-set analysis>

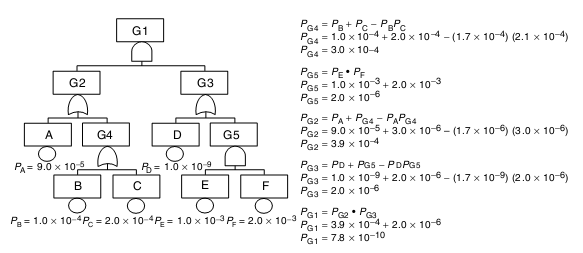
참고) OR gate expansion을 사용하여 모든 Cut-set의 합을 통해 PMHF 값을 산출 할 수 있다. 여기서 Px는 각 cut-set이 가지는 확률



<OR gate expansion formula>

참고) Bottom-up gate-to-gate calculation PMHF 값 산출

Fault Tree의 Bottom에서 시작하여 단계적으로 Tree를 타고 올라가면서 계산



<Bottom-up gate to gate calculation 예제>

* + 1. FTA 예시

|  |
| --- |
| <Functional Block Diagram 예>    <Fault Tree Analysis 전개 예> |

* 1. **하드웨어 아키텍처 메트릭 분석**
     1. 수행 방법

**■ 1단계: HAM의 목표 값 설정**

- SPFM 목표 값 산정 기준 (part5-8.4.5 참조)

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASIL B | ASIL C | ASIL D |
| SPFM | ≥ 90% | ≥ 97% | ≥ 99% |

(cf. well-trusted design principle에 따른 목표 값 산정은 feasibility에서 문제가 있을 수 있기 때문에 본 문서에서 다루지 않음)

- LFM 목표 값 산정 기준

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASIL B | ASIL C | ASIL D |
| LFM | ≥ 60% | ≥ 80% | ≥ 90% |

(cf. well-trusted design principle에 따른 목표 값 산정 또는 detection 기반 SM에 대한 DC을 이용한 목표 값 설정은 feasibility에서 문제가 있을 수 있거나 또는 evaluation 방법이 동일 할 수 있기 때문에 본 문서에서 다루지 않음)

**■ 2단계: Part별 “Safety-related” 여부 판단**

- Schematic을 구성하는 parts list에 대해서 해당 part가 “safety –related”요소인지 아닌지의 여부를 판단한다.

1) “safety-related” 여부는 해당 part가 가지고 있는 어떤 failure mode에 빠지더라도 safety goal의 위배에 관련이 없는 경우에 해당 part는 “safety-related”하지 않는 것으로 간주한다. (part1의 “safety-related element” 정의 참조)

2) “non safety-related”로 판정된 part는 HAM evaluation에서 고려하지 않는다.

- [consideration]: 해당 part가 Item 또는 element 고유의 중요한 기능과 관련이 있더라도 해당 part의 failure mode가 safety goal 관점에서 관련이 없다면 HAM evaluation의 대상이 되지 않는다. 뿐만 아니라 안전에 도움을 주는 기능을 수행하지만 해당 part가 직접적으로 safety goal달성에 영향을 미치지 않는 경우에도 “non safety-related”로 판정 한다.

**■ 3단계: Part들의 기본 고장율, 고장 모드 및 고장 분포 산출**

- ISO-26262 part5 8.4.3.에 따라 다음 3가지 방법 중 1가지 방법을 이용하여 part들의 기본 고장율을 산출 한다.

1) “recognized industry source”: IEC TR 62380, IEC 61709, MIL HDBK 217 F, RAC HDBK 217 plus, UTE C80-811, NPRD95, EN50129 Annex C, EN62061 Annex D, RAC FMD 97, MIL HDBK 338 등

2) Field return 또는 시험 값에 기반한 통계 값 (적절한 수준의 신뢰도 확보가 요구됨)

3) Expert judgment (판단기준이 명시되어야 함)

- 고장율 모델 선정 시 참고사항

1) IEC TR 62380: 유럽에서 많이 쓰이는 신뢰도 예측 모델 (주로 민수용으로 쓰이며 유럽 수출에는 필수적으로 알려짐)

2) MIL HDBK 217F: 군수용 신뢰도 예측모델임. 1994년도에 폐기된 표준이며 구형 표준이기 때문에 반도체와 같은 소자에는 잘 맞지 않으나 아직은 많이 쓰이고 있는 실정임. 217G로 대체될 예정

3) RAC HDBK 217 Plus: 사용법이 상당히 복잡함. MIL HDBK 217G에 의해서 대체될 예정임.

4) NPRD95: 신뢰도 예측 모델이 아닌 library (database)임. 따라서 모델보다 사용하기 쉬운 편임. NPRD 2011버전이 최신이며 “non-electronic, electromechanical”형식의 컴포넌트를 다룸

5) FMD97: 고장 유형 및 고장 분포를 다루고 있음 (고장율 모델이 아님)

6) 2개 이상의 고장율 모델을 혼합해 사용하는 경우 ISO-26262 요구사항에 따라 scaling factor 값을 결정해야 한다. (부적절한 bias를 방지)

**■ 4단계: SPFM의 도출**

1. Part의 해당 failure mode에 대한 SM이 설계되어 있지 않다고 가정한 상황에서 Safety goal을 위반하는지 여부를 판단한다. (실제 HW 설계에 SM이 구현되어 있더라도 배제한 상황에서 판단)

2. Safety goal을 위반 할 수 있다고 판단된 failure mode에 대해 SM이 구현되어 있는지 여부를 확인하고 구현되어 있다면 해당 SM의 failure mode coverage를 산출 한다. (산출 방법은 “부가설명” 참조) 만약 SM이 구현되지 않은 경우에는 이를 표기하고 failure mode coverage의 값은 0%로 표기한다.

3. ISO-26262 part5 annex C의 C.2.2의 정의에 따라 SPFM의 값을 산출 한다.

|  |  |
| --- | --- |
| SPFM의 계산 방법 |  |

**■ 5단계: LFM의 도출**

1. 2개 이상의 독립적인 failure mode가 동시 발생시 safety goal을 위반하는지 여부를 판단한다. (즉, 해당 failure mode가 MPF로 기능하는지 여부를 판단하는 것이다.)

2. Safety goal을 위반할 수 있다고 판단된 경우 이를 커버하기 위한 SM이 구현되어 있는지 여부를 확인하고 구현되어 있다면 해당 SM의 failure mode coverage를 산출 한다.

3. ISO-26262 part5 annex C의 C.3.2의 정의에 따라 LFM의 값을 산출 한다.

|  |  |
| --- | --- |
| LFM의 계산 방법 |  |

**■ 6 단계: HAM 목표 값 달성여부 확인 및 설계 수정**

- 4, 5단계에서 산출한 SPFM, LFM의 값이 1단계에서 산출한 HAM의 목표 값에 도달하였는지 확인하고 도달하지 않은 경우 SM을 추가하거나 또는 현재 설계된 SM의 failure mode coverage값을 높여서 HAM 목표값을 만족하도록 설계를 변경 한 후 4~6단계를 반복한다.

|  |  |  |  |
| --- | --- | --- | --- |
| Metric 이름 | 추정 값 | 목표 값(ASIL D) | 만족 여부 |
| SPFM (Single Point Faults Metric) | 99.345% | 99% 이상 | 만족 |
| LFM (Latent Faults Metric) | 99.300% | 90% 이상 | 만족 |

\*주의1: 산출 과정 및 산출 근거는 8절의 “첨부”를 참조하도록 한다.

\*주의2: ASIL decomposition 수행을 통해 ASIL이 변경 되더라도 HAM 및 PMFH 분석은 Safety goal 즉, ASIL decomposition 수행 전의 ASIL을 기준으로 한다.

* + 1. **하드웨어 아키텍처 메트릭 수행 예시**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 이 부속서는 아이템의 안전 목표에 대한 단일점 결함 메트릭과 잠재 결함 메트릭 계산의 예를 제공한다.  이 보기를 위한 시스템은 단일 ECU에 구현된 두 가지 기능을 실현한다.  **- 기능 1**은 한 개의 입력(센서 R3을 통해 측정된 온도)과 한 개의 출력(I71에 의해 제어되는 밸브 2)을 가지며, 온도가 90 ℃보다 높을 때 밸브 2를 여는 동작을 수행한다.  - I71을 흐르는 전류가 없으면 밸브 2가 열린다.  - 관련된 안전 목표 1은 “온도가 100 ℃보다 높을 때 밸브 2가 χms 보다 더 오랫동안 닫히지 않아야 한다”는 것이다. 안전 목표는 ASIL B로 할당된다. 안전 상태는 밸브 2가 열려있는 상태이다.  - 센서 R3의 값은 마이크로컨트롤러 ADC에 의해 읽혀진다. R3 저항은 온도가 상승함에 따라 줄어든다. 이 입력에 대한 모니터링은 없다. T71을 제어하는 출력단은 아날로그 입력 InADC1(표의 안전 메커니즘 SM1)에 의해 모니터링 된다. 이 보기에서는 안전 메커니즘 SM1이 안전 목표 위배와 관련하여 90 %의 진단 커버리지를 가지고 T71의 특정 고장형태를 검출할 수 있다고 가정한다. SM1에 의해 고장이 검출되면, 안전 상태가 활성화되겠지만 고장을 알리기 위해 켜지는 램프는 없다. 따라서 잠재 결함에 대한 진단 커버리지는 80 %로 한다(운전자가 데그러데이션(degradation)을 통해 고장을 인식할 것이다).  **- 기능 2**는 두 개의 입력(펄스를 생성하는 센서 I1과 I2를 통해 측정된 휠 속도)과 한 개의 출력(T61에 의해 제어되는 밸브 1)을 가지며, 차량 속도가 90 km/h 보다 높을 때 밸브 1을 여는 동작을 수행한다.  - T61을 흐르는 전류가 없으면 밸브 1이 열린다.  - 관련된 안전 목표 2는 “속도가 100 km/h다 높을 때 밸브 1이 Уms 보다 더 오랫동안 닫혀있지 않아야 한다”는 것이다. 안전 목표는 ASIL C로 할당된다. 안전 상태는 밸브 1이 열려있는 상태이다.  - 센서 I1과 I2 펄스 값은 마이크로컨트롤러에 의해 읽혀진다. 휠 속도는 센서에 의해 제공된 평균 값을 이용하여 계산된다. 안전 메커니즘 2(표의 안전 메커니즘 SM2)가 두 입력을 비교한다. 안전 메커니즘 SM2는 99 %의 진단 커버리지를 가지고 각 입력의 고장을 검출한다. 불일치의 경우 Out.1은 0으로 설정된다. 이것이 밸브 1을 열도록 한다(트랜지스터의 “0” 전압이 게이트를 연다. I61의 “0” 전압은 밸브 1을 연다). 따라서 안전 목표를 위배할 잠재성이 있는 결함의 99 %가 검출되고 안전 상태로 유도된다. 안전한 상태가 활성화 되면 램프 L1이 켜진다. 따라서 이러한 결함은 100 % 인지된다. 나머지 결함의 1 %는 잔존 결함으로 잠재 결함이 아니다.  - T61을 제어하는 출력단은 아날로그 입력 InADC2에 의해 모니터링 된다(표의 안전 메커니즘 SM3). 휠 속도는 센서에서 제공된 평균 값을 이용하여 계산된다.  - 마이크로컨트롤러는 내부 중복구현이 없다. 복잡한 부품의 안전측 결함 비율에 대한 자세한 정보가 없으면, 보수적으로 50 %의 안전측 결함 비율을 가정할 수 있다. 안전 목표 위배와 관련하여 내부 자체 시험과 워치독(표의 안전 메커니즘 SM4)을 통해 90 %의 전반적인 커버리지를 갖는 것으로 가정한다. 워치독은 마이크로컨트롤러의 출력 0을 통해 갱신(live) 신호를 받는다. 워치독이 더 이상 갱신되지 않을 때, 그 출력 신호의 값이 “low”상태가 된다. SM4(워치독과 마이크로컨트롤러 자체 시험)에 의해 결함이 검출된 경우, 두 기능을 안전 상태로 전환되고 L1이 켜진다. 따라서 잠재 결함에 대한 진단 커버리지는 100 %로 한다.  L1은 대시보드의 LED이며, 특정 비율로 검출 될 수 있는 다중점고장 검출 시 켜지며 운전자에게 기능 1의 안전 상태가(밸브 1 열림) 활성화되었다는 것을 알린다.   1. 하네스 고장은 이 보기에서 고려하지 않는다. 2. 제공된 전자 부품을 위해 사용되는 결함 모델은 부품 응용에 따라 다를 수 있다. 3. 저항기의 결함 모델은 하드웨어 부품이 디지털 입력(R11, R12, R13)이나 아날로그 입력(R3)중 어디에 사용되느냐에 따른다. 첫 번째 경우에서 결함 모델은 “개방/폐쇄”가 되고 두 번째 케이스에서는 “개발/폐쇄/드리프트”가 된다. 4. 첫 번째 메트릭은 안전 목표 위배를 막기 위한 안전 메커니즘의 고장형태 커버리지만 사용한다. 두 번째 메트릭은 잠재되어 있는 고장형태를 방지하기 위한 안전 메커니즘의 고장형태 커버리지만 사용한다. 5. R21의 고장모드 “개방”은 안전 메커니즘의 부재 시 안전 목표 2를 위배할 수 있는 잠재성을 갖는다. 안전 메커니즘 3은 99 %의 고장형태 커버리지로 이 고장형태를 검출하고 시스템을 안전 상태로 전환한다. 이 고장형태를 검출할 때 경고가 표시되며 따라서 잠재 고장에 대한 고장형태 커버리지는 100 %이다. 6. 이 보기에서는 하드웨어 엘리먼트의 고장형태 분포에 대한 가정을 감안하였다. 논의되거나 언급된 특별한 고장형태의 분포가 없는 경우 동일한 분포를 가지는 것으로 가정한다.   다음 표에서 하드웨어 엘리먼트의 특정 고장형태에 대한 안전 메커니즘에 의해 산출된 커버리지를 “고장형태 커버리지”라고 하는 것에 주의해야 한다.       |  |  |  |  | | --- | --- | --- | --- | |  | **ASIL B** | **ASIL C** | **ASIL D** | | 단일점 결함 메트릭 | ≥ 90 % | ≥ 97 % | ≥ 99 % | | 잠재 결함 메트릭 | ≥ 60 % | ≥ 80 % | ≥ 90 % |   안전 목표 1은 ASIL B로 할당되며 ≥ 90 %의 단일점 결함 메트릭 권장 값을 갖고, ≥ 60 %의 잠재 결함 메트릭 권장 값을 갖는다. 단일점 결함 메트릭 권장 값은 93.2 %로 계산된 메트릭 값으로 만족되었고 잠재 결함 메트릭 권장 값은 90 %의 값으로 만족되었다.   1. R3과 R13의 고장형태 ”개방”과 R23의 “폐쇄”는 단일점 결함이다. 이 결함은 직접 안전 목표 위배를 초래하며 이 하드웨어 부품의 결함을 다룰 수 있는 안전 메커니즘은 없다. 2. 이 하드웨어 부품의 목적은 전기적 보호이다. 폐쇄 고장형태는 전기적 보호 기능의 상실을 의미한다. 3. 이 하드웨어 부품의 목적은 ESD 보호이다. 개방 고장형태는 ESD 보호 기능의 상실을 의미한다. 4. 이 하드웨어 부품의 목적은 전기적 보호이다. 하나의 고장형태는 전기적 보호의 손실이다. 나머지 모드는 안전 메커니즘 부재 시 안전 목표를 위배할 잠재성을 갖는다. 5. 안전 목표 위배를 초래할 잠재성이 크지 않는 고장을 가지는 엘리먼트는 계산에서 고려하지 않는다. 여기서 L1과 R81은 잠재적인 이중결함을 방지하기 위한 안전 메커니즘을 구현하는 엘리먼트다. n > 2의 다중점 결함은 안전측 결함으로 간주된다. 6. 안전 목표 위배를 직접적으로 초래하는 결함(단일점 결함이나 잔존 결함)은 잠재 결함 부분에 더 이상 해당되지 않는다. 따라서 예들 들면, T71의 “닫힌 게이트” 잠재 고장형태의 고장율은 다음과 같이 계산된다.     ESD나 전기적 보호의 손실을 초래하는 고장형태의 분류는 사례 별 분석을 기반으로 하며 ESD나 전기적 스트레스의 유사도와 안전 목표에 대한 ESD나 전기적 스트레스의 특성 효과를 고려한다. 예들 들면, ESD 발생이 차량 수명 동안 발생하기 쉬우며 그 영향에 대한 보호 조치가 없을 때 안전 목표의 위배를 초래할 수 있는 경우, 보호 손실을 가져오는 고장형태는 단일점 결함으로 분류된다. 이 부속서는 메트릭 내에서 이러한 사례들을 어떻게 다루는 지에 대한 보기이다. 실제로 ESD나 전자기 방해 스트레스는 이 보기와 유사한 형태의 전형적인 설계에 영향을 미치지 않는다.    안전 목표 2는 ASIL C로 할당되며 **표 4**가 사용되는 경우 ≥ 97 %의 단일점 결함 메트릭이 권장되고, **표 5**가 사용되는 경우 ≥ 80 %의 잠재 결함 메트릭이 권장된다. 단일점 결함 메트릭 요구사항은 96.5 %로 계산된 메트릭으로 인해 충족되지 않았으며, 잠재 결함 메트릭 권장 값은 91.6 %로 충족되었다.   1. 이 하드웨어 부품의 목적은 전기적 보호이다. 하나의 고장형태는 전기적 보호의 손실이다. 나머지 모드는 안전 메커니즘의 부재 시 안전 목표를 위배할 가능성이 있다. 2. 두 고장형태는 두 사례 모두에서 안전 메커니즘의 부재 시 안전 목표를 위배할 가능성이 있으며, 속도 펄스가 전송되지 않는다. 이로써 잘못된 속도를 얻게 한다. 센서는 개방 콜렉터(open-collector) 형식이다. 3. 이 하드웨어 부품의 목적은 전기적 보호이다. 폐쇄 고장형태는 보호 기능의 상실을 의미한다. 4. 이 하드웨어 부품의 목적은 ESD 보호이다. 개방 고장형태는 보호 기능의 상실을 의미한다. 5. 안전 목표 위배를 초래할 가능성이 크지 않는 고장형태를 갖는 엘리먼트는 계산에서 고려되지 않는다. 여기서 L1과 R81은 잠재 중인 이중결함을 방지하기 위한 안전 메커니즘을 구현하는 엘리먼트다. n>2의 다중점 결함은 안전측 결함으로 간주된다. 6. ESD나 전기적 보호의 손실을 초래하는 고장형태의 분류는 사례 별 분석을 기반으로 하며 ESD나 전기적 스트레스의 유사도와 안전 목표에 대한 ESD나 전기적 스트레스의 특성 효과를 고려한다. 예들 들면, ESD 발생이 차량 수명 동안 발생하기 쉬우며 그 영향에 대한 보호 조치가 없을 때 안전 목표의 위배를 초래할 수 있는 경우, 보호 손실을 가져오는 고장형태는 단일점 결함으로 분류된다. 이 부속서는 메트릭 내에서 이러한 사례들을 어떻게 다루는 지에 대한 보기이다. 실제로 ESD나 전자기 방해 스트레스는 이 보기와 유사한 형태의 전형적인 설계에 영향을 미치지 않는다. 또한 여기에서는 이 고장형태들이 마이크로컨트롤러에 일부 손상을 가져올 수 있더라도 이 고장형태들을 SM4가 처리한다고 보지 않는다.   전기적 보호 기능의 상실은 잘못된 입력값을 초래하며 이는 SM2에 의해 검출되므로 잠재되지 않는다. |

* 1. **하드웨어 우발 결함으로 인한 안전 목표 위배 가능성 평가**
     1. 추정 방법
     2. PMHF 값 산출

PMHF 값 산출은 다음의 방법 중 하나를 선택하면 된다.

1) PMHF의 값은  로 표현될 수 있으며 이 값이 위의 table 6를 만족하면 된다. 이때 의 값은 SPFM 산출 과정에서 자동으로 구해지며 값은 LFM 산출 과정에서 구해진다.

2) ISO 26262-10, 8.3.3절에서 제시한 아래 식을 이용하여 산출 가능하다.



는 하드웨어 우발 고장에 대한 확률적 메트릭 값이다.(PMHF)

는 의도된 기능의 잔존 고장률이다.(미션 블록 "m")

은 미션 블록 "m"의 이중점 고장률이다.

은 차량의 수명(lifetime)이다

은 안전 메커니즘 "sm"의 잠재된 이중점 고장률이다.

은 안전 메커니즘 "sm"의 검출된 이중점 고장률이다.

는 안전 메커니즘 "sm"의 다중점 결함 검출 간격이다.

만약  안에 대응되는 안전 메커니즘의 고장과 결합하여 미션이 고장 날 확률을 나타내는 이 매우 작으면[즉, 만약 이 대략(in the order of) 한번의 운전 사이클이면(이 예시에서== 1000 FIT 기여 )], 계산식을 다음과 같이 간단히 하여 무시할 수 있다.



만약 조건적인 확률이 적용되지 않는다면, 예를 들어, 고장률의 차수가 상관없다면, 계산식은 다음과 같이 바뀐다.



3) 정량적 FTA를 통해 산출 가능하다. 정량적 FTA에 산출 방식은 관련 표준 (2.1.3절 참고)

단 ISO 26262 part5 9.4.2.1 ~ 9.4.2.7의 요구사항에 따라 다음과 같은 항목을 추가적으로 확인해야 한다.

1. HW 설계에 사용된 부품들이 “expected system life time”을 만족하는지 확인

- Expected system life time은 과거 유사한 item의 사용 이력 (usage profile)이나 또는 system 요구사항에 표기된 내구성 관련 요구사항 등을 이용해서 결정 할 수 있다.

2. SPF를 내포하는 part의 경우 해당 part가 “dedicated measure”에 의해 failure rate이 검증된 경우에만 사용 될 수 있다.

- Dedicated measure

1) Design feature (동작 조건 보다 높은 사양(ex. stress rating)의 부품 사용 또는 PCB의 contact space 조절 과 같은 물리적인 분리)

2) Special sample test (부품 내구성 확인을 위한 샘플링 테스트)

3) Burn-in test (시험을 통해 부품의 수명을 확인)

4) Control plan에 따른 dedicated control set (부품 제조 과정에서 내구성을 위해 특별히 제어되는 공정에서 생산된 부품을 사용)

5) 부품에 안전관련 특정 요구사항을 부여하고 해당 요구사항을 만족하는 부품을 사용

* + 1. 추정 예시

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 다음의 경우 PMHF 분석을 수행하면 다음과 같다.   |  |  | | --- | --- | | 구분 | Value | |  | 0 FIT | |  | 2.154 FIT | |  | 189.926 FIT | |  | 2.285 FIT | |  | 100000 hour |   주1) 은 IEC 62380 mission profile의 차량운행 시간 500h/1 year에 20년을 곱한 값으로 산정  1) 방식  = 4.439 FIT  2) 방식  = 2.197 FIT |

* 1. **종속고장 분석**

본 분석은 ISO 26262-9:2011의 7절에 따라 요구된 독립성 또는 주어진 엘리먼트 간에 간섭에 대한 자유성을 간과 또는 무효화 시킬 수 있거나 안전 요구사항이나 안전 목표를 위배할 수 있는 단일 사건 또는 단독 원인을 식별하는 것을 목적으로 한다

* + 1. **종속고장 분석 방법**

잠재된 종속 고장은 하드웨어 아키텍처의 특징을 고려하여 아래의 check list를 기반으로 식별한다.

(아래 checklist만으로 완전한 깃이 아니고 아키텍처의 특징을 따라 추가적인 잠재된 종속 고장이 고려될 수 있다.)

■ checklist for dependent failure

|  |  |  |  |
| --- | --- | --- | --- |
| Dependent Failure | Category | Sub-category | Description |
| CCF | design dependencies (coupling mechanism) | Same/similar design |  |
| Same/similar component |  |
| Same/similar interface |  |
| proximity(element간 근접정도) |  |
| common block (clock, test logic, voltage regulators) |  |
| common external source (power supply, input data, inter-system data bus and communication) |  |
| environmental factors shared cause(root cause) | temperature(heat) |  |
| vibration |  |
| pressure |  |
| humidity/condensation(moisture) |  |
| pollution |  |
| corrosion |  |
| contamination |  |
| EMC |  |
| human error(process) | staff |  |
| procedures(ex. faulty test procedure) |  |
| specification |  |
| CF | design dependencies | Function dependency(FTA 결과 참고) |  |
| Signal/data flow |  |
| non-safety 기능과의 간섭 여부 |  |

* + 1. 종속고장 분석 예시
    2. Common cause failure

|  |  |
| --- | --- |
| CCF 원인 | 분석 결과 및 대책 |
| Homogeneous redundancy  (APPS) | APPS1과 APPS2에서 동일 IC를 사용하지만 출력신호 기울기를 다르게 설정하여 출력 시, 서로 상이한 신호가 입력됨. 따라서 IC의 동질성으로 인한 리스크에 내성을 갖는다고 볼 수 있음. |
| Shared resource  (power) | 전원공급 경로가 분리되어 있기 때문에 전원에 대한 의존성이 없음 |
| H/W component placement | H/W 소자 및 컴포넌트의 배치는 서로간의 간섭이 발생하지 않는 범위에서 “PCB Layout 가이드”에 따라 설계되었으며 기능 시험 및 신뢰성 시험을 통해 컴포넌트간의 간섭여부를 확인함. |
| Environmental conditions  (Temp. / Humidity / Vibration / Water / Etc) | 온도/습도/충격/결로/진동과 같은 운용환경에 기인한 CCF 요소는 환경시험을 통해 기본적인 검증이 수행된 것으로 판단됨. |

* + 1. Cascading failure

|  |  |
| --- | --- |
| CF 원인 | 분석 결과 |
| Function dependency | APPS1과 APPS2 센서간 공유하고 있는 H/W 자원은 없으며 각 채널을 구성하는 IC 및 인터페이스 회로가 전자회로 관점에서 서로 분리되어 있기 때문에 채널간 기능적인 의존관계는 없음 |
| Signal/data flow | 각 센서 채널을 통해 센서-인터페이스-제어기로 신호 흐름이 존재하나 센서 채널의 redundancy 구현을 통해 보완 |

1. **부록**

