**3.1 Simulation Tool 등 정보 전부 붙여넣기**

하드웨어 요구사항 명세서

Hardware Requirements Specification

|  |  |  |  |
| --- | --- | --- | --- |
| 차종/프로젝트코드 | A-PUZL39 | | |
| 차종/프로젝트명 | Platform IP A-PUZL39 | | |
| 결재 정보 | 작성 | 검토 | 승인 |
| 김희조  Safety  Manager | 이광호  수석 | 이영곤  대표 |

문서 ID : Puzl39-HWE-T01

문서 상태: Release

배포 날짜: 2024. 01. 19

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **문서 수정 이력** | | | | | |
| **일자** | **버전** | **편집자** | **Chap** | **수정내용** | **승인** |
| 2023.12.12 | D1 | 김희조 | 1, 2 | 문서 작성 시작 |  |
| 2023.12.15 | D2 | 김희조 | 2 | Architecture revised |  |
| 2023.12.18 | D3 | 이광호 | 3 | Fill in Hardware safety requirements |  |
| 2023.12.19 | D4 | 김희조 | 3 | Review & Revise |  |
| 2024.01.09 | D5 | 김희조 | 3 | Diagram added |  |
| 2024.01.11 | D6 | 김희조 | All | 동료검토 후 수정 |  |
| 2024.01.19 | R1 | 김희조 | All | 1차 Release |  |

**목 차**

[1. 문서 개요 5](#_Toc156549818)

[1.1. 문서 목적 5](#_Toc156549819)

[1.2. 적용 범위 5](#_Toc156549820)

[1.3. 약어, 용어 설명 (식별자 부여 규칙 포함) 6](#_Toc156549821)

[1.4. 참조문서 6](#_Toc156549822)

[2. 하드웨어 기능 요구사항 (Hardware function requirements) 7](#_Toc156549823)

[2.1. HFR\_IP\_001 CPU feature 7](#_Toc156549824)

[2.2. HFR\_IP\_002 IP feature 8](#_Toc156549825)

[2.3. HFR\_IP\_003 Internal memory feature 9](#_Toc156549826)

[2.4. HFR\_IP\_004 External Interface feature 9](#_Toc156549827)

[3. 하드웨어 안전요구사항 (Hardware safety requirements) 11](#_Toc156549828)

[3.1. HSR\_IP\_001 Window watchdog << High Priority 여부 검토 11](#_Toc156549829)

[3.2. HSR\_IP\_002 External Window watchdog 13](#_Toc156549830)

[3.3. HSR\_IP\_003 Bus data parity check 15](#_Toc156549831)

[3.4. HSR\_IP\_004 Cache Memory ECC 16](#_Toc156549832)

[3.5. HSR\_IP\_005 I2C ACK/NACK check 18](#_Toc156549833)

[3.6. HSR\_IP\_006 I2C discard data 20](#_Toc156549834)

[3.7. HSR\_IP\_007 External I2C discard data 21](#_Toc156549835)

[3.8. HSR\_IP\_008 SPI discard data 22](#_Toc156549836)

[3.9. HSR\_IP\_009 External SPI discard data 24](#_Toc156549837)

[3.10. HSR\_IP\_010 LIN checksum check 26](#_Toc156549838)

[3.11. HSR\_IP\_011 External LIN checksum check 27](#_Toc156549839)

[3.12. HSR\_IP\_012 External LIN discard data 29](#_Toc156549840)

[3.13. HSR\_IP\_013 LIN parity check 31](#_Toc156549841)

[3.14. HSR\_IP\_014 UART discard data 32](#_Toc156549842)

[3.15. HSR\_IP\_015 External UART discard data 34](#_Toc156549843)

[3.16. HSR\_IP\_016 UART parity check 35](#_Toc156549844)

[3.17. HSR\_IP\_017 SRAM ECC 37](#_Toc156549845)

[4. 하드웨어 비기능 요구사항 (Hardware non-function requirements) 39](#_Toc156549846)

[4.1. HNFR\_IP\_001 Debug protocol 39](#_Toc156549847)

[5. 하드웨어 안전요구사항 추적 40](#_Toc156549848)

# 문서 개요

## 문서 목적

본 문서는 하드웨어 안전 요구 사항을 명시하기 위함이며, 이는 시스템 요구사항 명세서로부터 도출된다.

HSR(Hardware Safety Requirement), 즉 하드웨어 안전 메커니즘을 구현하기 위한 요구사항이며, 각 요구사항에 대한 Description, Implementation Concept, Time Interval, Requirement classifiacation Verification criteria 등 상세한 설명을 명세한다.

본 장에서는 본 문서 개요를 기술하며 2장에서는 HSR로 하드웨어 안전 요구사항에 대해 기술한다. 이어 3장에서는 요구사항 추척에 대해 기술한다.

## 적용 범위

본 문서가 적용되는 범위는 다음과 같다.

* 하드웨어 수준의 안전 요구사항 도출
  + 하드웨어 수준의 Target IC의 안전 메커니즘의 요구사항
  + 하드웨어 수준의 안전 요구사항 추척

## 약어, 용어 설명 (식별자 부여 규칙 포함)

|  |  |  |
| --- | --- | --- |
| **구분** | **항목설명** | **비고** |
| SEooC | Safety Element out of Context |  |
| HSR | Hardware Safety Requirement |  |
| SM | Safety Mechanism |  |
| FTTI | Fault Tolerant Time Interval |  |
| FDTI | Fault Detection Time Interval |  |
| FRTI | Fault Reaction Time Interval |  |
| FHTI | Fault Handling Time Interval |  |
| MPFDI | Multiple Point Fault Detection Interval |  |
|  |  |  |

## 참조문서

|  |  |  |
| --- | --- | --- |
| **No** | **문서명** | **버전** |
| 1 | ISO 26262-10:2018 Road vehicles — Functional safety —Part 10: Guideline on ISO 26262 | 2018 |
| 2 | ISO 26262-5:2018 Road vehicles — Functional safety —Part 5: Product development at the hardware level | 2018 |
| 3 | A-PUZL39 IP SEooC Application AoU | R4 |
| 4 |  |  |
| 5 |  |  |
|  |  |  |

# 하드웨어 기능 요구사항 (Hardware function requirements)

## HFR\_IP\_001 CPU feature

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HFR\_IP\_001 | Status | Draft |
| Type | HFR |  |  |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | CPU 사양 | Related SysFR | FN\_SoC\_001, FN\_SoC\_002,  FN\_SoC\_003, FN\_SoC\_004 |
| Description | Target IP는 주어진 사양에 따라 CPU를 설계 해야 한다. | | |
| Implementation  Concept | 1. Concept :  Target IP는 아래와 같은 사양의 CPU Processing을 구현해야 한다.  - Process : FPGA  - Operation Frequency :  CPU : TBD  AHB-BUS : TBD  APB-BUS : TBD"  - Analog IP  PLL : (Max : 100MHz)  Ext OSC : (24MHz)"  - Core : Andes N25F-SE  - Debug : JTAG (Serial-wire)  **- N25F-SE Specification**  5-stage in-order execution pipeline  Hardware multiplier  radix-2/fast  Hardware divider  Optional branch prediction  4-entry return address stack (RAS)  Choice of  \* Static branch prediction, or  \* Dynamic branch prediction  · 64/256-entry branch target buffer (BTB)  · 256-entry branch history table  · 8-bit global branch history  Machine mode and User mode  Misaligned memory accesses  RISC-V physical memory protection  ISO 26262 Automotive Functional Safety Compliant  Core trap status bus | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - CPU function Simulation (검증기준 : CPU 사양 만족)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : 하드웨어 **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information |  | | |

## HFR\_IP\_002 IP feature

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HFR\_IP\_002 | Status | Draft |
| Type | HFR |  |  |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | IP 사양 | Related SysFR | FN\_SoC\_001, FN\_SoC\_002,  FN\_SoC\_003, FN\_SoC\_004 |
| Description | Target IP는 주어진 사양에 따라 IP를 설계 해야 한다. | | |
| Implementation  Concept | 1. Concept :  Target IP는 아래와 같은 사양의 IP를 구현해야 한다.  - Timer (2ea)  - DMA (1ea)  - Watchdog (1ea)  - SMU(1ea)  - ECC / EDC / Parity  - Safety Manager (1ea)  - Fault Injector (1ea) | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - IP function Simulation (검증기준 : IP 사양 만족)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : IP **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information |  | | |

## HFR\_IP\_003 Internal memory feature

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HFR\_IP\_003 | Status | Draft |
| Type | HFR |  |  |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | Internal memory 사양 | Related SysFR | FN\_SoC\_001, FN\_SoC\_002,  FN\_SoC\_003, FN\_SoC\_004 |
| Description | Target IP는 주어진 사양에 따라 Internal memory를 설계 해야 한다. | | |
| Implementation  Concept | 1. Concept :  Target IP는 아래와 같은 사양의 Internal memory를 구현해야 한다.  - SRAM (512KB)  - ROM (32KB)  - I-Cache (32KB)  - D-Cache (32KB) | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - Internal memory function Simulation (검증기준 : Internal memory 사양 만족)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : Internal memory **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information |  | | |

## HFR\_IP\_004 External Interface feature

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HFR\_IP\_004 | Status | Draft |
| Type | HFR |  |  |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External Interface 사양 | Related SysFR | FN\_SoC\_001, FN\_SoC\_002,  FN\_SoC\_003, FN\_SoC\_004 |
| Description | Target IP는 주어진 사양에 따라 External Interface를 설계 해야 한다. | | |
| Implementation  Concept | 1. Concept :  Target IP는 아래와 같은 사양의 External Interface를 구현해야 한다.  - I2C (2ea)  - SPI (2ea)  - QSPI (1ea)  - UART (2ea)  - GPIO (32ch)  - LIN (2ea) | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - External Interface function Simulation(검증기준 : External Interface 사양 만족)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : External Interface **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information |  | | |

# 하드웨어 안전요구사항 (Hardware safety requirements)

## HSR\_IP\_001 Window watchdog

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_001 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | Window watchdog | Related TSR | TSR\_SoC\_01 ~ TSR\_SoC\_07 |
| Description | Target IP는 MCU Core의 결함을 감지하기 위한 Window watchdog을 설계해야 한다. | | |
| Implementation  Concept | 1. Concept :  일반적인 Watchdog과 달리, Window Watchdog 은 일정한 주기 뿐만 아니라, 설정한 윈도우 시간내에 Core가 접근하여 Watchdog counter를 초기화 해야 한다. 이를 위해 MCU Core는 일정한 주기 내에 Watchdog Timer를 초기화 할 수 있도록 프로그래밍 되어야 한다. 만약, Core가 비정상 동작에 의해 IP 내부 Watchdog Timer를 초기화 하지 못하면 Core의 오류를 감지하고, 시스템을 초기화 해야 한다.  <Related Diagram>    <Timing Chart>    2. Detection : MCU Core  3. Reaction :  SS1. Reset (Internal / External) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 정상적인 Window 범위 내에 Kick이 들어오는지 확인.)  - 오류 주입 Simulation (검증기준 : 정상적으로 Window의 범위를 벗어난 Kick에 대해 Reset 신호를 생성하는지 확인)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : Cadence (XCELIUM 18.03)  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : Linux, Min memory 1GB. Min Disk Space 5~6GB  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM001 | | |

## HSR\_IP\_002 External Window watchdog

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_002 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External Window watchdog | Related TSR | TSR\_SoC\_01 ~ TSR\_SoC\_07 |
| Description | Target IP는 MCU Core의 결함을 감지하기 위한 External Window watchdog을 포함해야 한다. | | |
| Implementation  Concept | 1. Concept :  일반적인 Watchdog과 달리, Window Watchdog 은 일정한 주기 뿐만 아니라, 설정한 윈도우 시간내에 Core가 접근하여 Watchdog counter를 초기화 해야 한다. 이를 위해 MCU Core는 일정한 주기 내에 Watchdog Timer를 초가화 할 수 있도록 설계되어야 한다. 만약, Core가 비정상 동작에 의해 IP 외부 Watchdog Timer를 초기화 하지 못하면 Core의 오류를 감지하고, 시스템을 초기화 해야 한다.  <Related Diagram>    <Timing Chart>    2. Detection : 외부 MCU or AP  3. Reaction :  - SS1. Reset (Internal / External)  - SS3. 외부 MCU or AP에서 detection (by external safety mechanism) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 정상적인 Window 범위 내에 Kick이 들어오는지 확인.)  - 오류 주입 Simulation (검증기준 : 정상적으로 Window의 범위를 벗어난 Kick에 대해 Reset 신호를 생성하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM002 | | |

## HSR\_IP\_003 Bus data parity check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_003 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | Bus data parity check | Related TSR | TSR\_SoC\_03, TSR\_SoC\_07 |
| Description | Target IP는 Bus(AHB, APB) 통신 data의 송수신 결함을 감지하기 위해 parity check가 가능한 parity bit를 포함하여 설계해야 한다. | | |
| Implementation  Concept | 1. Concept :  Bus에 연결된 주변장치로 전송되는 data의 송수신 결함을 감지하기 위해 parity check를 적용하여 설계한다.. 연결된 주변장치는 수신된 data에 대한 parity를 계산한다. 계산된 parity가 수신된 parity와 일치할 경우 올바르게 수신된 것으로 판단한다.  <Related Diagram>    2. Detection : 주변장치 내 parity checker  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 수신된 Data의 Parity를 계산하여 계산된 parity가 수신된 parity와 동일한 지 확인.)  - 오류 주입 Simulation (검증기준 : 강제로 전송되는 parity bit 및 data를 변경하여 parity error가 발생하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM006 | | |

## HSR\_IP\_004 Cache Memory ECC

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_004 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | Cache memory ECC | Related TSR | TSR\_SoC\_04, TSR\_SoC\_06 |
| Description | Target IP는 CPU 코어의 동작에 영향을 주는 캐쉬 메모리에 대하여 ECC를 통해 데이터의 오류를 검출 및 정정 동작을 수행한다. | | |
| Implementation  Concept | 1. Concept :  캐쉬 메모리에 쓰기 동작시에 ECC 값을 함께 저장하고, 읽기 동작시에 읽은 Data를 통해 ECC를 생성하여 쓰기 동작시에 저장한 ECC값과 비교한다. 두 ECC 값을 비교하여 오류가 발생하였는지 확인한다. 1bit 오류가 발생하면 정정하고, 2bit 이상의 오류가 발생하면 신호를 통해 Safety Manager에 알린다.  디코딩 및 비교 과정에서 발생할 수 있는 오류를 감지하기 위해 동일한 ECC 디코딩 블록을 중복으로 배치하여 이를 검사할 수 있도록 한다. 동일한 Data를 각 각의 ECC 디코더에 입력하여 두 블록의 결과값을 비교하도록 구성한다.  <Related Diagram>    2. Detection : 캐시 내 ECC checker  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 읽기 동작시에 읽은 Data를 통해 ECC를 생성하여 쓰기 동작시에 저장한 ECC값과 비교하여 오류가 발생하였는지 확인.)  - 오류 주입 Simulation (검증기준 : 강제로 전송되는 ECC bit 및 data를 변경하여 ECC error가 발생하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM007 | | |

## HSR\_IP\_005 I2C ACK/NACK check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_005 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | I2C ACK/NACK check | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 I2C Master는 통신이 정상적으로 전달되는지 ACK/NACK 를 통해 확인한다. | | |
| Implementation  Concept | 1. Concept :  -Master I2C로 구현되었을 때 : I2C 통신을 통해 Master가 데이터를 송신 하는 경우, Slave는 통신의 이상 유무에 따라 ACK 또는 NACK 신호를 Master로 전송한다. 이 때, Master는 수신된 ACK 또는 NACK 비트를 기반으로 통신의 실패 여부를 판단한다. I2C는 항상 Master가 통신을 시작하는 형태이다. Master는 통신을 시작하고 Slave는 Master로부터 전달된 Packet에 대해 ACK/NACK를 통해 통신이 정상적으로 처리되었는지 처리되지 않았는지 응답을 하여야 한다. 만약, Slave의 ACK 응답이 오류로 인해 NACK로 전달되는 경우 Master는 Slave에 다시 통신을 시도하여야 한다.  Master가 의도하지 않은 통신이 시작된 경우 Slave의 ACK/NACK 응답을 통해 이를 확인할 수 있다.  -Slave I2C로 구현되었을 때 : 해당사항 없음.  <Timing Chart>      2. Detection : I2C IP  3. Reaction :  - Master가 Slave에게 다시 request하여 data 요구함(retry request).  - 응답이 없는 경우 SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  (O)외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : I2C 통신을 통해 Data를 송신하여 ACK 신호가 수신되는 지 확인.)  - 오류 주입 Simulation (검증기준 : 의도적으로 ACK/NACK를 변경하여 Maste가 전송 성공 또는 실패를 판단하는지 시험)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM012 | | |

## HSR\_IP\_006 I2C discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_006 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | I2C discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 Master I2C는 protocol을 벗어난 잘못된 data가 입력될 시, 이를 discard 해야 한다. | | |
| Implementation  Concept | 1. Concept :  -Master I2C로 구현되었을 때 : Master I2C는 시작하지 않은 통신에 대한 입력 데이터나 다른 Master에 의해 시작된 통신에 대한 입력 Data는 무시하여야 한다. I2C는 항상 Master에 의해 통신이 시작된다. 하지만 Slave의 오류로 인해 시작하지 않은 통신에 대한 예상치 않은 Data가 입력되는 경우에 이를 무시하여야 한다.  I2C는 일반적으로 하나의 Master와 여러 개의 Slave를 연결하는 버스 구성을 갖지만, 여러 Master와 여러 Slave를 연결하는 버스 구성도 가능하다. 이 경우에 Master는 자신이 시작한 통신이 아닌 다른 Master가 시작한 통신에 대해서는 이를 감지하고 이에 해당하는 Data 입력이 들어오는 경우 무시하여야 한다.  -Slave I2C로 구현되었을 때 : 해당사항 없음.  <Timing Chart>    2. Detection : I2C IP  3. Reaction :  - 별도 Reaction 없음 (의도치 않은 data 수신 거절) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  ( )내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준: Master I2C가 통신을 시작하기 전에 I2C 버스 상의 SDA Data를 Toggle 시켜 이를 Master I2C가 무시하는지 확인)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM013 | | |

## HSR\_IP\_007 External I2C discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_007 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External I2C discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | 외부 Master는 Slave로부터 I2C protocol을 벗어난 잘못된 data가 입력될 시, 이를 discard 해야 한다. | | |
| Implementation  Concept | 1. Concept :  -Master I2C로 구현되었을 때 : 해당사항 없음  -Slave I2C로 구현되었을 때 : Slave I2C의 오류로 인해 외부로 데이터 전송이 되는 경우에, 외부 Master는 시작하지 않은 통신에 대한 입력 데이터로 간주하여 입력 Data는 무시하여야 한다. I2C는 일반적으로 하나의 Master와 여러 개의 Slave를 연결하는 버스 구성을 갖지만, 여러 Master와 여러 Slave를 연결하는 버스 구성도 가능하다. 이 경우에 Master는 자신이 시작한 통신이 아닌 다른 Master가 시작한 통신에 대해서는 이를 감지하고 이에 해당하는 Data 입력이 들어오는 경우 무시하여야 한다.  <Timing Chart>    2. Detection : External I2C IP  3. Reaction :  - SS3.외부 MCU or AP에서 detection (by external safety mechanism) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  ( )내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 외부 Master I2C가 통신을 시작하기 전에 I2C 버스 상의 SDA Data를 Toggle 시켜 이를 외부 Master I2C가 무시하는지 확인)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM014 | | |

## HSR\_IP\_008 SPI discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_008 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | SPI discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 SPI Master가 SPI protocol을 벗어난 잘못된 data를 전송 및 수신 시 이를 discard 해야 한다. | | |
| Implementation  Concept | 1. Concept :  - Master SPI로 구현되었을 때 : SPI는 Master와 Slave 간에 상호 정의된 프로토콜을 사용하여 통신을 수행한다.  정의된 Bit Count 가 위배되거나, 특정 신호(SS, SCK, MOSI, MISO)가 정해진 프로토콜에 맞지 않게 전송되는 경우에 이를 오류로 감지하고 무시해야 한다. 요청하지 않은 프로토콜이 수신되면, Master는 이를 정해진 프로토콜이 아니라 판단하여 무시하게 된다.  Master SPI로 구현되어 요청하지 않은 프로토콜이 전송되면, 외부 Slave는 이를 SW 처리를 통해 정해진 프로토콜이 아니라 판단하여 무시해야 한다.  - Slave SPI로 구현되었을 때 : 해당사항 없음  <Timing Chart>      2. Detection : SPI IP  3. Reaction :  - 별도 Reaction 없음 (의도치 않은 data 수신 거절) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  ( )내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 :  의도적으로 프로토콜을 변경하여 외부 Slave 가 Master 로부터 전송되는 data의 수신을 무시하는 지 확인.  의도적으로 프로토콜을 변경하여 Master가 외부 Slave 로부터 전송되는 data의 수신을 무시하는 지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM019 | | |

## HSR\_IP\_009 External SPI discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_009 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External SPI discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 SPI Slave가 SPI protocol을 벗어난 잘못된 data 송신 시, 외부 Master가 이를 discard 해야 한다. | | |
| Implementation  Concept | 1. Concept :  - Master SPI로 구현되었을 때 : 해당사항 없음  - Slave SPI로 구현되었을 때 : SPI는 Master와 Slave 간에 상호 정의된 프로토콜을 사용하여 통신을 수행한다.  정의된 Bit Count 가 위배되거나, 특정 신호(SS, SCK, MOSI, MISO)가 정해진 프로토콜에 맞지 않게 전송되는 경우에 이를 오류로 감지하고 무시해야 한다. Slave SPI일 경우 요청하지 않은 프로토콜이 송신되면, 외부 Master는 이를 정해진 프로토콜이 아니라 판단하여 무시해야 한다.  <Timing Chart>  텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진  자동 생성된 설명    2. Detection : External SPI IP  3. Reaction :  - SS3.외부 MCU or AP에서 detection (by external safety mechanism) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 :  의도적으로 프로토콜을 변경하여 외부 Master가 Slave 로부터 전송되는 data의 수신을 무시하는 지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM020 | | |

## HSR\_IP\_010 LIN checksum check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_010 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | LIN checksum check | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP는 LIN 프로토콜에 포함된 checksum 값을 통해 통신 상 오류 여부를 확인할 수 있도록 설계해야 한다. | | |
| Implementation  Concept | 1. Concept :  - Master LIN으로 구현되었을 때 : 해당사항 없음  - Slave LIN으로 구현되었을 때 : 외부 LIN Master에서 생성된 Data와 Checksum 이 전달되면, LIN Slave는 수신된 Data를 통해 Checksum 을 계산하고, 전송 받은 Checksum과 비교하여 통신상 오류가 발생하였는지 판단하여야 한다.  <Timing Chart>      Checksum 값은 전송되는 Data의 값을 모두 더한 후 Modulo 256을 취한 값을 Inversion하여 구한다.  이 값을 Data 전송 이후 Checksum Field 에 넣어 전송하게 된다.  LIN Slave는 수신된 Data를 동일한 Checksum 생성 방식으로 생성하고, Checksum Field로 수신된 Checksum 값과 비교하여 통신상 오류 발생 여부를 판단한다.  2. Detection : LIN IP  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  (O)외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 :  Slave LIN은 수신된 Data를 통해 Checksum 값을 생성해야 하며, 수신된 Checksum값과 전송된 data를 통해 생성한 Checksum 값을 비교하하여 오류 여부를 판단하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM022 | | |

## HSR\_IP\_011 External LIN checksum check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_011 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External LIN checksum check | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | 외부 LIN Master는 프로토콜에 포함된 checksum 값을 통해 통신 상 오류 여부를 확인할 수 있는 기능을 포함해야 한다. | | |
| Implementation  Concept | 1. Concept :  - Master LIN으로 구현되었을 때 : 해당 사항 없음  - Slave LIN으로 구현되었을 때 : LIN Slave는 송신하려는 Data와 송신 Data를 이용하여 생성한 Checksum 을 전달하여야 하며, 외부 LIN Master는 수신된 Data를 통해 Checksum 을 계산하고, 전송받은 Checksum과 비교하여 통신상 오류가 발생하였는지 판단하여야 한다.  <Timing Chart>    Checksum 값은 전송되는 Data의 값을 모두 더한 후 Modulo 256을 취한 값을 Inversion하여 구한다.  이 값을 Data 전송 이후 Checksum Field 에 넣어 전송하게 된다.  외부 Master는 이 전송된 Data를 동일한 Checksum 생성방식으로 생성하고, Checksum Field로 수신된 Checksum 값과 비교하여 통신상 오류 발생 여부를 판단한다.  2. Detection : External LIN  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  (O)외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 :  외부 Master LIN은 수신된 Data를 통해 Checksum 값을 생성해야 하며, 수신된 Checksum값과 전송된 data를 통해 생성한 Checksum 값을 비교하여 오류 여부를 판단하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM023 | | |

## HSR\_IP\_012 External LIN discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_012 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External LIN discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | 외부 LIN Master는 의도치 않은 Slave 로 부터의 데이터 수신을 discard 하여야 한다. | | |
| Implementation  Concept | 1. Concept :  LIN 프로토콜은 Master에서 통신을 시작한다. 때문에 Master에서 시작하지 않은 통신에 대해 Slave가 데이터를 송신하는 경우, 이를 무시하여야 한다.  <Timing Chart>      2. Detection : External LIN  3. Reaction :  - SS3.외부 MCU or AP에서 detection (by external safety mechanism) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  (O)타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 외부 Master LIN이 통신을 시작하기 전에 LIN 버스 상의 신호를 Toggle 시켜 이를 외부 Master LIN에서 무시하는지 확인)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM024 | | |

## HSR\_IP\_013 LIN parity check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_013 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | LIN parity check | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP는 Parity bit 를 체크하여 LIN Master가 보낸 데이터에 대한 오류를 체크해야 한다. | | |
| Implementation  Concept | 1. Concept :  - Master LIN으로 구현되었을 때 : 해당 사항 없음  - Slave LIN으로 구현되었을 때 : LIN Slave는 전송된 PID Field의 Identifier 값을 이용하여 Parity bit를 생성하고, 전송받은 Parity 값과 비교하여야 한다. 이 값을 비교하여 전송상 오류가 발생하였는지 판단해야 한다.  <Timing Chart>    2. Detection : LIN IP  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 수신된 PID의 Identifier 값을 이용하여 Parity bit을 생성하고 전송받은 Parity bit 과 비교하여 오류 발생 여부를 판단하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM025 | | |

## HSR\_IP\_014 UART discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_014 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | UART discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 UART 는 의도치 않은 Data 수신을 거절하기 위한 SW 기능을 포함하여 구성해야 한다. | | |
| Implementation  Concept | 1. Concept :  UART는 Full duplex 방식으로 Data의 수신과 송신이 각 각 분리되어 처리된다. UART는 송신과 수신간에 미리 정의된 프로토콜로 통신을 수행한다.  수신단에서 의도하지 않는 Data의 수신을 거절하기 위해서는 해당 수신라인(RX)에 대한 입력을 제어하는 SW 기능이 필요하다. SW를 통해 수신을 의도하는 경우에만 수신라인이 동작하도록 제어하여 Data 수신을 수행하도록 해야 한다. 수신을 원치 않는 경우에는 SW를 통해 수신라인이 동작하지 않도록 제어해야 한다.  <Related Diagram>    2. Detection : UART IP  3. Reaction :  - 별도 Reaction 없음 (의도치 않은 data 수신 거절) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  ( )내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : RX 데이터 라인을 SW를 통해 제어하여 UART 수신단에서 data 수신을 거절하는 지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM028 | | |

## HSR\_IP\_015 External UART discard data

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_015 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | External UART discard data | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | 외부 UART 는 의도치 않은 Data 수신을 거절하기 위해 SW 기능을 포함해야 한다. | | |
| Implementation  Concept | 1. Concept :  UART는 Full duplex 방식으로 Data의 수신과 송신이 각 각 분리되어 처리된다. UART는 송신과 수신간에 미리 정의된 프로토콜로 통신을 수행한다.  외부 UART 수신단에서 의도하지 않는 Data의 수신을 거절하기 위해서는 해당 수신라인(RX)에 대한 입력을 제어하는 SW 기능이 구현되어야 한다. SW를 통해 수신을 의도하는 경우에만 수신라인에 대한 동작을 제어하여 Data 수신을 수행하도록 해야 한다. 수신을 원치 않는 경우에는 SW를 통해 수신라인이 동작하지 않도록 제어해야 한다.  <Related Diagram>    2. Detection : External UART IP  3. Reaction :  SS3.외부 MCU or AP에서 detection (by external safety mechanism) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  (O)타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  ( )내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 외부 UART 수신단에서 SW 기능을 통해 RX 라인을 제어하여 data 수신을 거절하는 지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM029 | | |

## HSR\_IP\_016 UART parity check

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_016 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | UART parity check | Related TSR | TSR\_SoC\_02, TSR\_SoC\_05 |
| Description | Target IP의 UART는 Parity bit 를 체크하여 수신한 데이터에 대한 오류를 체크한다. | | |
| Implementation  Concept | 1. Concept :  UART는 전송 데이터에 대한 오류 여부를 판단하기 위해 Data를 이용하여 Parity bit를 생성하여 함께 전송한다.  UART 수신단에서는 전송된 Data를 이용하여 Parity bit를 생성하고, 함께 수신된 Parity bit와 비교하여 통신상 오류 발생 여부를 판단한다.  <Timing chart>    2. Detection : UART IP  3. Reaction :  - SS1. Reset (Internal / External)  - SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 수신된 Data를 통해 Parity bit를 생성하고, 수신된 Parity bit와 비교하여 오류 발생 여부를 판단하는지 확인.)  - 오류 주입 Simulation (검증기준 : 수신중인 Data를 임의로 변경하여 오류를 강제 주입하고, Parity bit 비교시에 오류발생을 판단하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM030 | | |

## HSR\_IP\_017 SRAM ECC

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HSR\_IP\_017 | Status | Draft |
| Type | HSR | ASIL | B |
| Operational mode | Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | SRAM ECC | Related TSR | TSR\_SoC\_01, TSR\_SoC\_04, TSR\_SoC\_06 |
| Description | 시스템 메모리는 메모리의 오류를 검사하기 위해 ECC 를 수행해야 한다. | | |
| Implementation  Concept | 1. Concept :  시스템 메모리에 쓰기 동작시에 ECC 값을 함께 저장하고, 읽기 동작시에 읽은 Data를 통해 ECC를 생성하여 쓰기 동작시에 저장한 ECC값과 비교하여 오류가 발생하였는지 확인한다. 1bit 오류가 발생하면 정정하고, 2bit 이상의 오류가 발생하면 신호를 통해 Safety Manager에 알린다.  <Related diagram>    2. Detection : SRAM Controller IP  3. Reaction : SS1. Reset (Internal / External)  SS2. Interrupt를 통한 Error message (I2C, UART, SPI, LIN) | | |
| Time Interval | FDTI (Fault Detection Time Interval) : TBD ms (System clock cycle)  FRTI (Fault Reaction Time Interval) : TBD ms (System clock cycle)  FHTI (Fault Handling Time Interval) = TBD ms  MPFDI (Multiple Point Fault Detection Interval) : N/A (이중점 결함 검출인 경우만 해당) | | |
| Requirement classification | (O)하드웨어 엘리먼트의 내부 고장을 제어하기 위한 안전 메커니즘과 관련된 요구사항  ( )외부 엘리먼트의 고장을 제어하거나 견디기 위한 안전 메커니즘과 관련된 요구사항  ( )타 엘리먼트의 안전 요구사항에 부합하기 위한 안전 메커니즘과 관련된 요구사항  (O)내부나 외부 고장을 검출하고 신호를 보내기 위한 안전 메커니즘과 관련된 요구사항  ( )안전 메커니즘을 명시하지 않는 하드웨어 안전 요구사항 | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - 기능 Simulation (검증기준 : 메모리 Read 동작 시 ECC bit 생성 및 저장된 ECC bit와 비교하여 ECC error를 판단하는지 확인.)  - 오류 주입 Simulation (검증기준 : 강제로 전송되는 ECC bit 및 data를 변경하여 ECC error가 발생하는지 확인.)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Software Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information | - Related Safety Mechanism : SM036 | | |

# 하드웨어 비기능 요구사항 (Hardware non-function requirements)

## HNFR\_IP\_001 Debug protocol

|  |  |  |  |
| --- | --- | --- | --- |
| ID | HNFR\_IP\_001 | Status | Draft |
| Type | HNFR |  |  |
| Operational mode | Initial mode  Normal mode | Priority  (High/Medium/Low) | Medium |
| Requirement  Title | Debug protocol | Related SysNFR | FN\_SoC\_003 |
| Description | Target IP는 Debug 시 요구되는 통신 프로토콜을 만족해야 한다. | | |
| Implementation  Concept | Debug 통신 protocol  - RISC-V External Debug Support  - Configurable number of breakpoints: 2/4/8  - External JTAG debug transport module  JTAG: IEEE Std 1149.1 style 4-wire JTAG interface  Serial: Andes 2-wire serial debug interface | | |
| Verification criteria | 1. 검증 방법 및 검증기준  - Debug 기능 simulation (검증기준 : Debug 통신 protocol 만족 여부 확인)  2. 검증 환경 조건 (온도, 진동, 전자파 등) : **검증 시 사용하는 Debug simulation Tool 이름**  3. 사전 조건 및 특정 운용 환경 (공급전압, mission profile 등) : **위 Tool 사용하기 위한 조건**  4. 제약사항 및 특수 요구사항 : N/A | | |
| Additional information |  | | |

# 하드웨어 안전요구사항 추적

관련된 요구사항 (HR, HSR, HNR)에 대한 추적은 별도의 요구사항 추적 Matrix 파일을 참조한다.