2019
Electronics and
Telecommunications
Trends

# 자율주행자동차 전장시스템을 위한 기능안전 프로세서 기술

Functional Safety Processor for Electronics of Autonomous Cars



**한진호** (J.H. Han, soc@etri.re.kr) 프로세서연구그룹 책임연구원/PL
**권영수** (Y.S. Kwon, yskwon@etri.re.kr) 프로세서연구그룹 책임연구원/그룹장
**강성원** (S.W. Kang, kangsw@etri.re.kr) 지능형반도체연구본부 책임연구원/본부장

Automotive electronics are complex and require high performance with an advanced driver assistant system (ADAS) and a functioning autonomous system. Thus, considering their complexity, the processor of the electronic control unit (ECU) requires a design that ensures high performance and reliability to ensure functional safety. This study discusses the technology used for developing a processor that can ensure functional safety of current automotive electronic systems.

* DOI: 10.22648/ETRI.2019.J.340111

## Ⅰ. 소개

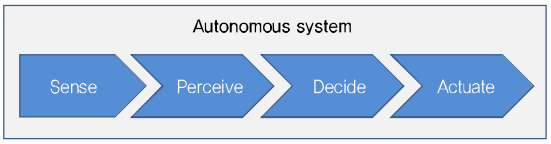
자동차는 자율주행 기능을 탑재하기 위해, 가깝게는 Advanced Driver Assistant System(ADAS) 장착을 위하여 자동차의 전장시스템은 높은 성능을 요구하고 있고 더욱더 복잡해 져가고 있다. 이로인해 자동차에 장착되는 Electronic Control Unit(ECU)에 쓰이는 프로세서는 더 많은 기능을 요구하고 있으며, 복합한 프로세서는 더 강한 기능안전 설계를 통해 Reliability를 가져야 한다. 여기서는 최근에 요구하고 있는 자동차 전장시스템에 적용되고 있는 기능안전 프로세서 기술을 살펴보겠다.

ADAS는 〈표 1〉과 같은 기능으로 나뉜다. 이름 그대로 차선, 주행 중 선행차량, 정차 시 앞차, 반대차선의 차량, 도로상의 표지판, 신호등, 도로상의 움직이는 보행자를 인식하여 그 정보를 경고로 알려주거나, 차량 제어를 통해 운전자를 보조한다[1].

자율주행(Autonomous Driving)은 환경인식, 위치인식 및 매핑, 판단, 제어, 그리고 인터랙션이라는 자율주행 기술 구성요소[2]를 이용하여 운전자의 개입없이 주변 환경을 인식을 하고 주행 상황을 판단하여 차량을 제어함으로써, 스스로 주어진 목적지까지 주행하는 자동차를 말한다. 자율주행 인프라가 설치된 센서를 통해 교통정보 및 신호 변경 정보를 수신하고 차량 간 통신을 통해 안전거리를 유지하며 도로를 주행할 수 있다. 이를 위해 해서는 아래와 같은 기능을 요구하는 반도체를 필요로 한다. 차량에 장착된 Sensor를 통해 주변 환경에 대한 정보를 Sensing한 정보를 받는 과정인 Sense 단계가 있고, 이 Sense한 정보를 바탕으로 인지(Perceive)를 해야 한다[(그림 1) 참조].

〈표 1〉 ADAS 기능

| 기능 | 설 명 |
|---|---|
| LDW | – 차선 및 운행방향 감지, 양 차선의 중심과 차량의 중심이 차이가 나면 차량이 차선을 이탈하였다고 판단하여 경고음 발생 |
| FCW | – 차선 내의 선행차량을 인식하여 상대속도와 거리를 계산, Time To Collision(TTC)를 예측하여 경보.<br>– 선행차량과의 차간 거리 모니터링을 통해 경보를 주는 방식은 충돌 시간 예측보다는 부정확함. |
| FCDA | – 정차 시에 앞차가 멈추어 있다가 출발하면 알람으로 운전자의 주위를 환기 시켜주는 기술 |
| HBA | – 상향등을 키고 운전하고 있을 때, 대형차 또는 선행차가 가까워지면 자동으로 하향등으로 바꾸었다가 시야에서 멀어지면 다시 상향등으로 바꿔주는 기술 |
| TSR | – 도로상의 표지판, 특히 제한속도 표지판을 인식하여 운전자에게 알려주는 기술 |
| TLR | – 도로상의 신호등을 인식하여 현재 도로에서 주행해야 하는지, 멈추어야 하는지를 알려주는 기술 |
| PD | – 한밤중에 사람이나 동물을 인식하는 나이트 비전과는 다르게 근거리에서 도로상의 움직이는 보행자를 인식하는 기술 |
| LKA | – 차선 인식을 통해 운전자가 차선을 무의식적으로 넘고 있다고 판단이 되면 핸들을 조정하여 차로를 벗어나지 않도록 제어하는 기술 |




(그림 1) Autonomous System의 처리단계

앞에 장애물이 될 수 있는 자동차, 보행자 등이 있는지 또는 주행이 가능한 도로 인지 아닌지, 신호등이 파란불인지 빨간 불인지 등을 인지한 정보를 이용하여 차량을 어떻게 제어할지를 결정하게 된다. 그리고 그 결정된 결과에 따라 차량의 조향장치, 액셀러레이터, 브레이크 등을 제어하게 된다.

또한, 기능안전을 요구하는 자동차 전장시스템에 사용이 되기 위해서 표준화된 기능안전 설계를 요구하고 있다.

### 1. ISO26262 기능안전 표준

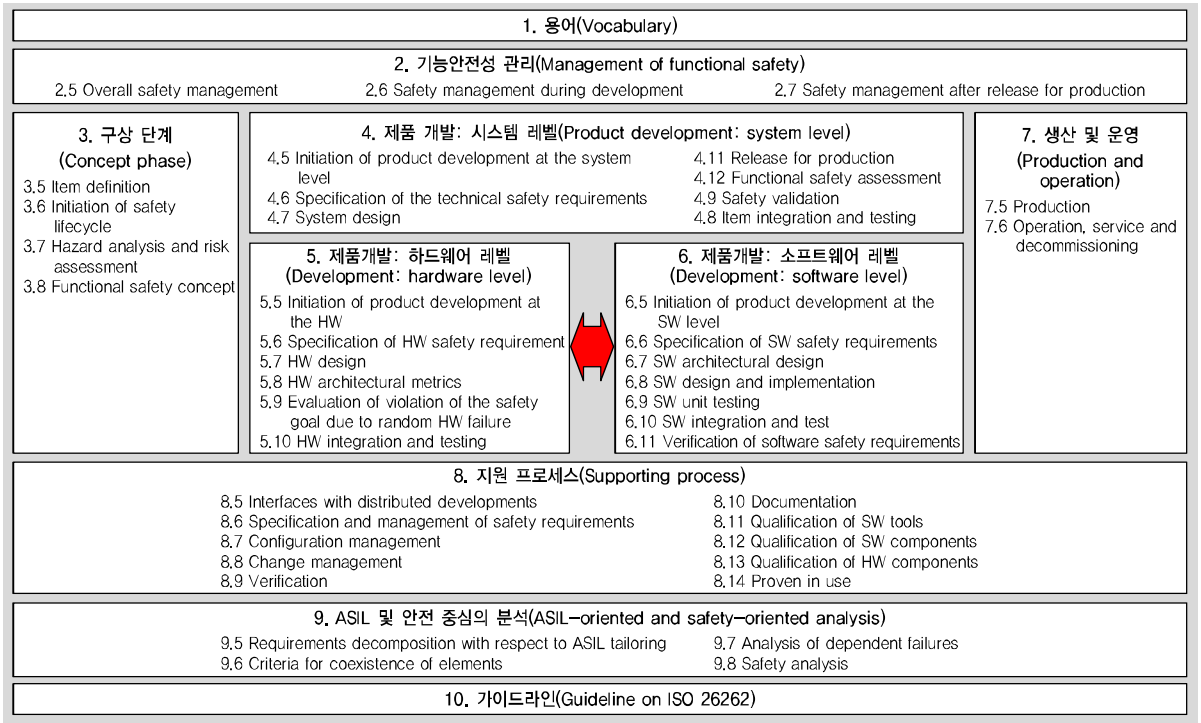
기능안전을 요구하는 자동차 전장시스템에 사용이 되기 위해서는 다음과 같은 표준화된 기능안전 설계를 요구하고 있다.

ISO-26262[3]는 도로 자동차를 위한 기능안전에 대한 표준으로 차량에 탑재되는 전기/전자 시스템의 오류로 인한 사고를 줄이기 위해 유럽, 미국, 일본의 주요 완성차 및 부품 업체 주도로 제정된 국제 규격으로 최대

중량 3,500kg까지의 승용차에 설치되는 전기, 전자시스템에 적용된다. 2011년 11월 15일 제정된 이 표준은 자동차용 전기 및 전자 시스템 제조업체에서는 사실상의 필수 기술규격으로, 관련 규정을 반드시 준수하여 제품을 개발해야 하고 표준 준수를 증명해야 한다. Par1~10으로 구성이 되어 있으며, 각 Part에서 정의하고 있는 내용은 〈표 2〉와 같다. 각 Part 별로 상호 관련성을 가지고 있으며, 상호 관련성은 (그림 2)와 같이

〈표 2〉 ISO26262 Par1~10

| | |
|---|---|
| Part 1 | – 관련 용어 정리 |
| Part 2 | – 기능 안전성에 관련된 개별 활동을 계획, 조정, 추적하는 요건 정의<br>– 전반적인 안전성 관리 요구사항을 정의 |
| Part 3 | – 개발 품목 정의를 기반으로 해저드 분석 및 위험심사를 통해 ASIL 판정<br>– 안전 목표와 안전 메커니즘 정의 |
| Part 4 | – 제조사 관점의 시스템 통합<br>– 외부 수단으로 구현된 안전 개념의 효과 확인<br>– E/E 시스템 외 기술 안전 메커니즘 확인<br>– 사람의 통제성 및 작동작업에 대한 전제 검증 |
| Part 5 | – V모델 개념에 따른 HW의 개발, 통합, 검증 등에 대한 요구사항 정의 |
| Part 6 | – SW 수준 개발에 대해 V모델 개념에 따라 개발, 통합, 검증 등에 대한 요구사항 정의 |
| Part 7 | – 품목 생산을 위한 계획, 샘플생산, 양산, 서비스 등에 관한 요구사항 정의 |
| Part 8 | – 안전 요구사항 관리, 명세 방법, 형상/변경관리, 검증, 문서화, 지원도구 자격 검증, 재사용 SW 자격검증, HW 자격검증, 실제 사용을 통해 입증된 안전성 등에 대한 요구사항 정의 |
| Part 9 | – 안전 요구사항 ASIL을 분해하는 방법<br>– 안전 관련 구성요소 사이 공존의 조건인 상호간섭의 정도, 위험분석 방법 기술 |
| Part 10 | – 주요 개념, 안전케이스, ASIL 분해 등 ISO 26262 이해에 도움이 되는 정보 기술 |




(그림 2) ISO26262 표준의 Product Development Lifecycle

[출처] Reprinted with permission from ISO-26262, "Road Vehicle - Functional Safety," ISO, 2011.

V개발 모델 혹은 V&V 모델로서 표현이 된다. Part 1과 10은 기본적인 용어와 이해를 돕기 위한 설명이고 Part 3, 4, 5, 6, 7은 핵심 프로세스(Core Process)로 개발 아이템의 개념 및 정의, 요구사항 도출, 설계 반영, 양산이관, 양산, 차량운행, A/S, 폐기에 이르기까지의 절차를 제시하고 있다.

반도체에 대한 기능안전 적용 Guideline(Part 11) 및 Motor-cycle, Truck 등에 대한 기능안전(Part 12) 내용을 포함하여 현재 2nd Edition이 FDIS 승인이 되었고, 한국전자통신연구원에서는 Part 11에 Fault Injection을 통한 Diagnostic Coverage Analysis Guideline을 제안하여 채택되었다.

Part 11에서는 반도체에 기능안전 설계 적용함에 있어 PAS-19451 기반의 내용을 포함하여 반도체 IP 기반 기능안전 성능 분석 방법, 반도체의 Fault Rate 분석을 위한 Fault Injection Method의 적용 Guideline, 및 BFR(Base Fault Rate) 계산 Guideline을 제시하고 있다.

반도체 기능안전 설계 성능 분석을 위해서는 기능안전 설계의 diagnostic coverage를 다음의 계산식 (1)과 같이 계산을 해야 한다.

$$\lambda_{RF} = \lambda \times (1 - F_{safe}) \times (1 - K_{FMC,RF}) \qquad (1)$$

$\lambda$는 Failure rate of the safety related faults, $F_{safe}$는 Fraction of safe faults of the part, $K_{FMC,RF}$와 $F_{safe}$는 기능안전 설계에 의해 안전 위반을 방지하는 비율이다.

이 중 $K_{FMC,RF}$, $F_{safe}$는 기능안전 설계에 Fault Injection Analysis에 의해 분석이 가능하다. 기능안전 설계가 적용된 회로에 Fault Injection이 가능한 위치에 Fault를 가상으로 발생시켜 기능안전 설계가 이를 방지 할 수 있는지, 전체 Fault 중 Failure를 발생시키지 않는 비율 등을 계산해 낼 수 있다. 그러나, $\lambda$는 복잡한 BFR(Base Failure Rate) 계산식 (2)에 의해 도출이 된다.

이는 $\lambda_{die}$, $\lambda_{package}$ 그리고, $\lambda_{overstress}$로 구성이 되고, 이는 이 중 $\lambda_1$과 $\lambda_2$는 IEC/TR 62380 Table 16에 의해 Type과 Transistor 수 반도체 컴포넌트의 기능에 따라 결정이 된다.

이를 이용하여 Fault Tolerant Architecture에 대한 Fault Analysis를 통해 Fault Tolerance 정도를 ASIL 등급으로 보여야 한다.

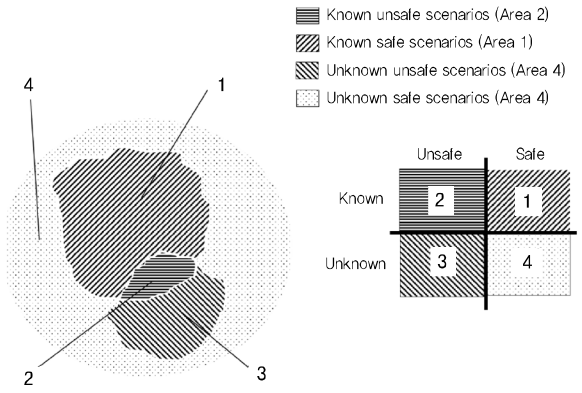
## 2. ISO/PAS21448 의도된 기능안전 표준

ISO/TC22/SC32/WG8에서 Safety of The Intended Functionality(SOTIF) 라는 Project Group으로 시작된 표준으로 올해 FDIS 승인 중에 있다.

ISO-26262 에 의한 기능안전 성능 분석을 통해 전장 시스템에서의 Malfunction에 의한 비합리적인 위험(Unreasonable Risk)이 없다는 것이 입증이 되었다고 하여도 Sensor를 통해 주변환경 정보를 취득하는 시스템의 의도된 기능은 센서 기능의 한계로 기능안전에 문제가 발생할 수 있다. 즉, ADAS에서 Machine Learning Algorithm을 이용하는 시스템이 상황을 이해하여 장애물을 회피하는 기능이 센서정보에서 장애물을 파악할 수 없을 정도의 정보를 얻게 되어 오동작할 수가 있다. 이러한 문제점을 해결하기 위해 표준 가이드를 설계 단계, 검증(Verification) 단계, 평가(Validation)단계에서의 방안을 제시하고 있다.

$$\lambda = \left( \underbrace{\left\{\lambda_1 \times N \times e^{-0.35 \times a} + \lambda_2\right\} \times \left\{ \frac{\sum_{i=1}^{y} (\pi_t)_i \times \tau_i}{\tau_{on} + \tau_{off}} \right\}}_{\lambda_{die}} + \underbrace{\left\{ 2.75 \times 10^{-3} \times \pi_\alpha \times \left( \sum_{i=1}^{z} (\pi_n)_i \times (\Delta T_i)^{0.68} \right) \times \lambda_3 \right\}}_{\lambda_{package}} + \left\{ \underbrace{\pi_I \times \lambda_{EOS}}_{\lambda_{overstress}} \right\} \right) \times 10^{-9} / h \qquad (2)$$

이러한 오동작을 방지하였다는 증거는 오동작 사례(Scenario)를 제시하고 이러한 경우 해결방안을 제시하고 해결 정도를 제시하게 된다. 이러한 사례는 (그림 3)과 같이 4가지로 구분이 된다. 중에 해결해야 할 사례는 2와 3이 되고, 2와 3의 경우의 수를 줄어 1 또는 4로 만들면 된다.

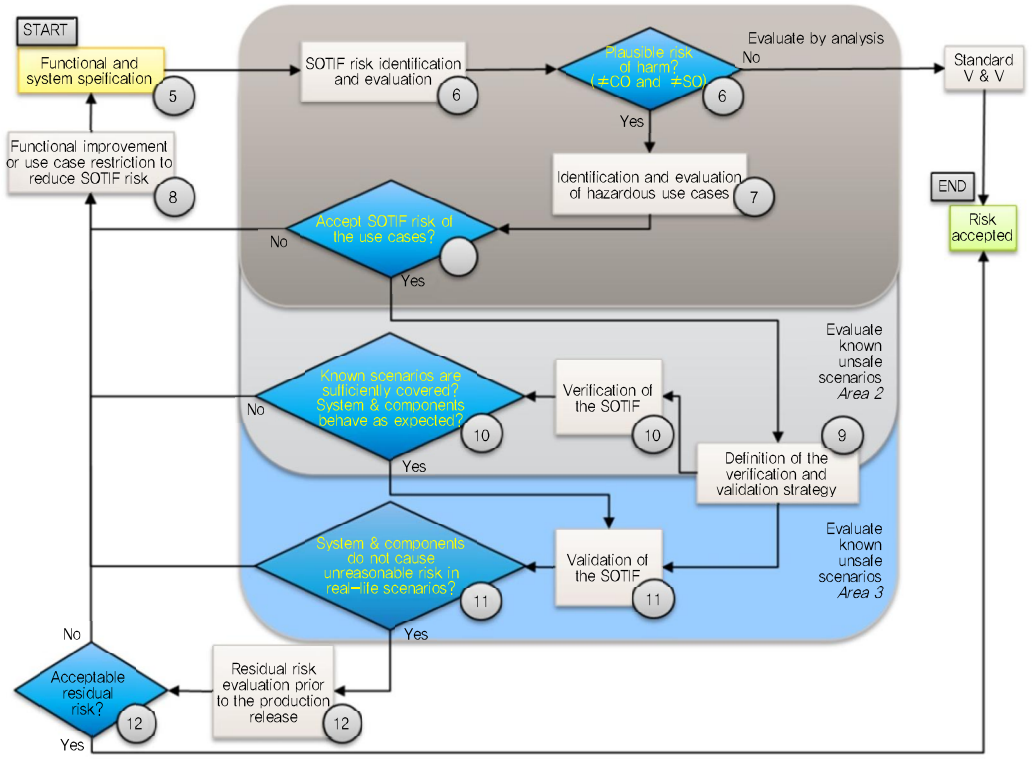



(그림 3) Known/Unknown Use Case 구분

[출처] Reprinted with permission from ISO/PAS 21448, "Road vehicles -- Safety of the Intended Functionality," ISO, 2019.

이를 위해 (그림 4)와 같은 SOTIF 활동을 통해 이룰 수 있다.

의도된 기능 또는 시스템 사양을 정의하고 이러한 사양에서의 가능한 SOTIF 위해(Risk)를 분석한다. 분석된 위해의 위험(Harm)을 Controllability와 Severity 분석을 통해 심각도가 높거나 제어력이 낮은 경우의 경우는 Use Case를 정의하고 이러한 Use Case의 SOTIF Risk 분석을 통해 Acceptance이면 Acceptance임을 검증 및 평가 단계에서 보이게 되고, 그렇지 않다면, 이러한 SOTIF 위해를 감소 및 제거하기 위해 기능 및 시스템 사양을 변경하게 된다. 이러한 사양 변경은 크게 네 가지로 나뉜다.




(그림 4) SOTIF 활동 순서도

[출처] Reprinted with permission from ISO/PAS 21448, "Road vehicles -- Safety of the intended functionality," ISO, 2019.

- SOTIF Risk에 의한 파급력을 줄이기 위한 시스템 성능 개선
- SOTIF Risk에 의한 파급력을 줄이기 위한 기능 제한
- 위험한 동작 상황에서 제어력을 개선하기 위해 시스템에서 운전자로 Handover
- 예상 가능한 오사용에 대한 효과를 줄이는 방법

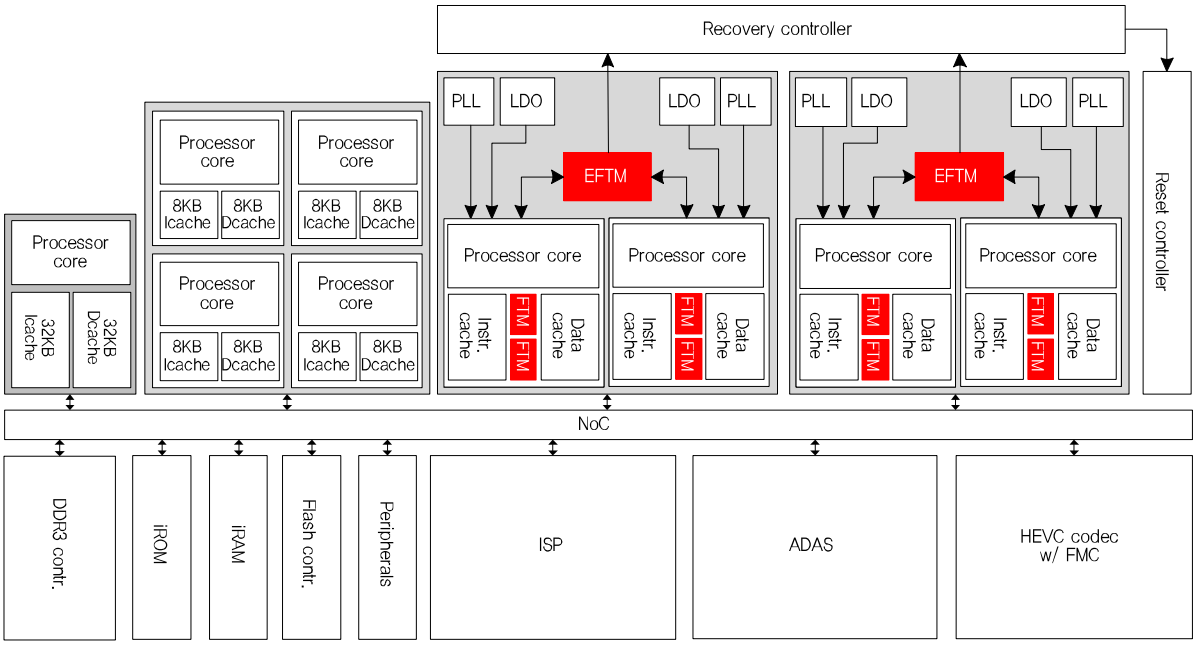
앞으로 자율주행차 전장시스템 또는 ADAS는 본 표준을 따라 위해 요소에 대한 분석이 되었음을 입증해야 할 것이다.

## II. 자율주행자동차 전장시스템을 위한 기능안전 프로세서 기술

그래서, 앞으로 자율주행차 전장시스템 또는 ADAS를 위한 반도체 프로세서는 앞에서 설명한 Autonomous System의 단계에서 Sense 단계를 제외한 나머지 단계를 처리하도록 설계가 되어야 한다. Perceive를 위해서는 센서 정보를 통해 인식할 수 있는 인지기능을 위한 하드웨어 IP가 있어야 할 것이며, Decide 및 Actuate를 위해서는 인지된 정보를 바탕으로 사전에 분류되어 있는 제어 분류 중 어떤 것을 할지를 결정해야 할 것이고, 결정된 제어 분류에서 필요한 Actuate를 위해 가동치를 결정하는 연산을 해야 할 것이다.

Vision 기반의 지능적인 운전 제어를 위한 차량용 프로세서는 물체 인식 기능을 위해 높은 연산 성능뿐만이 아니라 전력 효율성과 Programmability를 요구하고 있다[4]. Vision System은 높은 온도를 갖는 대기 안에 있는 Vehicle 안에 안전한 곳에 설치가 되어야 하므로 System Reliability를 위해 요구가 된다. 자동차, 오토바이, 차선, 장애물 등과 같은 시간과 날씨에 영향을 받아 그 모습이 변화하는 물체를 인식하기 위해서는 다양하고 복잡한 Image Recognition Algorithm이 필요하게 되고 계속해서 개발되어야 하기에 Programmability는 이러한 요구를 만족시키기 위해 많은 Execution Unit을 보유하는 기존의 Array Processor 기반으로 개발을 시도하는 경우도 있고[5], 한 번의 명령어로 많은 연산을 수행하기 위해 Very Long Instruction Word(VLIW) 명령어 기반 Processor로 개발된 사례도 있다[6]. 최근의 결과물에서는 앞에서 설명한 물체 인식 단계별로 필요한 Appli-cation Specific Processor를 기반으로 하는 Heterogeneous Multi-core Processor 구조로 많은 성능향상도 가져오고 있다[7]. 그러나 현재 자율주행에서 요구되는 영상 기반의 인지 Classification은 생각보다 간단할 수 있다. 보통 구분 및 인식이 필요한 것은 차량, 보행자, 신호등, 표지판 등이 될 수 있다. 그러나, 이를 기반으로 차량이 주행 경로를 운행할 때 충돌 등의 사고가 일어날 수 있는지, 보행자가 나의 차량에 충돌하여 인명사고가 일어날 수 있는지, 신호등을 보고 교차로를 지나갈 때 다른 차선의 차량과 충돌이 예상되는지 등의 사고 가능성(Risky)을 판단하는 일이 더 많게 된다. 즉, Perceive 기능뿐만이 아니라 나의 차량의 행동을 계산하여 Decide를 위한 처리 또한 많은 연산을 필요로 하게 된다. 이에 ETRI에서는 자율 주행을 위한 기능안전 프로세서를 (그림 5)와 같은 구조로 개발하였다.

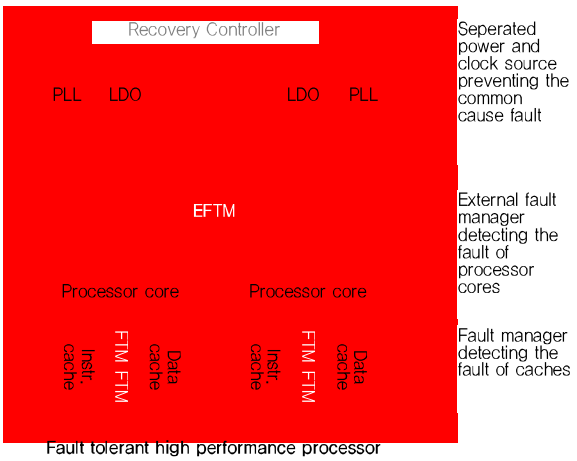
이는 최대 1GHz로 동작하는 RISC 아키텍처를 따르는 9개의 프로세서를 탑재하고 있으며, 이 중 기능안전 설계가 되어 있는 4개의 프로세서가 있다. 또한, 영상센서를 정보를 이용한 Perceive를 가속하기 위하여 ISP, ADAS 하드웨어 IP가 포함되어 있으며, 보안을 위한 영상 저장을 위한 HEVC 표준 기반 4K영상 크기의 압축, 해제가 가능한 Frame Memory Compression을 이용하는 High Efficiency Video Coding(HEVC) Codec이 포함되어 있다. 그 외에 센서 정보 입출력을 위한 Video Input Module(VIM), Video Output Module(VOM)이 있




(그림 5) 자율주행차를 위한 전장시스템을 위한 SoC 기능도

〈표 3〉 Autonomous System 기능 담당 칩 내 IP

| 자율주행차 전장시스템을 위한 기능 단계 | 칩내 담당 하드웨어 |
|---|---|
| Sense | ISP, VIM |
| Perceive | ADAS, 1 × processor |
| Decide | 2 × safety processor, 1 × processor |
| Actuate | 2 × safety processor, 1 processor |
| System Control, HEVC | 2 × processor, VOM |



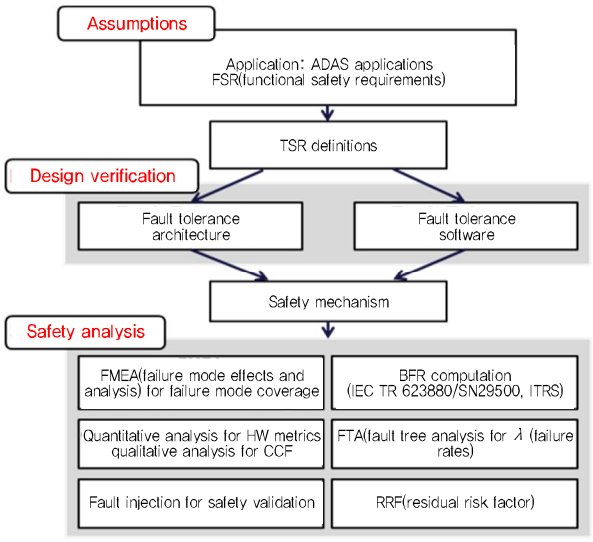

(그림 6) 기능안전 설계

다. 이러한 칩 구성은 아래와 같은 자율주행차 전장시스템 및 ADAS을 위한 기능을 모두 수행할 수 있다[〈표 3〉 참조]. 이를 통해 하나의 칩으로 자율주행차 전장시스템에서 필요로 하는 모든 기능을 수행할 수 있다.

또한, Decide, Actuate 단계에서의 결과는 기능안전 설계를 적용하여 ISO-26262 표준 규격에 맞게 (그림 6)과 같이 분석되었다.

기능안전 설계 사양은 Functional Safety Requirement(FSR)와 Technical Safety Requirement(TSR)로 정의되고, 해당 사양을 만족시키기 위해 반도체 내 프로세서는 (그림 7)과 같이 전원, Clock Source 분리, Dual Modular Redundancy(DMR) 기능을 통한 두 프로세서의 결과 오류 검출, 단일 프로세서 내에 캐시 오류 모니터링을 통한 검출 및 정정을 통한 기능안전 설계가 적용이 되고 이를 제어하기 위한 소프트웨어도 함께 코딩을 되었다. 이러한 기능안전 설계는 Failure Mode Effects and Analysis(FMEA) 및 정량분석(Quantitative Analysis)을 통해 안전 분석을 하였다.

이렇듯 자율주행 기능을 포함하는 자동차 전장시스템




Quantitative analysis of fault tolerant processor

$\lambda_{RF} = \lambda(1-F_S)(1-K_{FMC,RF})$

RF FIT rate, FIT rate, Fraction of safe fault, Diagnostic coverage = proportion of the hardware element failure rate that is detected or controlled by the implemented safety mechanisms

| Failure parts | Permanent | |
|---|---|---|
| | Single point faults metric (SPFM) | Lateny faults metric (LFM) |
| Core | 99.64% | 93.23% |
| Memory | 95.00% | 89.52% |
| Peripheral | 90.00% | 83.88% |
| PADs | 90.00% | 90.00% |
| SM | 93.83% | 87.88% |

(그림 7) ISO-26262 호환 Fault Analysis 순서도

은 기능안전 설계와 함께 센서 정보를 처리하여 자동차를 제어하기 위한 전 단계를 처리할 수 있는 반도체 프로세서를 요구하고 있기에 최근에는 Perceive, Decide 단계를 한꺼번에 처리할 수 있고, 인식률을 높일 수 있는 Deep Learning Algorithm을 가속할 수 있는 기능을 탑재한 기능안전 프로세서 설계가 요구되고 있다.

## Ⅲ. 시사점

자동차 분야에서 자율주행 기능에 필요한 요구사항을 만족하는 기능안전 프로세서에 대한 요구는 계속해서 증가하고 있다. 이런 요구사항 중 인지 및 결정을 위한 센서 정보 처리를 위한 프로세서는 아직 시장에 존재하지 않고 있으며 이러한 요구사항을 만족하는 프로세서를 기능안전 설계를 포함해서 개발이 필요하다.

또한, 인지 및 결정 기능을 통합하여 수행하는 악천 후등의 센서 정보가 부정확할 수 있는 요인이 많은 상황에서는 인식률을 저하를 막을 수 있는 Deep Learning Algorithm 활용하고 이를 가속 처리를 할 수 있는 자율주행차를 위한 Deep Learning Processor 개발이 필요하다.

## 약어 정리

| | |
|---|---|
| ADAS | Advanced Driver Assistant System |
| DMR | Dual Modular Redundancy |
| ECU | Electronic Control Unit |
| FCDA | Front Car Departure Alert |
| FCW | Forward Colision Warning |
| FMEA | Failure Mode Effects and Analysis |
| FSR | Functional Safety Requirement |
| HBA | High Beam Assist |
| LDW | Lane Departure Warning |
| LKA | Lane Keeping Assistant |
| PD | Pedestrain Detection |
| SOTIF | Safety of The Intended Functionality |
| TLR | Traffic Light Recognition |
| TSR | Technical Safety Requirement |
| TSR | Traffic Sign Recognition |
| VIM | Video Input Module |
| VLIW | Very long Instruction Word |
| VOM | Video Output Module |

## 참고문헌

[1] PLK Home page, plk.co.kr

[2] 안경환 외, “자율주행 자동차 기술 동향,” 전자통신동향분석, 제28권 제4호, 2013. 8, pp. 35-44.

[3] 한진호, 변경진, 엄낙웅, “자동차 비전 프로세서 동향,” 전자통신동향분석, 제30권 제4호, 2015. 8, pp. 102-109.

[4] ISO-26262, “Road Vehicle – Functional Safety,” ISO, 2011.

[5] U. Ramacher et al., “A 53-GOPS Programmable Vision Processor for Processing, Coding-Decoding and Synthesizing Of Images,” *Proc. Eur. Solid-State Circuits Conf.*, Aillach, Austria, Sept. 18-20, 2001, pp. 133-136.

[6] S. Kyo et al., “A 51.2-GOPS Scalable Video Recognition Processor for Intelligent Cruise Control Based on a Linear Array of 128 Four-Way VLIW Processing Elements,” *IEEE J. Solid-State Circuits*, vol. 38, no. 11, Nov. 2003, pp. 1992-2000.

[7] J. Oh et al., “A 320mW 342GOPS Real-Time Dynamic Object Recognition Processor for HD 720p Video Streams,” *IEEE J. Solid-State Circuits*, vol. 48, no. 1, Jan. 2013, pp. 33-45.