SPRi Issue Report
2017. 2. 24. (2016-016호)

자동차 산업의 SW안전 이슈와 해결과제

Software safety issue and challenges in automobile industry

진회승 (hschin@spri.kr)
박태형 (parkth@spri.kr)

SPRi 소프트웨어정책연구소

○ 본 보고서는 「미래창조과학부 정보통신진흥기금」을 지원받아 제작한 것으로 미래창조과학부의 공식의견과 다를 수 있습니다.

○ 본 보고서의 내용은 연구진의 개인 견해이며, 본 보고서와 관련한 의문사항 또는 수정・보완할 필요가 있는 경우에는 아래 연락처로 연락해 주시기 바랍니다.

- 소프트웨어정책연구소 SW안전연구팀 진회승 선임연구원(hschin@spri.kr)

《 Executive Summary 》

ICT 기술이 기존의 산업과 융합되면서, 새로운 제품과 서비스가 창출되고 있다. 융합의 결과로 유연하고 효율적인 제4차 산업혁명이 일어나고 있으며, 융합의 근간으로서 소프트웨어가 중요한 역할을 하고 있다.

자동차는 소프트웨어라고 할 만큼 자동차 산업에서도 소프트웨어의 역할이 커지고 있다. 커넥티드카와 자율주행차 등 자동차의 기능이 복잡해짐에 따라 하드웨어, 소프트웨어, 인터페이스도 또한 복잡해지고, 사고를 예방하고 분석하는 방법에 대한 소프트웨어 중심의 새로운 방향의 연구가 필요하다.

자동차에서 전장제품의 사용이 늘어나며, 소프트웨어의 재사용과 안전성을 위해서 소프트웨어 표준 플랫폼이 제정되고 확산되고 있다. 네트워크에 접속하여 신호체계, 다른 자동차 등에 연결되는 커넥티드카와 제어의 주체가 소프트웨어인 자율주행차에서 소프트웨어 안전은 자동차 안전의 중요한 요소이다.

자동차 사고 사례를 통해 소프트웨어가 자동차와 자동차 사고에 미치는 영향을 검토한다. 도요타 급발진 사고, 테슬라 자율자동차 사망사고, 구글 자율주행차 사고 사례를 검토하고, 사고 사례를 통한 교훈을 도출한다.

자동차 산업의 소프트웨어 안전 보장을 위해서 정부 주도의 소프트웨어 안전 관련 법제, 표준 및 지원 체계 정비, 소프트웨어 안전 검사 제도와 시설 지원, 사고 데이터를 확보하고 관리하는 체계 마련이 필요하다. 자동차 관련 업계에서는 표준을 정확히 이해하고 준수하는 노력이 필요하며, 소프트웨어 적용이 확대되는 자율 주행, 커넥티드카 분야의 안전관련 소프트웨어 기술 개발이 선행되어야 한다. 소프트웨어 안전 인력 양성을 위해서는 정보와 산학연이 연계하여 전문가 역량 제고에 노력해야 한다.

《 Executive Summary 》

As converging ICT technology and existing industries, new products and services are being created. As a result of convergence, a flexible and efficient the fourth industrial revolution is taking place, and software plays an important role as the basis of convergence.

The role of software in the automobile industry is growing that we can even assert automobile is software. As functions in connected cars and autonomous vehicles become more complex, hardware, software, and interfaces become complicated. To prevent and analyze accidents of software intensive systems, adoption of the new research methods focused on software is required.

As the use of ECU in automobiles has increased, software standard platforms for software reusability and safety have been established and become widespread. Software safety is an important attribute of automobile safety in autonomous vehicles in which software is the main controller. Also it is an important in a connected car which share internet access with other vehicles and other devices such as signaling systems.

We review the influence of software on vehicles and automobile accidents through analyzing automobile accident cases. Through study of automobile accident cases like Toyota sudden unintended acceleration, Tesla fatal autonomous car crash, and Google self-driving car accident, lessons are brought up.

To ensure the software safety of the automobile industry, it is necessary to establish software safety legislation, standards and support system, to support software safety inspection system and facility and to construct information sharing system that build and manage accident data in government. The automobile industry should accurately understand and comply with standards. Also safety skill for software should be developed in advance in autonomous driving car and connected car field in which software application is expanded. To enhance software safety expert competence, Government-Industry -Academic cooperation is necessary.

《 목 차 》

1. 연구 배경

□ 자동차산업에서 SW의 비중이 커지면서 기존과는 다른 형태의 사고 사례[1]가 늘어나고 있으며, 사고를 예방하고 대응하는 방안도 기존과는 다른 연구가 필요함

○ 자동차는 기존의 전통적 기능에서 자율 주행 등 새로운 기능이 추가되면서 SW 비중이 늘어나고 SW에 의한 고장도 증가

- 1998년에서 2001년 사이에 SW에 의한 차량 고장은 23%가 증가한데 비해, SW를 제외한 원인으로 인한 고장은 3% 증가함[2]

○ 자동차 산업에서 SW는 커넥티트카, 자율주행기능 등에 사용되어 안전을 강화시키는 방법으로 사용되기도 하고, 사고의 원인으로 작동하기도 함

- 각국 정부는 차량자세제어장치(ECS), 타이어공기압경고장치(TPMS) 등을 안전을 위해 단계적으로 의무화하고 있으며, 신차 안전도평가에서도 자율주행기술이 평가항목에 추가

- 자동차 사고 사례를 살펴보면 SW 오류가 새로운 사고 원인으로 부각

□ SW 안전 보장을 위한 정부, 산학연 연계 과제 도출과 실행 필요

○ SW가 사고의 원인이 되는 이유를 세밀히 검토하고, 사고를 예방하고 사고 시 대처하는 방안 마련

- HW, SW, 인터페이스 오류에 인한 복합적인 원인 분석이 요구됨

○ 소프트웨어 안전 확보를 위해서는 산업적 이익 논리에서만은 구현이 어려우며, 법제, 기술, 인력 등 다차원적인 지원

1) 구글 자율자동차 사고(2016.2), 테슬라 오트파일럿 기능 사용 중 사망사고(2016.5) 등
2) 백재진, 2011.3, 차량용 임베디드 소프트웨어 신뢰성평가 연구, 한국자동차공학회

2. 자동차 산업과 SW

□ (전장 부품) 자동차산업에서 전장[3] 부품의 사용 증가로 SW의 활용과 SW 안전의 중요성이 커지고 있음

○ 다수의 공급자가 제공하는 ECU[4]에 의한 SW가 다양화되고, SW 재사용, 안전성을 위해 AUTOSAR[5], GENIVI[6] 등 표준 플랫폼이 제정되고 확산되고 있음

- 차선유지 지원시스템, 자동 긴급제동시스템, 샤시[7] 통합제어시스템 등의 자율주행시스템을 가진 첨단 자동차로 발전되면서 부품의 전장화가 급격히 일어남
- 완성차 업체는 다양한 차량 모델에 ECU를 공통으로 적용하고, 부품 개발 업체는 원가를 낮추기 위해 부품을 여러 완성차 업체에 납품기 때문에 표준 플랫폼 필요
- AUTOSAR는 산업계 표준으로 사용하던 OSEK/VDX[8]를 기반으로 작성하였고, 재사용이 가능한 방법론을 제시하고 신뢰성을 제공할 수 있는 SW의 제작을 위한 SW 플랫폼 표준

○ ECU의 복잡도 및 오류가 증가하여 안전에 대한 중요성이 커지고 있음

- 최근 개발되는 고급 자동차의 경우 약 70여개 이상의 ECU를 사용하고, 1억 라인의 SW 코드를 사용[9]하여, ECU의 복잡도 및 오류 증가
- 자동차 안전 국제 표준인 ISO 26262[10]가 제정되었으며, 적용 범위 확장과 새로운 기술 적용을 위해 '18년을 목표로 2nd 버전을 만들고 있음

3) 전장이란 전기장치를 줄임말로 자동차를 위한 전기/전자, 반도체 부품를 말함
4) Electronic Control Unit 또는 Engine Control Unit라고도 함, 엔진 제어, 변속기, 차체 제어, 에어백 등 자동차의 내부 장치들을 컴퓨터로 제어하는 전자제어 장치임
5) AUTomotive Open System Architecture의 약자, 자동차 전장용 임베디드 SW 개발의 생산성 향상을 목표로 한 개방형 자동차 표준 SW 구조
6) Geneva In Vehicle Information의 약자로 차량 인포테인먼트(infotainment : information + entertainment)용 산업표준 SW 플랫폼, 2009년 유럽의 대표적인 자동차 회사, 반도체 회사, 자동차 부품사, OS 개발사를 주축으로 설립
7) 차체를 제외한 부분으로, 동력발생장치, 동력전달장치, 조향장치, 제동장치, 타이어 등 포함
8) OSEK OS는 선점형 멀티태스킹을 지원하는 운영체제이며, 응용 프로그램에 표준화된 인터페이스를 제공함으로써 HW에 독립적인 개발을 가능케 하며, 확장성과 안정성을 높임, 박미룡, 김재영, 자동차 전장 SW플랙폼 규격 표준화 동향, 2008.06
9) R.Charette, 2009.02, 'This car runs on code', www.spectrum.ieee.org/feb09/7649,
10) 자동차에 탑재되는 시스템 오류로 인한 사고 방지를 위해 ISO에서 제정한 자동차 기능 안전 국제 규격으로, 자동차 전체 시스템이 적용대상이며 개발 초기부터 생산, 폐기에 이르는 전체 생명주기에서의 안전 관련 사항을 관리(2011.11 초판 제정)

□ (커넥티드카) 커넥티드카는 운전자에게 엔터테인먼트와 편의성, 안전성을 제공함으로써 자동차 산업에서 점유율이 지속적으로 증가되고 있으며, SW의 활용을 증가시키는 분야임

○ 커넥티드카는 차량 내 엔터테인먼트 기능과, 모바일 정보 제공, 차량 제어 및 관리, 안전 기능, 운전 기능 보조 등을 제공해 운전자 및 탑승자의 편의성 및 안전성을 강화

[표 2-1] 커넥티드카의 기능

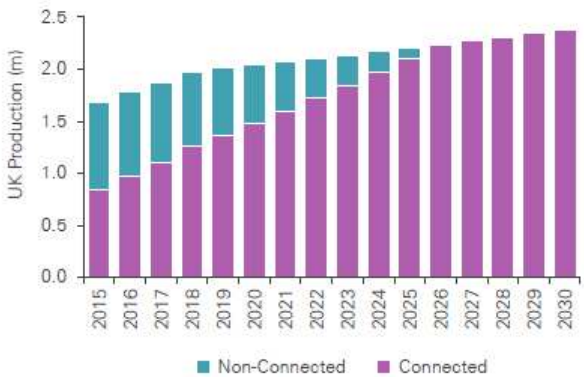
구분	세부 사항
모바일 관리	운전자를 빠르고 안전하게 목적지에 도착하게 하는 기능 ex) 현재 교통 정보, 주차 보조, 연료 사용량 검사
차량 관리	운행 비용 절감 및 사용상 편리성을 위하여 운전자를 도와주는 기능 ex) 자동차 상태, 원격 운행, 운행 데이터 전송
엔터테인먼트	운전자 및 승객에게 엔터에인먼트 제공 기능 ex) 스마트폰 연결, 음악/비디오/인터넷, 모바일 오피스
안전성	외부와 자동차 내부 위험원을 운전자에게 경고하는 기능 ex) 충돌 방지, 위험 경고, 응급 기능
운전자 보조	부분적 자율 운전 기능 ex) 주차 시나 고속도로 등에서 부분적 자율 운전 기능
웰빙	운전자에게 편안함을 제공 ex) 피로 인식, 의료 관련 보조

자료 : Strategy&(2014), In the fast lane, The bright future of connected cars

* 커넥티드카는 네트워크에 접속하여 스마트폰, 신호체계, 다른 자동차, 가전 등과 연결되는 차로 정의

○ 자동차 산업에서 커넥티드카의 생산량과 점유율은 급속히 증가할 것으로 예상

[그림 2-1] UK 커넥티드카 생산량 예측



<표 2-2> UK 커넥티드카 점유율 예측

년도	2015	2020	2025	2030
점유율 비율	50%	73%	95%	100%

자료 : KPMG(2015), Connected and Autonomous Vehicles-The UK Economic Opportunity

○ 일반 DB(지도, 교통), Big Data(위치 정보, 스마트 기기 연동 데이터 등), 운전자 관련 정보를 통한 차량 제어가 가능한 분야로 SW의 활용 요구가 증가되고 안전이 중요한 분야임

- HTMLS, 클라우드 서비스, SNS, MAP 서비스, 미디어 스트리밍 등 SW 관련 서비스와 플랫폼 사용[11)]
- 커넥티드카의 복잡한 기능을 SW로 구현해야하기 때문에 SW 안전 구현이 점점 어려워짐

□ (자율주행차) 안전성 제고, 새로운 이동 방법 제공을 위한 자율주행차는 제어의 주체가 SW가 되어 더욱 SW 안전이 중요하게 부각되는 분야임

○ 안전사고 예방, 고령자 등 교통약자에 대한 서비스를 위해 자율주행 기능이 적용된 자율주행차 필요성 도래

- 에어백, 안전밸트 등 안전장치 도입으로 교통사고 피해가 15~20% 감소된 것으로 보고 있으며, 일본 국토교통청 자료에는 자율주행차의 보급으로 승용차에서 교통사고 절감효과는 40%라고 전망[12)]

○ 자율주행차 개발의 촉진 기술인 긴급제동, 차선이탈경고, 전방충돌경고 등의 능동형 안전 시스템이 안전을 위해 도입

- 유럽은 '14년 차선이탈경고시스템(LDWS), 긴급제동시스템(AES) 장착 의무화 하는 등 법규 강화를 통한 시스템 장착 유도

○ NHTSA[13)]가 정의한 자율주행차 5단계에 의하면, 현재는 3~4단계 상태이며, 자동차의 주행을 부분적으로 SW가 제어하게 됨

11) 이재관, 2016.4, 스마트카 최신 동향 및 산업적 과제, 대한전자공학회 학술대회
12) 에이티씨, 2016.1, 글로벌 자율주행차 시장전망과 기술개발 참여업체 사업전략 1편-기술・시장편 p74
13) NHTSA (National Highway Traffic Safety Administration, 미국도로교통안전국)

- 2단계는 차선 유지 지원 시스템, 샤시 통합제어 시스템 등의 단일 기능을 제어하는 자동화 시스템
- 3단계는 2개 이상의 합쳐진 기능을 제어하는 자동화 시스템
- 4단계는 제한된 특정한 상황(고속도로 주행 등)에서 자율주행이 가능한 상태이며, 필요시만 운전자가 개입하는 상태
- 5단계는 완전 자율 주행이 가능한 상태임

○ 자율주행차의 점유율은 커넥티드카보다 작지만 점차적으로 늘어날 것으로 예상

<표 2-3> 자율주행차 시장전망

구분	2015	2020	2025	2030	2035
비율	0.0%	0.01%	4.4%	40.5%	75.1%

자료 : Aotonomous Vehicles (Navigant Research, Q3 2013)

○ 자율주행차 기술은 라이더, 영상센서 기반 주행상황인지 기술, V2X 통신 기술, 디지털지도 기술, 운전자 모니터링 기술, 재해 방지 기술 등이 있으며, 이러한 기술들에서 SW가 중요한 역할을 함[14)]

□ 자율주행차나 커넥티드카에서 보안과 더불어, SW 안전에 대한 확보방안도 이슈화되어야 함

○ 현재 자동차 사고 사례를 살펴보면 SW 오류는 자동차 안전은 물론 사회의 여러 산업의 안전에 위협이 될 수 있음을 확인[15)]

- SW 오류일 가능성이 크다는 판결이 난 도요타 급발진 사고
- 센서 오류로 추정되는 테슬라 자율자동차 사고
- 알고리즘으로 인한 구글 자율자동차 사고

○ 제품의 위험 분석 시 제품 안전에 SW 역할의 중요성을 인식하고, SW 안전 구현을 위한 방안 마련이 필요

14) 이재관 자동차 부품연구원, 2015.8, 자율주행자동차 동향과 전망, 융합연구정책센터
15) 상세 설명은 3장 SW결함으로 인한 사고 사례 참조

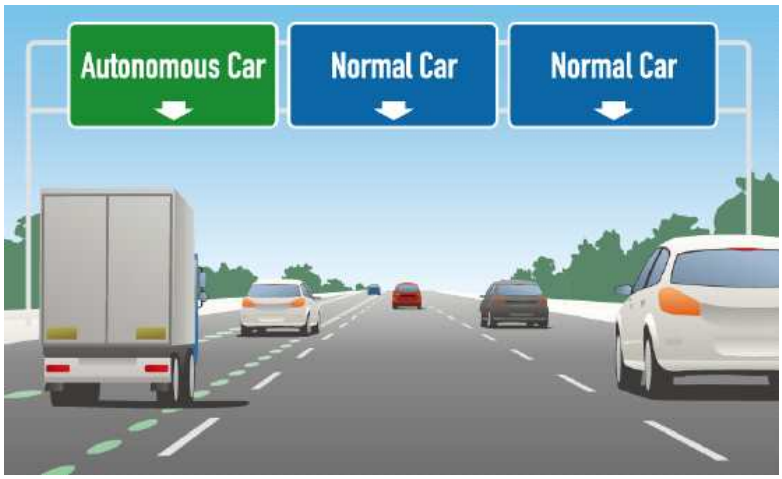
- SW 안전이 중요한 제품을 만드는 기업과 사용자들이 SW 안전에 대한 의식을 높여야 함

- SW 안전을 보장하기 위해서는 법제 정비, SW 안전 기술 발전, 데이터 확보 등 SW 안전 보장 체계가 구축되어야 함

○ 우리가 생각하는 것보다 빠르게 새로운 기술이 나오고 적용되고 있으며, SW안전에 대한 대책 마련이 시급함

- '16년 9월에 나온 리포트에 의하면 교통 정체를 줄이고 운전자 편의를 위하여 시애틀과 벤쿠버 구간에 자율주행차 전용 도로를 만들자는 제안이 나옴16)

[그림 2-2] 자율주행차 전용도로



자료 : Tom Alberg 외(2016), Autonomous Vehicle Plan for the I-5 Seattle/Vancouver B.C. Corridor

16) Tom Alberg 외, 2016.9. Autonomous Vehicle Plan for the I-5 Seattle/Vancouver B.C. Corridor

SW안전이란?

□ SW안전이란 전체 시스템의 안전 보장을 위하여 외부에 미치는 위험 요소를 분석하고 제거하여 SW의 오류로 인한 사고를 예방하는 것

○ SW 안전 요소에는 안전공학(예 : 자산, 사고, 위험, 약점)과 요구공학, 아키텍처(예 : 안전 체계 및 기술)가 포함되어 있으며, 각 요소의 상호 작용에 의한 안전 구현

- 안전을 구현하기 위해서는 안전 목적과 정책을 기반으로 위험을 제거할 수 있도록 안전 요구사항을 설정해야 함
- 안전 요구사항은 안전 체계 및 기술에 의해 달성되어야 하며, 안전 요구사항이 달성됨으로써 위험에서 HW, SW, 데이터의 위험을 제거하여 시스템이 안전하게 됨

□ SW 안전에 대한 중요성 인식이 SW 안전 확보에 가장 기본적인 단계

○ 안전이 중요한 시스템(항공, 자동차, 철도 등)에 SW가 점점 더 많은 부분을 차지하게 된다는 사실을 인식

○ SW 안전은 단일 시스템뿐만 아니라 CPS(사이버물리시스템, Cyber Physical System) 등 네트워크로 연결되는 시스템이 확장됨에 따라 사회 전체 시스템에 영향을 줌

□ SW 안전 구현을 위해서는 위험분석이 중요하고, SW 안전 체화가 필요

○ 시스템의 안전 구현을 위해서는 개발 프로세스에 따라 기획부터 시스템의 오작동에 의해 발생할 수 있는 위험을 분석하고 관리하여, 시스템을 구현되어야 함을 인지

- 수용 가능한 시스템의 안전을 보장하기 위해 위해도 분석 및 위험 평가 수행하고, 인지된 위험은 기획 단계부터 운영 단계까지 추적하여 제거하고 관리되는 것이 필요
- 인지된 위험은 위험의 확률 및 영향의 심각성에 따라 분류하고, 분류된 등급에 따라 위험을 방지할 수 있는 방법을 결정해야 함

○ 안전 특성 때문에 SW 안전 확보를 위해서는 SW 안전에 대한 체계적, 지속적, 반복적 교육이 필요

- 안전을 중요하게 생각하는 인식의 전환이 필요하며, 이를 위해서는 단순한 기술습득 차원을 넘어선 지속적 교육 차원의 접근 필요
- 안전 문제에 제대로 대응하기 위해서는 전체 시스템 구현 프로세스 이해와 동시에 시스템 관련 분야에 대한 기술(관련 도메인 기술, 관련 표준 등) 습득 필요

3. SW 결함으로 인한 사고 사례

(1) 도요타 급발진 사례

□ 자동차 급발진 사고[17]는 해가 거듭될수록, 신규 제작 차량일수록 늘어나며, 원인 규명이 쉽지 않음

[그림 3-1] 자동차 급발진 신고 접수

발생 년도	건수
2010	28
2011	34
2012	136
2013	139
2014	113
2015.7	32
계	482

제작 년도	건수
2000 이전	17
2001 ~05	62
2006~10	195
2011~14	201
2015	7
계	482

자료 : 교통안전공단 제출(2015), 강동원 의원 보도 자료

○ 급발진 사고의 원인으로 지금까지 알려진 것은 운전 조작 미숙, 차체 결함, 자동차 매트의 영향, SW 오류 등임

○ 급발진 사고 방지 방법은 브레이크를 밟은 상태 시동, 가속페달 장치 변형 금지, 계기판 엔진 체크 경고등 소등 후 시동 등이 있으나, 시스템적 방지 방안 마련이 필요

□ 도요타 급발진 사고는 SW가 사고 원인으로 알려졌으며, 도요타에게 총 40억 달러의 손해를 준 사건

○ 2002년 생산 차량부터 엔진가속장치와 스로틀[18] 연결을 전자 제어로 변경한 후에 급발진에 대한 신고가 급증

○ 미국 고속도로교통안전청(NHTSA)[19]이 NASA NESC[20]에 2005년 캠리 모델

17) 급발진 상태는 자동차의 가속이 운전자의 의지에 따라 일어나지 않는 상태임
18) 기화기 아랫부분에 설치되는 장치. 가속 페달 위치에 따라 밸브를 개폐하여 실린더에 들어가는 공기와 연료의 혼합 가스량을 조절함으로써 엔진의 회전 속도를 변화시킴
19) National Highway Traffic Safety Administration

에 대해 급발진 사고 조사를 의뢰하였으나, 자동차 급발진이 전자제어 장치와 무관하다고 발표

○ 그러나 북아웃(Bookout) 소송에서 급발진 사고의 원인이 SW적 요인이라고 밝혀져 도요타는 총 40억 달러의 손해를 입음

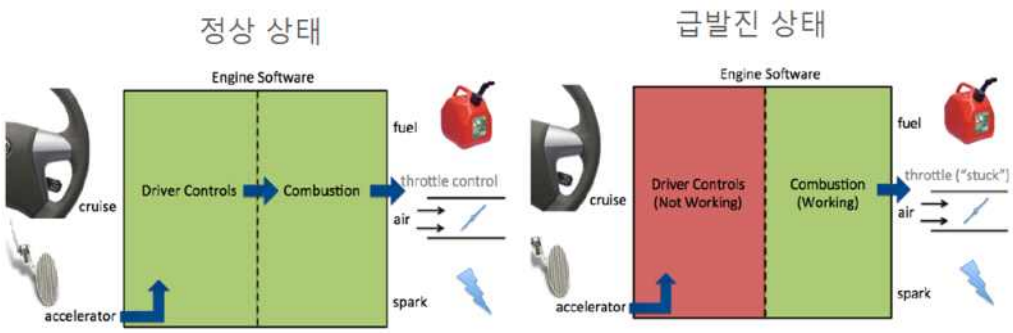
- 북아웃 소송은 2007년 일어난 사고로 운전자는 중상, 동승자 1명이 사망한 사고로, 2012년 1월부터 15개월간 임베디드 SW 전문 Barr 그룹이 조사하여, SW의 문제를 밝혀 냄

- 도요타는 미국 법무부에 12억 달러의 벌금과 338건의 급발진 소송 합의, 1천 200만대 리콜 등 총 40억 달러의 손해를 입음

□ 급발진 사고에 대해 NASA는 ETCS(전자식 연료분사 제어장치)[21]를 심층 조사한 후, 안전장치가 설계되고 ETCS 고장이 없으며 SW 오류가 없다고 발표했으나, 시스템이 복잡하여 증명이 어렵다고 함[22]

○ 운전자의 제어에 의해 가속 페달, 정속주행 장치가 작동하고, 연료와 공기가 주입되어 연소가 일어나야 정상상태인데 반해, 급발진 상태는 운전자 제어가 아닌 다른 이유에서 연소가 일어나는 상태임

[그림 3-2] 자동차 급발진 상태



자료 : Michael Barr(2013), Bookout V.;참고 Toyata 2005 Camry L4 Software Analysis

20) NASA Engineering and safety Center, NASA의 고위험 프로젝트의 안전과 임무 성공을 보장하기 위해 독립적인 테스트, 분석 및 평가를 수행, 외부 기관의 요청에 의한 기술 지원 수행

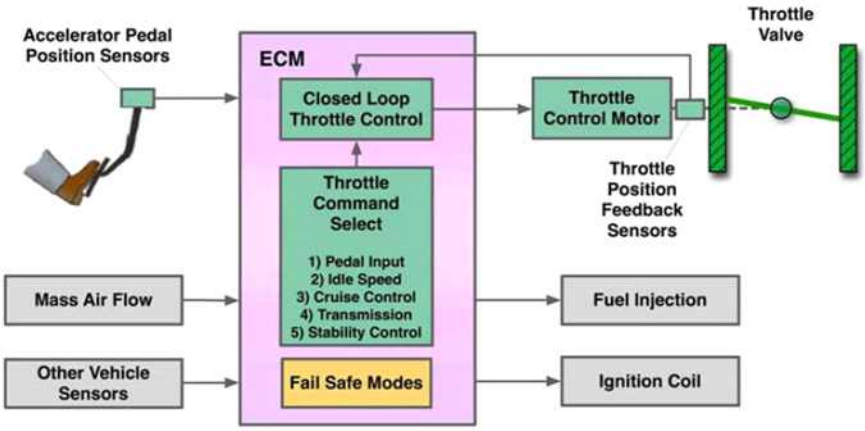
21) Electronic throttle control system, 전자식 연료분사 제어장치, 가속 페달을 스로틀에 전자적으로 연결하여 기계적 연결 장치를 대체하는 자동차 시스템

22) NASA NESC Technical Assessment Report, 2011.1, NHTSA Toyota Untended Acceleration(UA) Investigation pp. 170~172, pp. 20, pp. 13~16, pp. 147~152, pp. 169, pp. 54

○ NASA는 툴과 논리 분석을 이용하여 소스코드 분석을 시행하고 메모리 이중화에 대한 검토를 하였으나, ETCS가 급발진사고를 야기할 수 있는 SW 오류를 찾아내지 못함 23)

- ETCS는 페달의 위치 센서와 다른 센서들의 신호에 의해 연료와 스로틀 밸브를 제어함

[그림 3-3] 도요타 ETCS-i



자료 : NASA NESC Technical Assessment Report(2011), NHTSA Toyota UA Investigation

- 스로틀 오픈이 소프트웨어 오류에 의한 것인지 확인하기 위해 두 개의 가설을 세웠으나, 가설이 맞음을 증명하지 못함

- 첫 번째 가설은 페달 위치 확인 시스템과 CPU SW 버그의 결합, 두 번째 가설은 Main CPU 기능 오류로 세움

□ 그러나 북아웃(Bookout) 소송에서 BARR group에 의해 급발진 원인이 bit-flip[24]에 의해 일어난 SW 오류라고 밝혀짐[25][26]

○ 급발진 사고는 메인 OS의 프로세스를 관리하는 중요 변수가 바뀜으로써 사용자 의도와는 상관없이 스로틀 기능이 잘못 작동하여 일어남

23) 상세 설명은 별첨1 참조
24) 랜덤 액세스 메모리 또는 다른 매체에 저장된 비트의 메모리 오류 또는 소프트 오류, 0에서 1로 또는 그 반대로 의도하지 않은 상태 전환
25) Michael Barr, 2013.4, Bookout V. Toyata 2005 Camry L4 Software Analysis
26) 상세 설명은 별첨1 참조

- 방사선 등에 의해 반도체 오류를 일으켜 메모리의 변수가 변경될 수 있으며, 변수 변경에 의해 프로세스가 죽음
- 프로세스가 제대로 실행되지 않아 가속페달과 정속 주행시스템이 스로틀을 제어할 수 없게 되어, 스로틀 제어 시스템이 사용자의 의도와는 다르게 작동함

○ 소스코드는 스파게티코드[27], 리커전(Recursion)[28]에 의한 스택 오버플로우(메모리 문제) 등의 문제로 시스템 안전에 문제를 일으킬 수 있음

- 너무 복잡해서 이해하기 어려운 코드를 작성하여, 오류 생성 가능성이 커지고 안전 검증도 어려움
- MISRA-C의 규칙에 위배되는 리커젼을 사용함으로써 스택 오버플로우의 문제가 있음

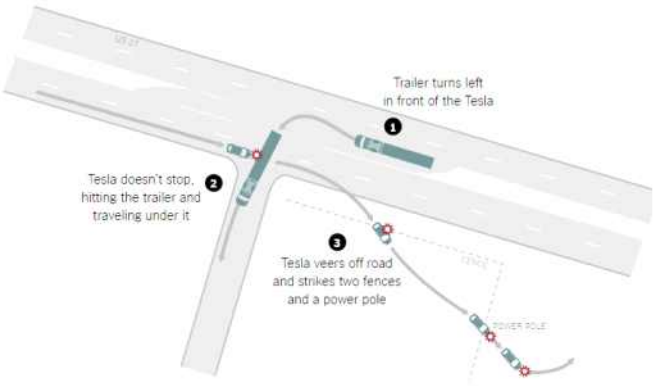
27) 의미없는 GOTO 문을 사용하고, 너무 복잡해서 이해하기 어려운 코드
28) 재귀함수, 수학이나 컴퓨터 과학 등에서 자신을 정의할 때 자기 자신을 재참조하는 방법, 이해하기 쉽고 코드가 간단하나, 함수 호출로 인한 오버헤드가 있어 스택 오버플로우의 위험이 있음

(2) 테슬라 자율자동차 사례

□ SW에게 자동차의 제어를 부분적으로 위임하는 테슬라의 모델S의 자율주행 중, 미국 플로리다 주에서 운전자 첫 사망사고 발생(2016년 5월)

○ 테슬라 차량은 자율주행모드 '오토파일럿' 기능이 좌회전 중이던 대형 트레일러를 식별하지 못하여 해당 차량과 충돌하여, 운전자가 사망함

[그림 3-4] 테슬라 차량 사고 경위



자료 : The New York Times(2016.7.12.) ;Florida traffic crash report

- 사고 당시 알려진 사고원인은 차량의 자율주행 센서가 파란색의 하늘과 백색의 트레일러 옆면을 구분하지 못하여 충돌한 것으로 파악
- 오토파일럿을 사용하면 자동으로 차선이 유지되며, 방향지시등을 가볍게 두드리면 차선 변경 가능함. 다른 차량이 많은 곳에서는 능동형 트래픽 크루즈 컨트롤을 이용하여 속도 조절 가능함
- 테슬라는 오토파일럿 기능을 사용 중 운전자의 전방 주시 의무를 강조

[그림 3-5] 트래픽 어웨어 크루즈 컨트롤, 오토스티어

자료 : 테슬라 홈페이지

○ 미국 고속도교통안전청(NHTSA)이 사고 원인을 조사한 결과 AEB(Automatic Emergency Braking), 오토파일럿 등 SW에 안전 결함을 찾을 수 없다고 발표[29)]

[그림 3-6] 테슬라 사고 차량

자료 : NTSB Preliminary Report Hoghway HWY16FH018, Florida Highway Patrol

- NTSB(연방교통안전위원회)[30)]의 예비조사 결과에 의하면 사고차량은 제한속도 이상의 과속 중이었으며, '오토파일럿' 기능을 사용함
- 차량 여러 전자 시스템의 데이터를 분석한 결과, "테슬라 자율주행 SW인 '오토파일럿'에 안전 문제가 발견되지 않았다" 며 조사 종결
- 시스템의 설계 및 성능 결함은 발견하지 못했으나 안전 관련 결함이 존재하지 않다는 증명은 못하며, 사건을 계속 모니터링 할 것이라 함

○ 테슬라는 자율주행 중 첫 사망사고라고 인정하지만, 자율주행의 안전을 주장

- 미국에서 운행되는 기존의 차량은 주행거리 1억 5100만km당 1건의 사망사고 발생했으나, 테슬라 자동차 무사고 자율주행 운행거리는 총 2억 900만 km라는 점을 근거로 주장

□ 테슬라는 사고 후 오토파일럿 작동 방식을 안전을 강조하는 방향으로 변경

○ 이미지 처리 보조 역할을 하던 레이더를 물체 인식을 위한 주된 수단으로 변경

- 사고 시 카메라가 인식하지 못한 흰 트럭을 레이더는 인식가능하며, 안개 낀 날 같이 앞이 잘 보이지 않을 때도 인식이 가능하다고 설명

○ 오토파일럿 모드로 주행 중 운전자가 핸들을 잡으라는 경고를 1시간 이내에 3차례 무시했을 때, 오토파일럿 시스템이 저절로 해제됨

29) NHTSA ODI Resume PE 16-007, 2017.1, Automatic vehicle control systems
테슬라 모델 S 첫 사망사고 "차량 안전 결함 없어" NHTSA 조사, http://www.itworld.co.kr/news/103113

30) National transportation Safety Board, 미국의 모든 민간 항공 사고와 철도, 고속도로, 해상 운송 등 운송 수단의 중대한 사고를 조사하기 위해 의회가 위탁한 독립적인 연방 기관

□ 테슬라 모델S 화재사고 등 관련 사고가 여러 나라에서 아직 알려지지 않은 원인으로 발생

○ 2016년 1월, 노르웨이 전기차 급속 충전소에서 운전자가 충전플러그에 소켓을 꽂다가 불꽃이 튀어 화재 발생

○ 2016년 2월, 캐나다 토론토에서는 비충전 상태에서 화재가 발생

○ 2016년 8월, 프랑스 남서부 비아리츠에서 시승 행사 도중 화재 사고가 발생

- 화재 발생 전 여러 차례 폭음이 들렸고, 정보표시 화면에 '충전에 문제가 발생했다'는 경고 문구를 봤다고 증언

○ 2016년 8월, 중국에서 고속도로에 불법 주차된 차량과 충돌하는 오토파일럿 운행 중 두 번째 사고 발생

○ 2016년 9월 네덜란드에서 사망사고 일어났으나, 오토파일럿을 쓰지 않았음

□ 테슬라 사고 이후 자율주행차 시험을 포함하여 안전을 위한 각국의 대응이 다르며, 산업발전과 안전의 두 가지 목표를 동시에 달성할 수 있는 방안 도출에 노력

○ 미국의 경우는 불완전한 기술에 대한 규제 목소리보다 오히려 더욱 기술적으로 완벽한 자율주행차를 개발해야 한다는 여론 발생

○ 중국정부는 테슬라 사망 사고 이후 자율주행 기능의 위험성을 우려하여 자율주행 차량을 통제할 수 있는 가이드라인이 완성되기 전까지 고속도로에서 자율주행차 시험 주행 금지 명령 내림[31]

○ 한국은 테슬라 전기자동차가 충전기 호환성과 한국 도로 환경에 맞는 오토파일럿 실험에 초점을 맞춘 한국 도로 주행 테스트 시작했으며, 한국 도로 상황에 맞추려면 SW 수정이 상당 부분 필요할 것으로 전망[32]

31) 중 정부, 고속도로서 자율주행차 테스트 금지, http://www.autoview.co.kr/content/article.asp?num_code=59194 2016.7

32) 전자신문, 2016.8, 테슬라 전기차, 한국 도로테스트 들어갔다. http://www.etnews.com/20160822000429

(3) 구글 자율자동차 사례

□ 2016년 2월, 미국 캘리포니아 주에서 구글의 자율주행차가 SW에 의해 제어되는 자율주행 기능의 과실로 첫 사고가 남

○ 우측 차로에서 우회전을 준비하던 구글 차량이 갓길 모래주머니를 피하려고 왼쪽으로 차선을 변경하다 옆 차선에서 주행하던 버스와 접촉[33)]

- 사고 원인은 속도를 늦출 것이란 자율주행 차량의 판단과 달리 버스가 주행속도를 유지했기 때문임

[그림 3-7] 구글 자율주행차 사고

자료 : JTBC 홈페이지

○ 구글의 자율주행 차량은 도로교통법을 엄격하게 지켜 도로 흐름을 방해한다는 지적 때문에 사람의 운전습관을 따라하도록 자율주행 기능 알고리즘을 변경하여 사고 유발

□ 구글은 자율주행차 시험 주행 시 자율주행차의 안전성에 대한 여러 관점의 테스트 수행

○ 구글은 최근 6년간 자율주행차로 330만 km를 주행하면서 작은 사고 17건을 겪었으며, 이는 구글 자율주행차의 과실이 아니라고 발표

33) Google Self-Driving Car Project Monthly reports, 2016.2 ;
구글 자율차, 330만km 주행 첫 판단 미스 사고
http://news.jtbc.joins.com/article/article.aspx?news_id=NB11184061

○ 구글의 시험운행은 아직은 자율주행이 위험하다는 것을 알려주나, 위험 상황 개선을 위한 노력을 계속하고 있음

- 구글은 시험운행을 통해 교통 흐름, 보행자 행위, 예측하지 못했던 상황에 운전하는 방법에 대해 학습하며, 위험한 상황일 경우는 수동 모드로 전환하여 위험 방지

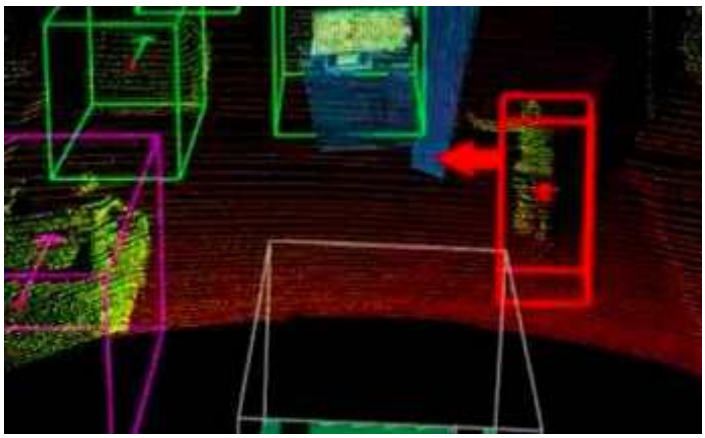
- 자율 주행 약 200만 마일, 수동 모드 약 120만 마일로 시험운행 중 38% 가량이 수동 모드를 사용한 점은 아직도 자율주행을 위한 학습 중이며, 자율 주행으로 운행하기는 위험한 상황이 있다는 것을 시사하고 있음

[그림 3-8] 200만 마일 자율주행 모드 주행

자료 : Google Self-Driving Car Project Monthly Report, 2016.9

- 반면 자율주행차는 인간의 300년 운전 경험을 가지고 있으며, 자전거 운전 등 위험한 상황에 대한 테스트를 하고 있을 강조

[그림 3-9] 자전거 운전자의 수신호 감지



자료 : Google Self-Driving Car Project Monthly Report, 2016.6

(4) 사고 사례를 통해 본 교훈

□ 급발진 사고 원인 규명은 쉽지 않으며, 사고기록장치(EDR)[34] 장착 등을 통한 원인 규명의 노력이 필요함

○ 기술의 급격한 발전에 의한 새로운 오류가 출현하고, 사고의 원인이 SW 요소 하나의 원인이 아닌, HW, SW, 자동차 도메인 특성 등 복합적인 원인으로 규명이 쉽지 않음

- 기술의 급격한 발전에 의해 새로운 오류가 출현하고 그 오류의 위험원도 물리적(예 :칼, 전기), 화학적(예 :벤젠, 석면), 생물학적 위험 요인으로 인식되었던 지금까지의 경향과 달라 원인 파악이 어려움
- 시스템 위험원은 HW, SW (예 :디자인 오류, 호환성), 인터페이스(예 :입출력 오류, 예상치 못한 복합성), 기능, 환경(예 :날씨, 외부 장치) 오류가 있음
- 시스템 오류의 원인은 복합적이라서 원인 규명이 어려움

○ 사고의 원인규명을 위해 EDR 장착 등의 법적, 기술적 지원이 필요함[35]

- 미국의 경우는 2012년 9월부터 EDR의 장착이 의무화 됨
- EDR에 대한 법규는 자동차관리법(제30조의 2)에 포함되어, 차량에 EDR을 장착한 자동차제작·판매자 등은 EDR기록내용을 요구하는 경우 기록정보를 15일 이내에 의무적으로 제공해야 함[36]

  * EDR에 표시되어야 하는 정보는 자동차 속도, 제동페달 작동 여부, 에어백 전개 시간 등 필수 정보 15개와 엔진회전수, 제동장치(ABS) 작동 여부진행방향 가속도. 등 선택 정보 30개가 있음

- EDR의 정보 공개는 제작자의 일방적 제공이 아닌 미국의 규정과 같이 소비자의 자유로운 검색 보장 필요
- EDR 정보에 사고 원인 규명 취지에 맞도록 필요한 기록정보가 추가되고

34) Event Data Recorder, 초기 에어백의 작동상태 모니터링과 성능평가 진단을 위해 일부 차량에 도입되어 적용되었는데,GM에서는 에어백 감지시스템(SDM : Sensor Diagnostic Module)을 적용하면서 사고 전의 운행정보(5초 정도)와 충돌정보를 보다 상세히 기록하기 시작

35) 윤대권, 김용현, 2014.8, 국내 자동차 사고기록장치의 법규 동향, 한국자동차공학회

36) 요구 가능한 자는 자동차 소유자, 소유자의 배우자. 직계존속(직계비속), 사고 자동차의 운전자, 운전자의 배우자. 직계존속(직계비속), 국토교통부장관, 성능시험대행자 등으로 한정

수정되어야 함

* 급발진을 확인할 수 있는 스로틀밸브 및 가속페달 변위는 둘 중 하나만 기록되고, 브레이크 압력은 수치 없이 on/off만 기록되어 원인규명에 어려움

□ 안전 확보를 위해서는 시스템 위험 분석 및 고장 분석을 통하여 그에 따른 시스템 제어를 위한 안전 기술 구현이 필요

○ 시스템에 맞는 위험 분석 기술을 사용하여 위험 분석 및 관리

- FTA(Fault Tree Analysis), FMEA(Failure Mode and Effect Analysis) 등의 수십 년 전에 개발된 고전적인 위험 분석 방법이 많이 쓰이고 있음
- 사고 발생의 원인이 선형적이지 않고 비선형적 요인이 서로 작용하여 사고가 발생하므로 STPA(System Theoretic Process Analysis)[37] 등 상호 작용을 분석하는 방법 사용이 필요

○ 안전 구조의 구현은 시스템의 정확한 분석에 따른 구현이 필요하며, 이를 위해서는 안전 작동방법 기술과 함께 도메인 지식이 필수임[38]

- 도요타 ETCS를 분석하면 CPU가 이중화 되어 있으나 입출력 데이터 처리의 이중화가 잘 못 구현되어, 운전자 가속 패달 사용 여부를 제대로 인식하지 못함

○ 기존 자동차와 자율주행 자동차의 안전을 위해 재해 방지 기술(Fail Safe[39], Fail Operational[40]) 의 정확한 구현이 요구됨[41]

- 기존 자동차는 물론이고 특히 자율주행 자동차의 경우, 자동차 장애 발생에도 자동차의 사고로 진행되지 않고, 장애를 감지하고 처리할 수 있는 기능 구현이 필요

37) 시스템 이론을 기반으로 시스템의 안전성을 분석하는 기법으로, SW, HW 이외에도 사람, 환경 등의 요소와 같이 시스템의 개발과 운영과 관련된 모든 요소들을 모델로 표현하여 위험을 분석하는 기법
38) 상세 설명은 별첨2 참조
39) Fail Safe는 시스템 고장 발생 시 일정기간 기능을 계속하는 것이 가능한 상태로 재해까지 진행되지 않도록 함
40) Fail Operational은 장애가 발생 시, 장애를 감지하고 중복 등의 적절한 방법을 사용하여 계속 정상적으로 작동하도록 하는 방식으로 자율주행차의 안전보장에 중요한 기능임
41) 상세 설명은 별첨2 참조

□ 자율주행차의 안전 이슈에 대한 정밀한 검토와 해결 방안 마련에 노력이 필요

○ 테슬라 사고 사례의 경우 자율주행에 대한 사고 원인을 밝히기가 쉽지 않은 것이 현실이며, 급발진 사고의 경우(EDR 의무 장착 및 정보 공개)와 같이 자율주행차도 사고 시 원인을 밝힐 수 있는 정책적 방안이 마련되어야 함

○ 사고 후 해결보다는 자율주행차 개발 시 안전에 대한 고려가 필요하며, 업체에서 시행하고 있는 자율주행차 검증 실험에 맡기는 것보다는 정부차원의 자율주행차 안전 검증에 대한 방안 마련이 선행되어야 함

- 구글의 경우는 2009년부터 시험주행을 시작하고, 2015년 5월부터 매월 테스트 리포트와 사고기록 공개

- 사고 후 미국은 자율주행차 가이드라인을 마련하고 자율주행차 안전 기술 개발에 노력 중임

□ SW 안전을 고려할 때 전체적인 사회 시스템 내에서 시스템 안전을 검토해야 함

○ 자율주행차의 경우는 도로상에서 다른 운전자가 운행하는 자동차와 같이 운행이 되므로, 다른 운전자의 운행 상태를 고려해야 함

- 구글 자율주행차는 버스가 속도를 줄일 것으로 예측하고 운행하여 사고를 일으킨 예와 같이 자동차의 흐름을 방해하지 않으면서, 사고를 방지할 수 있는 방안을 고려해야 함

○ 테슬라의 자율주행차 사망사고에서 보듯이 현재 자율주행시스템이 완벽하지 않음을 강조하고, 운전자의 주의의무를 강조하고 교육하는 것이 필요

4. 자동차 산업의 SW안전 확보를 위한 과제

□ 자동차 산업에서 SW 안전 보장을 위한 SW 안전 관련 법제, 표준 및 지원체계 정비

○ 자동차 SW 안전 관련 법제 마련을 통해 SW 안전 확보

- 자율주행기능 등 소프트웨어에 의한 사고에 대한 법적 책임 이슈 해결

  * 센서나 소프트웨어로 인한 사고의 경우 사고 처리 방안

- 글로벌 시장의 자동차 관련 안전 규제에 선제적 대응을 위한 정책 마련

  * 안전 보장과 동시에 기술개발을 통한 산업발전에 도움이 되는 법제 예제

[그림 4-1] 주요국의 의무 자동차 안전 기능 법제 현황

Safety measure	2011	2012	2013	2014	2015
ESC	USA, EU		Japan, Korea		
TPMS	USA		Korea	EU	
Rear-view camera		USA			
Smart pedal					USA
AEB			EU	Japan	Korea

자료 : Daiwa(2015), Smart cars :who has the head start? Pan-Asia Autos

ESC :Electronic stability control, TPMS :Tire Pressure Monitoring System, AEB :Autonomous Emergency Breaking

○ 안전을 보장하고 산업을 발전시킬 수 있는 자동차 SW 안전 표준화 지원

- 정부에서 국제 표준 제정에 적극 참여하여, 자국 산업에 이익이 되는 표준 설정

  * 안전 선진국은 ISO 26262(자동차), IEC 62279(철도), DO-178C(항공) 등의 기능 안전성 국제 표준을 만들어 무역에 있어서 기술 장벽으로 사용

  * ISO 26262 2nd 버전에서, 대상을 버스와 트럭 등으로 확대하고, 반도체, SW 안전 분석, 보안, 자율주행자동차 기술 등의 사항을 고려하고 있음[42)]

- SW 안전 표준에 대한 이해 및 적용을 위한 교육 지원

○ 국제 표준이 정립되지 않은 자율주행차 분야의 안전 가이드라인 마련

- 자율주행차의 경우 자동차 제어권이 소프트웨어에 있어 소프트웨어

42) Vector, 2015.5, Safety and Security for vehicles-best practices, vector UK Conference; 고병각, 2015.3, ISO 26262 2nd edition 현재 이슈사항, KTL

안전에 대한 대책 마련이 필수임

* 미국 정부는 15개 안전과 관련된 사항을 포함하는 자율주행차에 대한 가이드라인을 발표[43]했으며, 내용은 관련 데이터 저장과 활용, 인터페이스, 관련 기술에 대한 교육, 시스템 안정성, 차체 안정성, 연방&주법률 준수, 도적적인 부문에 대한 검토, 기능 작동 범위, 사물 확인과 추적에 대한 부문 등임

○ 안전 강화가 자동차 산업 발전에 저해되지 않도록 규제와 산업발전의 균형을 지키도록 법·제도 조율

- 클라우스 슈바프 세계경제포럼(WEF) 회장은 기업들은 4차 산업혁명에 대응하기 위해서는 '빠른 속도'와 '경량화'를 갖추고, 정부는 규제가 장애요소가 되지 않도록 제도 정비가 필요하다고 했음[44]

- 자율주행차 산업을 발전시키기 위해 제정한 『자율주행자동차 고시』의 구조 및 기능 제한과 운전자 탑승의무를 완화하는 방안을 고려[45]

* 조향핸들, 변속레버 등 자동차의 구조를 전제로 된 규정은 자율주행차를 기존 자동차 기준에서 정의하여 개발자들의 연구 및 투자를 저해할 수 있음

□ 자율주행차 안전 확보를 위한 테스트 및 검증, 운영 시 지속적인 안전 상태 점검 인프라 지원

○ 자율주행차 전문 시험테스트를 위한 인프라 구축

- 다른 자동차, 보행자 및 외부환경과의 상호작용을 인위적으로 만들어 테스트 할 수 있는 공간 마련

- 미국 미시간 주 정부는 2015년 M-city라는 자율주행차 실험도시를 구축, 한국도 K-city, 판교 제로시티 등 자율주행차 실증단지 구축 진행

○ 자율주행차 시험운행을 위해 법 개정을 통해 기술개발을 간접적으로 지원

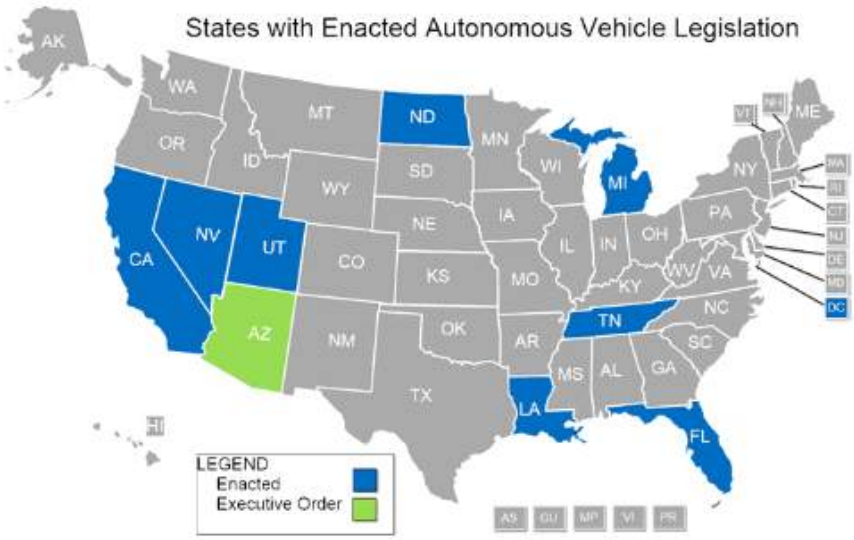
* 미국은 네바다, 캘리포니아, 애리조나 등 9개주 도로에서 자율주행차 시험운행 가능

43) U.S. DOT issues Federal Policy for safe testing and deployment of automated vehicles http://www.nhtsa.gov/About-NHTSA/Press-Releases/dot%E2%80%93federal%E2%80%93policy%E2%80%93for%E2%80%93automated%E2%80%93vehicles%E2%80%9309202016, 2016.9

44) 세계경제포럼(WEF, World Economic Forum), 중앙일보, 2016.10, 4차 산업혁명 키워드는 혁신

45) 강소라, 2016.8, 자율주행자동차 법제도 현안 및 개선과제, 한국경제연구원

[그림 4-2] 자율주행차 도로 시험운행 가능한 주



자료 : NCSL(National Conference of State Legislatures) 홈페이지, Autonomous/Self-Driving Vehicles legislation(2016) 파란색 : 제정완료, 연두색 : 주지사 행정명령

□ 사고 방지 및 대응을 위해 자동차 오작동 및 교통사고 데이터를 확보하고 관리하는 체계 마련

○ 안전을 보장하기 위해서는 자동차 도메인 위험 분석이 필요하며, 위험 분석을 위한 정보 구축이 되어야 함

- 결함 분류체계를 구축하고, 사고원인 분석을 위한 데이터 관리가 필요
- 동일 결함 재발 방지를 위한 변경 관리, 유사 파생 제품의 변경 파급 관리에 결함 데이터 활용

○ 사고 재발 방지를 위한 책임 추궁과 사고 원인 규명·제거는 목적은 같으나, 두 가지를 동시에 수행하기에 어려움이 있어 안전을 지키기 위해서는 적절한 수준의 협의가 필요

- 도요타 급발진 사고의 원인 파악이 어려웠던 이유는 시스템의 복잡성에 의한 원인도 있었으나, 사고사의 사고 보상 및 처벌에 대한 기피에 원인도 있음
- 사고 원인 분석을 통한 초기 사고 방지가 최소한의 비용 소요와 향후 산업발전의 기초가 된다는 점을 인식

○ 미국의 경우 원인규명과 미래의 안전대책을 위한 사고 조사가 중시되어 법적 책임 추궁의 비중을 낮추어, 사고 조사의 효율성 극대화[46]

- 형사책임 추궁에 대한 의존을 줄이고 광범위한 행정적 책임추궁과 행정 처분으로써 사고 당사자의 정보 제공 기회 확대

  * 항공사고조사에서 사고조사담당 연방교통안전위원회(NTSB), 행정적 처분 담당 미국연방항공국(FAA), 형사책임담당 미국연방수사국(FBI) 등의 역할 분리[47]

- NTSB는 여객회사, 항공기 제조회사 등을 포함한 사고당사자를 사고조사에 참가시켜, 당사자의 전문지식을 활용하고, 신속한 정보 수집

□ 자동차 관련 업체에서는 시스템 안전을 보장하기 위해서 기능 안전 표준을 정확히 이해하고, 지키려는 노력이 필요

○ 자동차 산업에서 소프트웨어의 활용도가 늘어날수록 자동차 기능 안전 표준과 함께 다른 산업 도메인에서 사용되는 기능 안전 표준들이 복합적으로 사용되기 때문에 다른 도메인 표준 습득 필요

  * 예 : IEC 61508, DO-178C(항공 부분)

○ 안전 표준을 형식적인 수준의 문서작업이나 인증 수단이 아닌 시스템 안전 보장을 위한 방안으로 사용하는 것이 필요

- '16년 출간한 ISO/DIS 26262 2nd[48] 에서는 안전 평가 시 안전 목표 달성에 집중하고, ASIL[49]에 맞는 안전 구현을 위해 추천되는 방법을 변경함

- 기능 안전성 표준과 더불어 MISRA-C[50] 등의 안전을 보장하기 위한 코드 표준도 SW 분야의 구체적 안전 구현 방법임

□ 신기술 이용이 늘어나는 자율주행차는 SW 안전이 산업 발전에 중요한 요소로 안전 관련 기술 개발이 선행되어야 함

46) 시로야마 히데야키, 2004.6, 사고조사・정보수집과 법 시스템 - 일미 비교, 일본기계학회지
47) NTSB, National Transport Safety Board/ FAA, Federal Aviation Administration/ FBI, Federal Bureau of Investigation
48) DIS, Draft International Standard, 국제 표준 초안, 2016.9
49) ASIL, Automotive Safety Integrity Level, 자동차 위험 등급으로 사고 심각도, 사고 빈도, 통제 가능성에 따라 결정되고, 안전 요구사항 결정 시 중요한 요소임
50) 코드의 안전성, 호환성, 신뢰성을 보장하기 위한 C 프로그래밍 개발 표준

○ IoT, 인공지능, CPS 등 신기술을 이용한 자율주행차, 무인항공기, 헬스케어 등 새로운 산업 분야는 SW 안전이 산업 발전에 기본 요소

- 일반인들은 물론 전문가들도 새로운 기술 안전에 대한 두려움을 가지고 있으므로, 안전에 대한 불안을 해소시키는 것이 필요

  * 스티븐 호킹,『완전한 인공지능의 개발이 인류의 멸망을 불러올 수 있다』, 2014.12

- 안전에 대한 비용 지출은 상대적으로 효과가 크고, 경제적 효율성도 있어 안전 투자로 비용 감소

  * 미국의 교통안전투자로 인한 교통사고 사망자수 감소의 사회경제적 효과를 추정하면 B/C(Benefit/Cost)가 42.7에 이르는데, 이는 예방비용 투자는 복구비용 지출보다 효율적인 투자라는(저비용-고효율) 좋은 사례[51]

□ 정부·산학연이 연합하여 소프트웨어 안전 구현을 위한 전문 인력 양성

○ 정부와 산업계 모두 표준 커리큘럼 개발에 참여하며, SW 안전 의식과 기술, 표준, 도메인 부분 SW 안전 교육 담당

- 정부는 안전 SW 발주자, 개발자, 사용자를 위한 체계적인 표준 커리큘럼 제안 및 관련 과정 개발

- SW 안전에 공통된 안전 의식이나 기본 이론은 정부에서 상시 교육을 담당하는 전문 강사를 양성하여 교육 담당

- 각 도메인별 특화 부분은 각 산업 현장에서 실무를 담당하던 전문가를 전문 강사로 양성하여 도메인별로 교육 담당

○ SW 안전 국제표준에 부합하는 SW 안전 전문가 자격제도 도입하고, SW 안전 전문가들에 대한 우대정책과 사후관리를 통한 전문가 역량 제고

- 국가기반시설 SW 안전 검점에 대한 업무독점형 자격제도를 통한 SW 안전 전문가 우대정책 마련

- 빠른 속도로 발전하는 SW 기술 습득을 위한 자격 유효 기간 설정 및 보수 교육 및 인증을 통한 자격 갱신 체계 구축

51) 안홍기 외, 2014.12, 안전의 사회적 가치와 비용부담에 관한 기초 연구, 국토연구원

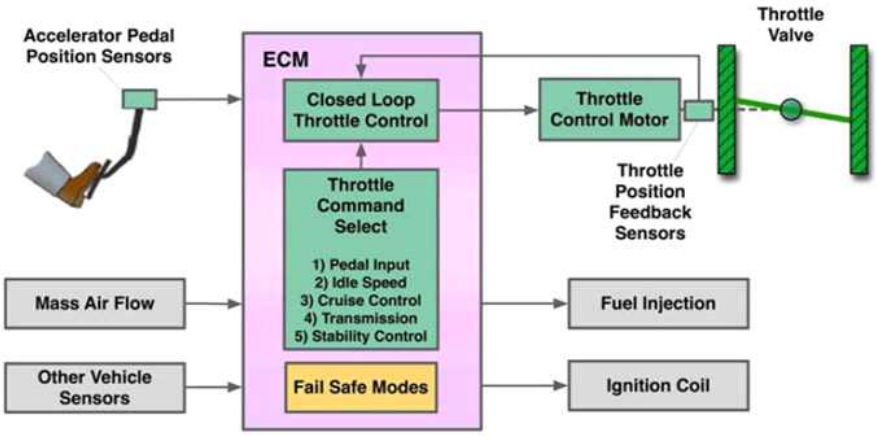
[별첨1] 토요타 급발진 사례 소프트웨어 오류 상세 설명

□ 급발진 사고에 대해 NASA는 ETCS(전자식 연료분사 제어장치)를 심층 조사한 후, 안전장치가 설계되고 ETCS 고장이 없으며 SW 오류가 없다고 발표했으나, 시스템이 복잡하여 증명이 어렵다고 함[52)]

○ NASA는 정적분석[53)], 논리 모델 테스팅[54)], WCET(worst case execution timing)[55)] 등을 통해서 소스코드를 검사했으나, ETCS가 급발진사고를 야기할 수 있는 SW 오류를 찾아내지 못함

- ETCS는 페달의 위치 센서와 다른 센서들의 신호에 의해 연료와 스로틀 밸프를 제어함

[그림 별첨1-1] 도요타 ETCS-i



자료 : NASA NESC Technical Assessment Report(2011), NHTSA Toyota UA Investigation

- 스로틀 오픈의 2가지 가설을 페달 위치 확인 시스템과 CPU SW 버그의 결합, Main CPU 기능 오류로 세웠으나, 가설이 맞음을 증명 못함

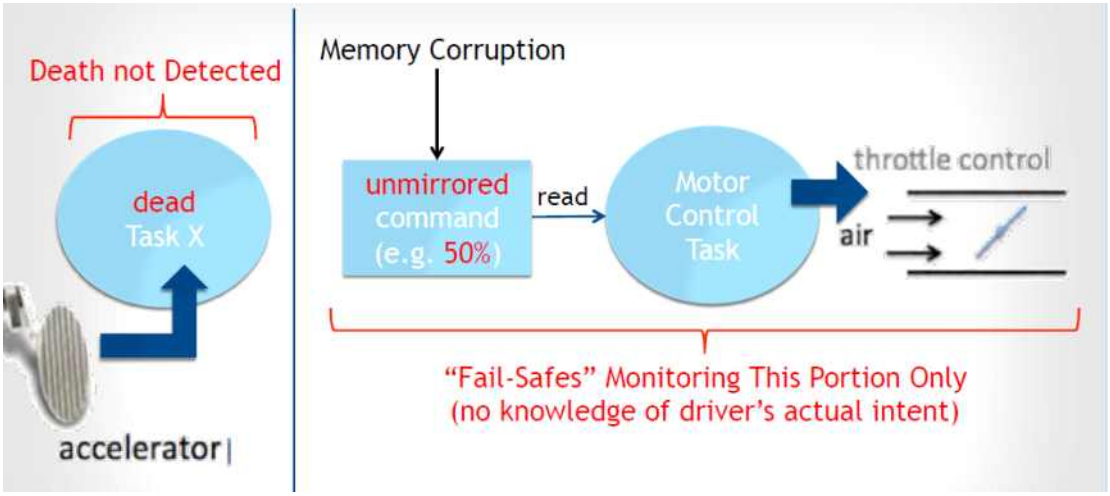
- 메모리 오류는 EDAC(error detection and correction,오류 검출 정정), data mirroring(이중 관리)에 의해 방지된다고 했으나, 향 후 EDAC가 없던 것으로 밝혀짐

52) NASA NESC Technical Assessment Report, 2011.1, NHTSA Toyota Untended Acceleration(UA) Investigation pp170~172, pp20, pp13~16, pp147~152, pp169, p54
53) 실제 프로그램 실행 없이 SW 분석, Coverity, CodeSonar, Uno 등의 툴 사용
54) 정형 기법의 한 종류로, 정형 언어로 작성한 모델이 검증하고자 하는 특성을 만족하는지 여부를 입증하는 기법
55) 실시간 시스템의 안전성 검증을 위해 시스템의 가장 긴 실행시간 계산

□ Bookout 소송에서 BARR group은 급발진은 bit-flip을 다음과 같은 4가지 복합적 원인으로 해결하지 못한 데 원인이 있다고 분석함

○ 급발진을 일으킨 시스템 문제는 중요 변수관리, Fail-safe modes 구축[56], Watchdog 디자인, 모니터 CPU의 구현 등 복합적 원인으로 일어남

[그림 별첨1-2] 스로틀 제어 오류 상태



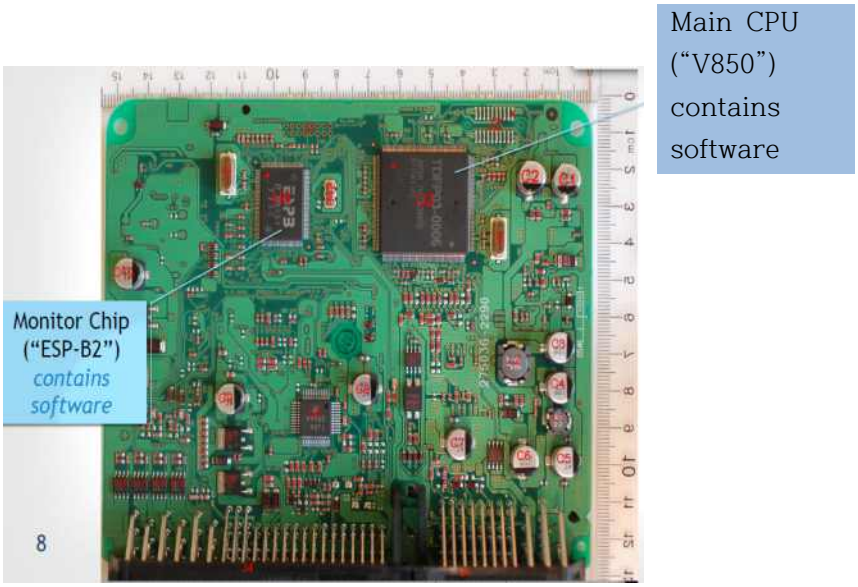
자료 : Michael Barr(2013), Bookout V. Toyata 2005 Camry L4 Software Analysis

- 자동차의 OS인 OSEK의 중요 데이터 영역이 하드웨어 오류에 보호되지 않았고, 스로틀 밸브 각도를 저장하는 변수가 전역변수로서 여러 프로세스에 영향을 주어, 문제를 일으킴
- Limp Modes[57], Fuel Cut[58] 등과 같은 Fail-safe 기능[59]이 문제가 된 프로세스와 같은 프로세스 상에 있어, 사용자의 의도와는 다르게 스로틀 제어가 작동하는 것을 방지하지 못함
- Watchdog[60]이 태스크 중단을 감지할 수 없게 디자인됨
- ESP-B2 모니터 CPU가 태스크 중단 후 데이터 오류를 감지하지 못해 운

56) 인간의 과오나 기계의 동작상 실패가 있어도 안전사고를 발생시키지 않도록 2중 또는 3중으로 통제를 가하거나 기계내부에 고장이 발생한 경우 피해가 확대되지 않고 한시적으로 운영이 지속되도록 하여 안전을 확보하는 설계 개념
57) 페달 센서의 오류 시 엔진출력을 조절하는 기능
58) 페달을 밟지 않은 상태에서 엔진 속도를 제한하는 기능, 2500 rpm으로 제한함
59) NASA NESC Technical Assessment Report, 2011.1, NHTSA Toyota Untended UA Investigation pp79-83
60) 시스템이 기계적인 고장으로 중단 상태가 되거나 프로그램의 오류로 시스템에 이상이 발생하는 것을 감시하는 장치, 이와 같은 오동작을 방지하기 위해 프로그램으로 설정된 타이머로 어떤 조건을 만족하면 경보를 표시하게 하는 장치

전자의 의도를 인식하지 못함

[그림 별첨1-3] 도요타 ECM(Engine Control Module)



[별첨2] 토요타 급발진 사례 소프트웨어 오류 해결 방안 상세 설명

□ 안전 보장을 위해서는 시스템 위험 분석 및 고장 분석을 통하여 그에 따른 시스템 제어를 위한 안전 기술 구현이 필요

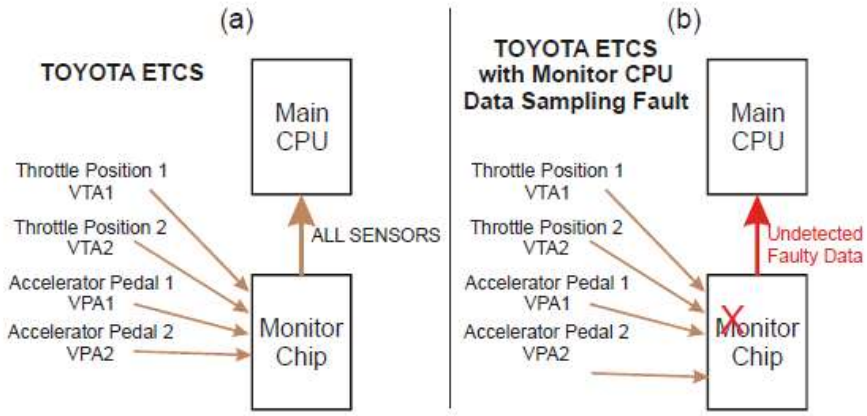
○ 시스템에 맞는 위험 분석 기술을 사용하여 위험 분석 및 관리

- FTA(Fault Tree Analysis), FMEA(Failure Mode and Effect Analysis) 등의 수십 년 전에 개발된 고전적인 위험 분석 방법이 많이 쓰이고 있음
- 사고 발생의 원인이 선형적이지 않고 비선형적 요인이 서로 작용하여 사고가 발생하므로 STPA(System Theoretic Process Analysis) 등 상호 작용을 분석하는 방법 사용이 필요

○ 안전 구조의 구현은 시스템의 정확한 분석에 따른 구현이 필요하며, 이를 위해서는 안전 작동방법 기술과 함께 도메인 지식이 필수임

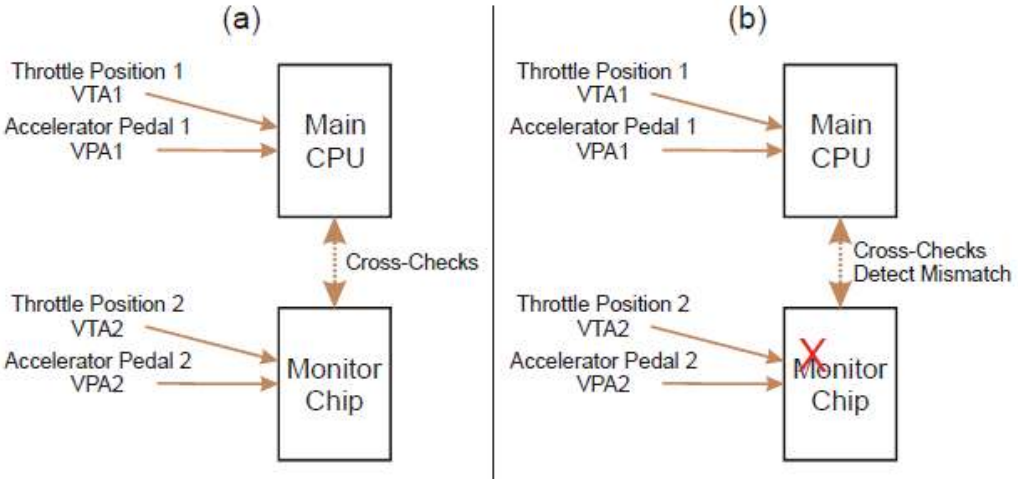
- 도요타 ETCS를 분석하면 입력 데이터와 CPU가 두 개씩 구성되어 있었으나, 잘못된 구현으로 단일고장점(single point of failure) 발생[61]

[그림 별첨2-1] 데이터 오류를 감지하지 못한 경우



61) 이중화되지 않음으로 인해 해당 시스템의 장애 시 전체 또는 일부 서비스의 중단을 가져오는 시스템 자원, Phil Koopman, 2014.9, A Case Study of Toyota Uninted\nded Acceleration and Software Safety

[그림 별첨2-2] 데이터 오류 인지를 위한 올바른 구현

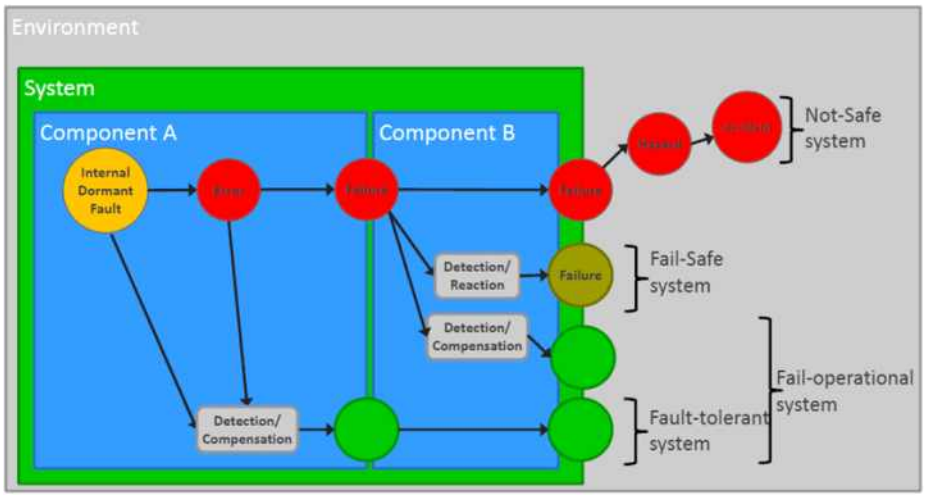


자료 : Phil Koopman(2014), A Case Study of Toyota Unintended Acceleration and Software Safety

- 안전 보장을 위해서는 독립된 여러 개의 FCR(Fault Containment Region)[62] 구현이 필요

○ 기존 자동차와 자율주행 자동차의 안전을 위해 재해 방지 기술(Fail Safe, Fail Operational) 의 정확한 구현이 요구됨

[그림 별첨2-3] Fail safe, Fail Operational 의 오류 전파



자료 : Avizienis et al.(2004), Basic Concepts and Taxonomy of Dependable and Secure Computing(이론)
Rudolf Grave(2015), Autonomous Driving – From Fail-Safe to Fail-Operational Systems(그림)

62) 이 영역의 결함이 시스템의 다른 영역으로 전파되지 않으며, 다른 영역의 결함도 영향을 미칠 수 없는 독립적인 영역

- Fail Safe는 시스템 고장 발생 시 일정기간 기능을 계속하는 것이 가능한 상태로 재해까지 진행되지 않도록 함

- Fail Operational은 장애가 발생 시, 장애를 감지하고 중복 등의 적절한 방법을 사용하여 계속 정상적으로 작동하도록 하는 방식으로 자율주행차의 안전보장에 중요한 기능임

[참고문헌]

1. 국내문헌

강소라, 2016.8, 자율주행자동차 법제도 현안 및 개선과제, 한국경제연구원
고병각, 2015.3, ISO 26262 2nd edition 현재 이슈사항, KTL
백재진, 2011.3, 차량용 임베디드 소프트웨어 신뢰성평가 연구, 한국자동차공학회
안홍기 외, 2014.12, 안전의 사회적 가치와 비용부담에 관한 기초 연구, 국토연구원
에이티씨, 2016.1, 글로벌 자율주행차 시장전망과 기술개발 참여업체 사업전략 1편-기술・시장편 p74
윤대권, 김용현, 2014.8, 국내 자동차 사고기록장치의 법규 동향, 한국자동차공학회
융합연구정책센터, 이재관 자동차 부품연구원, 2015.8, 자율주행자동차 동향과 전망
이재관, 2016.4, 스마트카 최신 동향 및 산업적 과제, 대한전자공학회 학술대회

2. 국외문헌

시로야먀 히데야키, 2004.6, 사고조사・정보수집과 법 시스템 - 일미 비교, 일본기계학회지
Avizienis et al., 2004, Basic Concepts and Taxonomy of Dependable and Secure Computing
Daiwa, 2015.06, Smart cars :who has the head start? Pan-Asia Autos
Donald G. Firesmith , 2012, 12, Common Concepts underlying Safety, Security and Survivability Engineering
ISO/DIS 26262 2nd 2016.9
KPMG, 2015.03, Connected and Autonomous Vehicles-The UK Economic Opportunity
McCabe Software, 1996,9, Structured Testing : A Testing Methodology Using the Cyclomatic Complexity Metic
Michael Barr, 2013.4, Bookout V. Toyota 2005 Camry L4 Software Analysis, Testimony Jean Bookout and Estate of Barbara Schwarz v. Toyota Motor Corporation, et. al. (automotive product liability), District Court of Oklahoma for Oklahoma County
Mike Kirsch, 2011.3, NASA Engineering and Safety Center Study of Unintended Acceleration in Toyota Vehicles, NASA Engineering and safety center
NESC Director, 2011.1, National Highway Traffic Safety Administration Toyota Unintended Acceleration Investigation, NASA Engineering and safety center technical assessment report
NHTSA, 2016.9, Federal automated vehicles Policy, U.S. DOT issues
Phil Koopman, 2014.9, A Case study of toyota unintended acceleration and software safety, TSP(Team Software Process) Symposium 2014
Strategy&, 2014, In the fast lane, The bright future of connected cars

Tom Alberg 외, 2016.9, Autonomous Vehicle Plan for the I-5 Seattle/Vancouver B.C. Corridor

Vector, 2015.5, Safety and Security for vehicles-best practices, vector UK Conference

3. 기타(신문기사 등)

세계경제포럼(WEF, World Economic Forum), 중앙일보, 2016.10, 4차 산업혁명 키워드는 혁신

오토뷰, 2016.7, 중 정부, 고속도로서 자율주행차 테스트 금지, http://www.autoview.co.kr/content/article.asp?num_code=59194

전자신문, 2016.8, 테슬라 전기차, 한국 도로테스트 들어갔다. http://www.etnews.com/20160822000429

행정기관 및 공공기관 정보시스템 구축·운영 지침 제50조, 53조, 2015.12

Google Self-Driving Car Project, 2016.3, Monthly reports, 2016.2 http://news.jtbc.joins.com/article/article.aspx?news_id=NB11184061,

NCSL(National Conference of State Legislatures) 홈페이지, 2016.10 , Autonomous/Self-Driving Vehicles legislation,

R.Charette, ‘2009.2, This car runs on code’, www.spectrum.ieee.org/feb09/7649,

주 의

1. 이 보고서는 소프트웨어정책연구소에서 수행한 연구보고서입니다.
2. 이 보고서의 내용을 발표할 때에는 반드시 소프트웨어정책연구소에서 수행한 연구결과임을 밝혀야 합니다.