정 보 보 호 학 회 지
제25권 제1호, 2015. 2

자동차 소프트웨어 & 공급망 보증(A-SSCA)

김 동 원*, 한 근 희**

요 약

현대의 자동차는 안전중요(Safety Critical) 시스템이기 때문에 차량의 안전성을 보장하는 것은 물론 초 연결사회를 지향하는 사물인터넷 기술의 발전과 자동차의 스마트화 됨에 따른 자동차 보안문제가 대두됨에 따라 자동차 소프트웨어와 공급망에서의 보증 방안이 필요하다. 본 논문에서는 자동차 소프트웨어의 보안성을 확보하고, 공급망에서의 보안성을 보증하기 위한 자동차 소프트웨어&공급망 보증(A-SSCA, Automotive-Software& Supply Chain Assurance)을 위한 보안 쟁점 및 고려사항을 제시하고자 한다.

Ⅰ. 서 론

현대의 자동차는 사람에게 상해나 사망을 유발할 수 있는 안전중요(safety critical)시스템이기 때문에, 차량의 안전성을 보장하는 것은 자동차의 개발 및 판매에 있어 필수요건이다. 최근 ESC(electronic stability control), ACC(adaptive cruise control) 등에서 볼 수 있듯이, 차량 안전성에 대한 시장의 요구가 사고완화나 피해경감에서 사고예방으로 이동 하면서, E/E/PE (electrical/electronic/programmable electronic) 기술이 안전기능의 구현에 대폭 적용되고 있다. 따라서 자동차의 안전성을 보장하기 위해서는 E/E/PE시스템의 안전요건을 체계적으로 분석하고, 안전기능이 바르게 동작하도록 개발 및 검증할 수 있는 프레임웍을 구축하는 것이 필요하다.[1]

특히 자동차 기능이 최대 85%까지 소프트웨어에 의해 구현됨[3]에 따라, 차량용 소프트웨어의 안전성과 신뢰성을 보장하기 위한 개발 및 검증 프로세스를 구축하고, 안전관련 소프트웨어가 가지고 있어야 할 안전성 특성(safety property)을 이해하는 것은 자동차 전반의 안전성 보장을 위해 필수적인 일이다.[1]

이에 본 논문에서는 ISO26262 안전프로세스와 소프트웨어 & 공급망 보증(Software & Supply Chain Assurance)을 기반으로 지능형 자동차(이하 스마트카)의 안전한 공급을 위한 방법으로, 자동차 소프트웨어 & 공급망 보증(A-SSCA, Automotive-Software & Supply Chain Assurance)을 위한 보안쟁점 및 고려사항을 제시하고자 한다.

Ⅱ. 자동차 보안위협 분석

2.1. 자동차 보안사고 사례

현대의 자동차는 다양한 잠재적인 보안공격에 노출되어 있다. 외부와의 연결을 통해 자동차의 내부 통신망 또는 전자제어장치(ECU) 등에 악성코드를 삽입하거나 도청, 변조, 오작동 유발, 권한상승, 서비스 거부 등과 같은 공격이 가능하다. 자동차 보안사고 사례를 살펴보면 2010년부터 2014년 최근까지 자동차 해킹 사례는 끊임없이 발생하고 있다. Table 1.에 따르면 자동차 해킹 사례는 그 횟수가 점차 증가하고 있으며, 국내외 유수의 컨퍼런스에서 핵심 주제로서 다루어 지고 있다.

자동차의 해킹문제는 전 사회적인 위험이 될 수 있으며, 사이버공간의 위험이 현실세계로 전이·확대 될 가능성이 높다. 즉 자동차의 보안위협은 사람의 생명을 위협할 만큼 치명적이다.

"본연구 는 미래창조과학부 및 정보통신산업진흥원의 대학IT연구센터육성지원사업/IT융합고급인력과정지원사업의 연구결과로 수행되었음" (NIPA-2014-H0301-14-1023)

* 고려대학교 정보보호대학원 (blast.kim@gmail.com)
** 고려대학교 융합소프트웨어전문대학원 (khhan@formal.korea.ac.kr)

〔표 1〕 자동차 보안사고 사례

Year	내용	Ref
2010	브레이크나 와이퍼의 제어에 영향	[9]
2010	타이어 공기압 감시 시스템 취약성 제기	[10]
2010	OBD-II에 WLAN 수신기를 통한 ECU 조작	[11]
2011	Smart Phone과 SMS를 이용한 Telematics 서비스 해킹	[12]
2011	딜러들이 이용하는 웹시스템(Webtech Plus)를 해킹하여 차량의 오동작 발생	[13]
2011	이동통신 네트워크 상에서 전송되는 패스워드를 탈취함으로써 Android Smart Phone을 이용하여 차량의 시동을 켜는 시연	[14]
2012	SBS 뉴스, 모바일 자동차 진단 앱 이용 해킹	[15]
2013	전자제어식 제동장치 무력화	[16]
2013	해킹을 통한 자동차 절도	[17]

2.2. 자동차 보안위협 분석

자동차는 기능에 따라 크게 차량제어부분과 비 제어부분으로 나눌 수 있다. 차량제어 부분은 자동차를 운행하는데 있어 필요한 장치들은 직간접적으로 제어가 가능한 기능으로 내부적으로는 자동차 제어 관련 ECU와 연결되어 안전에 크게 영향을 준다. 비 제어부분은 차량 운행 중 직접적인 제어는 하지 않지만 안전확보 및 다양한 서비스를 지원하기 위한 기능으로 외부 통신망과 연결되거나 추가적으로 사용될 기능이 포함된다. 그리고 자동차 내 연결 경로는 제어 및 비 제어 부분에 항상 접목되기 때문에 각 기능의 위협분석 시 함께 고려되어야 한다.[21] 자동차의 공격지점은 크게 직접적인 물리적 공격지점, 간접적인 물리적 공격 지점, 근거리 원격/무선 공격 지점으로 분류할 수 있다.[8,9,18]

자동차 보안위협을 분석하기 위해 보호대상을 명확하게 할 필요할 필요가 있으므로 자동차 보안사고 사례 및 관련자료, 자동차 모의해킹 결과를 분석하여 자동차에서 보호해야할 대상을 연구하였다. 자동차 모의해킹은 실제 자동차의 안드로이드 및 WinCE 기반의 텔레매틱스 단말, 모바일 장비, 웹 서버를 대상으로 실험하였다. 자동차는 현재 알려진 취약점 및 위협이 정의되지 않았기 때문에 시나리오 기반으로 진행하였으며, EVITA(E-safety Vehicle Intrusion protected Applications)의 Attack Tree를 참조하였다. [24,25]

〔표 2〕 자동차의 기능 분류〔8〕

구분	기능분류	기능
차량 제어	Power Train	엔진제어, 변속기 등 자동차 운행을 위한 기능
	Chassis	동력생성, 동력전달, 조향, 브레이크 등 기본적인 자동차 동작을 위한 기능
	Body	바디 전장품, 편의장치, 램프류, 의자류 제어 등의 동작을 위한 기능
차량 비제어	진단/보수	차량 스캐너 및 OBD-II 등과 같이 차량의상태 및 고장을 진단하고 보수하는 기능
	Telematics Unit	이동통신 및 방송망을 이용해 인터넷, 위치추적 등의 다양한 원격서비스를 제공하는 Unit
	Head Unit	Audio, Video, Navigation 등의 기능을 제공하는 Unit
	ITS/V2X	자동차 주변시설 및 차량간의 통신을 통해 요금자동징수, 자동단속, 교통사고 예방 등 다양한 응용서비스를 제공하는 기능
차내 연결	차량 Networks	CAN, CAN FD, LIN, FlexRay, MOST 등 자동차 내 구현되는 기능들 간의 통신을 위한 차량 내부 네트워크
	X by Wire	기존의 기계 또는 유입으로 제어하던 스티어링 휠, 브레이크 등의 장치를 전자적으로 제어하는 기술

자동차에서 보호해야할 정보 등의 자산에는 크게 자동차의 주행 중 발생하는 정보나, 자동차 이용자가 자동차에 등록하는 정보, 탑재 소프트웨어 오류, 외부 통신 등이 이에 해당된다.[25]

자동차 시스템에서 발생할 수 있는 보안위협은 공격자가 의도적으로 일으키는 보안위협(공격자에 의한 간섭)은 물론 이용자가 우발적으로 일으킬 수 있는 실수(이용자에 의한 조작) 등에 의한 위협도 포함하여야 한다. 이용자에 의한 조작은 크게 2가지로 분류할 수 있다.[25]

공격자에 의한 간섭은 크게 13가지로 분류할 수 있다.[25]

〔표 3〕 자동차 시스템에서 보호해야 할 정보자산

구분	설명
기본 제어기능	기본제어기능의 일관성과 가용성, 실행환경이나 동작을 위한 통신
자동차 고유정보	차량ID, 기기 ID, 인식정보, 주행정보, 동작이력, 저장정보 등
자동차 상태정보	자동차 상태 데이터, 위치정보, 속도 등
유저정보	개인정보, 인증정보, 과금정보, 이용이력 등
S/W	ECU 펌웨어, 관련 소프트웨어 등
콘텐츠	비디오, 음악, 지도, Application 데이터 등
설정정보	기본 조작설정, 공장초기 설정 데이터 등

〔표 4〕 이용자 조작에 따른 위협

위협	설명
설정 실수	- 자동차 내의 유저 인터페이스 등을 통하여 이용자가 행한 조작 오류등으로 인한 위협 - 인포테인먼트 기능에 의도하지 않은 개인정보 전송 및 보안설정 해제로 인한 위협
바이러스 감염	- 이용자가 외부에서 도입한 기기나 매체에 의하여 탑재 시스템이 바이러스나 멀웨어 등에 감염 - 인포테인먼트 기기에 감염된 바이러스가 N/W를 통해 전파

〔표 5〕 공격자의 간섭에 의한 위협

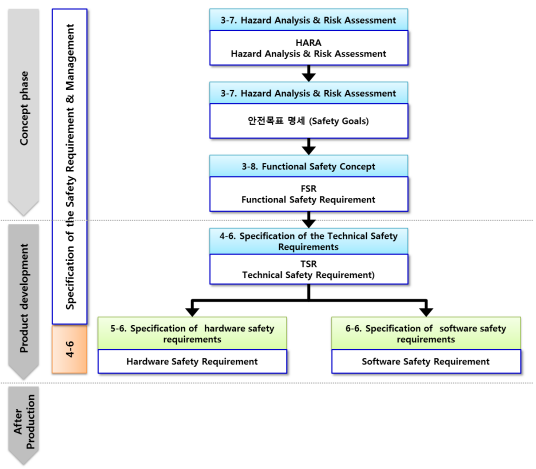
위협	설명
Sybil Attack	여러 개의 가짜 노드를 만들어서 혼란을 일으키는 공격
Spoofing	네트워크의 메세지를 변조하여 통신을 방해하거나 정보를 탈취하는 공격
Sniffing	네트워크의 메세지를 도청함으로써 정보를 탈취하는 공격
Jamming	차량 통신에 장애를 유발하는 신호를 발생시켜 정상적인 통신을 방해하는 공격
Malware Injection	스마트 폰에 악성코드 삽입된 어플리케이션을 다운 받게 한 후 차량과 디바이스 통신시 개인 정보 및 차량 정보 유출
DoS/DDoS	대량의 데이터를 전송하여 서비스 이용을 못하게 하는 서비스 거부 공격
Impersonation	허가 받지 않은 사용자가 인증서버로부터 인증이나 권한을 받아내는 공격
Web Attack	차량과 네트워크로 연결된 웹 시스템을 공격함으로써 자동차에 위해를 가하는 공격
Fuzzing	프로그램이나 단말, 시스템에 비정상적인 입력 데이터를 반복적으로 보내 자동차에 위해를 가하는 공격
Reverse-Engineering	프로그램, 펌웨어 등을 역분석 하여 자동차에 위해를 가하는 공격
In-transit Traffic Tampering	주행 중 메시지를 전달하는 과정에서 공격 차량에 의한 메시지 삭제 및 변조를 통해 차량 통신 방해하는 공격
Injection	비 정상적인 데이터를 삽입하여 프로그램이나 단말, 시스템에 위해를 가하는 공격
Manipulate	비 인가자가 허가되지 않은 차량의 기능을 조작하는 행위

Ⅲ. 자동차 소프트웨어&공급망 보증 관련 표준

3.1. 자동차 기능안전성 표준 (ISO 26262)

기능안전 표준인 ISO 26262는 대표적으로 IEC 61508을 자동차 개발 프로세스에 맞추어 새롭게 개정한 표준[4,5]으로 2011년 이후 개발되는 3.5톤 이하의 차량에 적용해야 할 전세계 자동차 업체가 참여한 기능안전 표준이다. ISO 26262는 자동차 부품 및 시스템에 점점 더 많은 전기/전장부품의 증가로 인한 위험관리를 주요 목적으로 하고 있으며, 제품개발 프로세스의 일반적 모델 중 하나인 V-모델을 기반으로 하고 있다.

안전요구사항을 간단히 살펴보면, 개념단계에서 위험원 분석 및 리스크평가(3-7. HARA)를 수행하고 이를 통해 안전목표(3-7. Safety Goals)을 설정하며, 기능안전 요구사항(3-8. FSR)을 도출한다. 기능안전 요구사



〔그림 1〕 ISO26262 안전 요구사항 구조

항이 시스템 레벨 제품개발 단계에서 기술안전 요구사항(4-6. TSR)로 연계되어 Part5 하드웨어 레벨의 하드웨어 안전 요구사항과 Part6 소프트웨어 레벨의 소프트웨어 안전요구사항으로 분해된다.[19]

따라서 제품개발 단계에서 안전요구사항 분석을 필요로 한다. 이를 위한 방법으로 ISO 26262에서는 ASIL(Automotive Safety Integrity Level) 준수를 요구하고 있다. ASIL은 ISO 26262 준수를 위한 핵심 사항으로 A~D 등급으로 분류하고 있다.[5]

ISO 26262는 일반 산업(항공 우주 및 군수를 제외한) 분야에서는 IEC 61508, “Functional safety of electrical, electronic and programmable elelctronin (E/E/PE) safety-related stystem'을 개발하여 중심적인 국제적 표준으로 채택하게 되었으며, 복잡도가 적은 E/E/PE 안전 관련 시스템을 제외하고는 안전 기능을 수행하는 모든 분야에 대해 IEC 61508을 적용하도록 규정하고 있다. ISO 26262는 IEC 61508을 근거로 자동차분야 전기전자 시스템의 안전요구사항을 충족하여 개발 및 공급될 수 있도록 하기 위한 체계적인 방법 및 절차에 대한 요구사항을 정의 하고 있다.

IEC 61508 및 ISO 26262 등 기능안전성 관련 표준은 RAMS(Reliability, Availability, Maintainability, Safety) 즉, 신뢰성, 가용성, 보전성, 안전성을 적용하는 것이 기능안전(functional safety)을 적용하는 것이다.[4]

이처럼 ISO 26262는 기능안전 즉, RAMS만을 보장하고 있다. 현재의 지능화, 고도화되고 있는 자동차는 전기전자 기능이 최대 85%까지 소프트웨어에 의해 구현되고 있으며, 외부와 연결(Connected)됨에 따라 보안 위협이 지속적으로 증가되고 있는 추세이다. ISO 26262의 기능안전에 보안(Confidentiality, Availability, Integrity)을 위한 방안의 필수 적용이 필요할 것이다.

〔표 6〕 기능안전 관련 표준

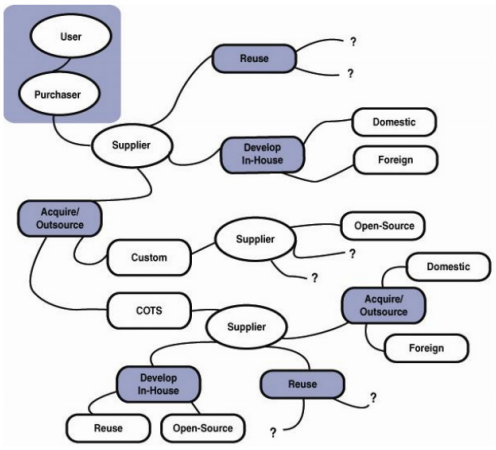
구분	관련기준
Automotive	ISO 26262
Railway	IEC 50126, 50127, 50128
Medical	IEC 60601 / ISO 62304
Energy & Process	IEC 61511
Nuclear	IEC 61513
Manufacturing	IEC 62061 / IEC 13849-1
Household Appliance	IEC 60335
Aerospace	DO-178 B, DO-254
Military	Def Stan 00-56

〔표 7〕 RAMS

Attributes	Descriptions
Reliability	주어진 사용조건에서 일정 기간동안 요구되는 기능을 고장없이 수행할 능력
Availability	어느 시점에서 시스템이 운영되고 있을 능력
Maintainability	규정된 조건하에서 일정 시간 내에 목적을 완료할 수 있는 능력
Safety	제한된 조건하에서 규정된 기간동안 인원, 설비에서 발생할 수 있는 상해 및 손상을 최소화하기 위한 설계적 보증

3.2. 소프트웨어 보증 (SwA, Software Assurance)

소프트웨어 취약점, 악의적 코드, 원하는 동작을 하지 않는 소프트웨어는 개인의 정보와 서비스를 제공하는 소프트웨어 중심적인 사회 기반 시설에 상당한 위험을 초래한다. 소프트웨어 보증(Software Assurance)의 역할은 이러한 위험들을 최소화 하는 것이다. 소프트웨어 보증은 소프트웨어가 취약점으로부터 자유롭고 신뢰 가능한지를 나타낸다. 소프트웨어는 “원하는 동작을 하는 신뢰 가능한 소프트웨어” 와 “보안취약점과 악의적 코드로부터 자유로운 소프트웨어”로 구분할 수 있다. 소프트웨어 보증의 주요 역할은 과정, 절차, 그리고 제품에 대해 모든 표준과 요구사항을 만족하는 소프트웨



〔그림 2〕 소프트웨어 공급 경로 예상

어를 개발 또는 유지하기 위함이다.[20,21] 소프트웨어 공급 사슬은 산업과 정부로부터 구매자, 개인 정보 보증을 지원하는 구매 관리자, 소프트웨어 취득자에 대한 의사 결정자, 주 계약업체와 하도급 계약자, 그리고 소프트웨어 공급자가 있다.[20]

제품에 사용될 Software & Hardware는 오류나 버그가 없이 정상적으로 작동하고 안전하다는 것을 입증해야 하고 또한 보증해야만 한다. 소프트웨어에 의해 야기될 수 있는 상황은 Information Assurance 대상별 보안인증 요구사항에 따른 표준 및 제도를 활용하여 보안인증을 입증할 수 있으나, 소프트웨어 공급 사슬망에서 발생할 수 있는 보안위협을 예방하고 방지하기 위한 방안이 필요하다. 소프트웨어 결함(설계·구현 오류)은 예상치 못한 작동, 시스템 오류나 장애, 또는 사이버 공격(attack)으로 이어지는 소프트웨어 취약점(vulnerabilities)으로 귀결되기 때문이다.

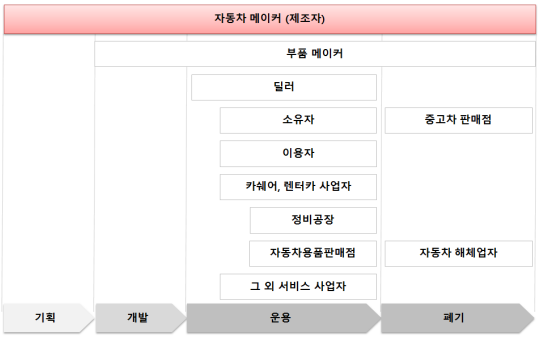
3.3. 공급망 보증 (SCA, Supply Chain Assurance)

소프트웨어 & 공급망 보증은 미국의 오바마 대통령이 제정한 국방수권법에 의해 공식화 되었으며, 이는 소프트웨어 보증을 생명주기 안에서 고려하던 것에서 벗어나 하드웨어 및 공급자(vender)까지 고려한 확장된 소프트웨어 보증 정책이다.[20] 정부·공공·민간 모든 분야에서 시스템 외주개발이 증가되고 있으나, 요구자·수요자·주문자·고객의 관심은 오로지 개발기간 단축, 정시 납품과 비용절감에만 관심이 있고, 시스템 보증(System Assurance)과 관련된 위험요소와 요구사항대로 시스템 기능이 구현되었다는 신뢰도의 확인 과정에는 관심이 없다. 또한 상용 소프트웨어 제품(COTS), Open Source 소프트웨어 제품 사용도 많아지고 있으나, 이 과정에서 사용되는 소프트웨어나 정보시스템의 획득(Acquisition) 과정에서 발생하는 복잡 다양한 소프트웨어 공급망(supply chain)에 대한 위험관리(Risk Management)의 중요성을 인식하고 확인하는 사례는 없다. 소프트웨어 & 공급망 보증은 공급망 위험(Supply Chain Risks)을 식별, 분석, 평가하는 과정으로, 이를 수행하는 작업 중에 발생할 수 있는 비용과 이익을 수용할 수 있는 범위 안에서 공급망 위험을 수용(Accepting)하거나 회피(Avoiding)하거나 전환(Transferring)하거나 통제(Controlling)하는 것을 말한다.[22]

SSCA의 주요한 목적은 상업제품(COTS), 특정 제품뿐만이 아니라 안전한 소프트웨어를 개발 할 수 있는 공급자의 능력을 평가하고 전문기업에 의해 고객맞춤형으로 개발된 소프트웨어에서 소프트웨어 공급망 위험을 줄이기 위한 현존하는 기술 적용에 도움을 주고, 조직의 획득 시나리오에 적절한 기술을 적용할 수 있도록, 획득자(acquirers : 요구자·수요자·주문자·고객)에게 여러 가지 도움이 되는 방안을 제공하는 것이 주목적이다. 공급자를 선택하는 부분에서, 제품 선택·통합 그리고 소프트웨어 하청업자와 관련된 공급망 위험들을 평가하고 완화시킬 수 있는 공급자의 능력을 평가하게 된다. 공급망 무결성을 위해 개발기간 동안과 공급망 상의 참가자들(participants)간 수송되는 과정에서 컴포넌트, 부품, 모듈 등을 각종 위험요소들로 부터 보호한다. 가장 중요한 공급망 위험은 설치(deployment) 이후에 주로 발생하게 되므로, 공급망 위험들을 관리하는 지침(guidance)을 제공하고, 확장된 사용(expanded usage)의 결과에 의한 새로운 위협과 공격패턴, 제품 개선/대체(pgrades/replacements), 변화(change)에 의해 발생할 수 있는 초기 획득과정에서 발생할 수 있는 공급망 위험 평가를 수행한다. 소프트웨어 개발부터 유지보수까지 계약자/하청업자의 빈번한 변경이 일상적으로 발생하므로, 공급자(Supplier)의 능력 범위 안에서 심각한 공급망 위험(critical supply chain risks)을 이해하고 식별 가능하도록 한다.

Ⅳ. 보안 쟁점과 고려사항

자동차 보안을 향상시키기 위해서는 자동차에 연관되는 다양한 정보자산을 대상으로 하여 그 가치에 맞는 적절한 보안 대책을 수행해야 할 필요가 있다. 본 논문



〔그림 3〕 자동차 시스템의 생명주기

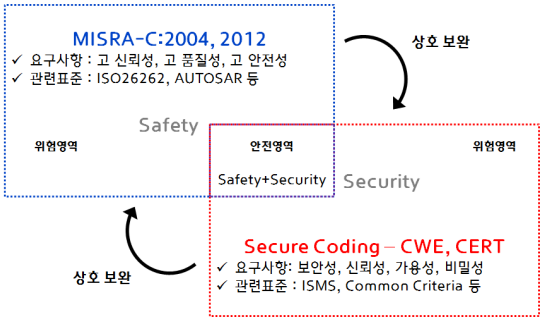
에서는 자동차 시스템의 생명주기를 [기획], [개발], [운용], [폐기]의 4개의 과정으로 분류하고, 각 과정에서 전체를 총괄하는 [관리정책]으로 분류할 수 있다.

자동차 소프트웨어 & 공급망 보증을 위한 방안으로서, 자동차 Life-Cycle 내에서 이해관계자 별 보안 대응 방침을 과정별로 4레벨로 분류하고, [기획], [개발], [운용], [폐기]의 각 과정에서 전체를 총괄하는 [관리정책]을 포함하여 “Approaches for Embedded System Information Security"[23]와 기본적으로 자동차 특유의 항목을 연계하여 다음과 같은 통제방안을 구성하였다.

자동차는 높은 안전성과 보안성이 요구되고 있기 때문에 기존의 안전성 코딩규칙(MISRA-C)과 보안성 코딩규칙(Secure Coding) 상호보완을 통하여 자동차 소

〔표 8〕 생명주기 과정 별 위험 통제 방안 1

	관리방침	기획, 개발
L1	보안 대응을 수행하고 있지 않음	보안을 고려한 기획, 설계가 수행되지 않음
L2	보안대응은 현장(기획, 개발 담당등)에게 일임하고 있어 문제를 조건에 따라 개별적으로 대처함	보안에 대한 검토가 현장(기획, 개발 담당 등)의 주도로 실시
L3	보안 대응에 대하여 조직에서 정책을 수립하여 수행함	조직의 정책을 기본으로 보안을 고려하여 개발 진행
L4	보아대응에 대하여 조직정책 및 감사 프로세스 보유	조직의 정책을 기본으로 보안을 고려한 개발을 실시하고, 그 내용에 대한 평가를 객관적으로 실시
	운용	폐기
L1	출하 후 제품에 대한 보안문제가 발생했을 경우 대책에 대한 검토를 수행하지 않음	잔존정보에 대한 취급에 대하여 고려하지 않음
L2	출하 후 제품에 보안문제가 발생했을 경우 대책을 현장(개발 책임자 등)이 제품별로 담당	잔존정보의 제거방법을 명세서 등에 명기하고 있음
L3	조직의 방침을 기본으로 출하 후의 제품에 보안문제가 발생했을 경우의 대책 보유	폐기시 보안위험의 경감방법을 보유하고 있음
L4	조직의 정책을 기본으로 출하후의 제품에 보안문제가 발생했을 경우 대책을 설정하며 보안관련 정보를 다루는 외부 창구를 운용	공개기관이 추천하는 보안위험의 경감 방법을 보유하고 있음



〔그림 4〕 Secure MISRA-C 개념

프트웨어 개발 시 필요한 Secure MISRA-C가 필요할 것이다.

자동차의 안전성(Safety)은 ISO 26262를 준수함으로써 위험(Hazard)을 식별하고 관리하는 것이 가능하다. 하지만 현재 자동차 보안에 대한 위험(Risk)을 사전에 식별하기 위한 방법이 필요하며, 이는 "NIST SP 800-39 Managing Information Security Risk"를 통해 위험 관리가 가능할 것으로 기대된다.

Ⅴ. 결 론

자동차는 본 논문에서 제시한 Life-Cycle 내에서의 이해관계자에 따른 공급망에서의 보안성을 유지하고 관리하기 위한 방법이 매우 필요한 실정이다. 자동차의 안전성은 ISO 26262를 통해 대처할 수 있지만, 개발 단계에서부터 내재된 보안취약점과 외부 공격으로부터 시스템을 보호하는 보안기능 적용방안은 개발이 필요한 실정이다. 이를위해 향후 아래와 같은 연구가 필요할 것으로 예상된다.

(1) 자동차 소프트웨어 개발보안 표준 개발
- 자동차 소프트웨어 개발시 안전성과 보안성 확보를 위한 Secure MISRA-C 등에 관한 연구
- 자동차 소프트웨어의 안전성 및 보안성 검증, 시험도구, 시험 시나리오 등

(2) 자동차 공급망 위험관리 방안
- 자동차 공급망에서의 보안위험을 관리하기 위한 방법과 프로세스 및 통제방안 연구
- ISO 26262 안전분석(ASIL) 시 보안분석 및 검증, 시험도구, 시험 시나리오 등

(3) 자동차 소프트웨어 보안인증 체계 구축
· CC 인증제도와 유사한 형태의 자동차 소프트웨어 인증체계 방안 연구

(4) 자동차 시스템 내 취약점점검 및 모의해킹 방안 연구
· 자동차 임베디드 소프트웨어의 취약점 점검 및 모의해킹 방안 연구

(5) 자동차 보안 인력 양성
· 자동차 보안을 위한 보안개발, 보안시험, 보안품질시험, 보안테스트 전문인력 양성

(6) 국제 표준개발 참여 및 가이드라인 개발
· 자동차 보안을 위한 신규 표준 아이템 도출 및 제안
· 자동차 보안관련 국제표준에 기초한 자동차 보안 가이드라인 개발 및 배포 등

참 고 문 헌

[1] Seonghyun Yun, "A study on international standards and safety requirements for the development of automotive safety-related software", KSAE, 2009.

[2] Younho Kim, "A Method of System Requirements Specification Corresponding to ISO 26262 Functional Safety", KSAE, 2011.

[2] Automotive SPICE, "www.automotivespice.com", Introduction, 2013.

[4] IEC 61508, "Functional safety of E/E/PE safety-related systems", Part 1~7

[5]5ISO CD 26262, "Road vehicles ? Functional Safety", Part 1~9

[6] AUTOSAR, "Main Requirements", Sep. 2008.

[7] AUTOSAR, "Specification of operating system", Jun. 2008.

[8] Stephen Checkoway, "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX Security, pp.1-16, Nov. 2011.

[9] Kari Koscher, "Experimental Security Analysis of a Moderm Automobile", IEEE Symposium of Security and Privacy, pp.16-19, May. 2010.

[10] Ishtiaq Rouf, "Security and Privcy Vulnerabilities of In-Car Wireless Network: A Tire Pressure Monitoring System Case Study", USENIX Security, pp.1-16, Aug. 2010.

[11] 김강석, "CAN 통신 도청 및 조작을 통한 차량 ECU의 외부위협 가능성 분석", Korea University, Dec, 2010

[12] US: Researchers hack BMW, OnStar, Ford SYNC and Hyundai telematics, "http://telematicsnews.info/2011/07/29/us-researchers-hack-bmw-onstar-ford-sync-and-hyundai-telematics_jl2291", Telematicsnews, July. 2011.

[13] Hacker Disables More Than 100 Cars Remotely, "http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars" WIRED,

[14] Hackers steal Subaru Outback with smartphone, "http://content.usatoday.com/communities/driveon/post/2011/08/hackers-show-you-could-steal-a-subaru-with-your-smart-phone-black-hat-unlock-start/1#.UGPslbRjIRA", DRIVEON, Aug. 2011.

[15] SBS News, "http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1001371173", Sep. 2012.

[16] hankooki.com, "http://news.hankooki.com/lpage/world/201303/h2013032502344222450.htm", hankooki, Mar. 2013.

[17] Police admit they're 'stumped' by mystery car thefts, "http://www.today.com/news/police-admit-theyre-stumped-mystery-car-thefts-6C10169993", TODAY, Jun. 2013.

[18] 김원종, "Car Secrutiy Technology", ETRI, Jun. 2013.

[19] 임관택, "On the Improvement and Application of the FMEA Process in ISO 26262", AJOU University, Dec. 2013.

[20] Software Assurance in Acquisition and Contract Language, buildsecurityin.us-cert.gov, May. 2012.

[21] Rome, NY: Data and Analysis Center for Software, "Software Development Security: A Risk M

anagement Perspective," in The DOD Software Tech News? Secure Software Engineering 8, no. 2, July 2005).
[22] NIST SP800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations(Second Draft)", June. 2014.
[23] Approaches for Embedded System Information Security(2010 revised Edition), IPA, Feb. 2011.
[24] EVITA, "Security requirements for automotive on-board networks based on dark-side scenarios", July. 2008.
[25] IPA, "Approaches for Vehicle Information Security", Aug. 2013.

〈저자소개〉

김 동 원 (Dong-won Kim)
정회원

2009년 2월 : 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월 : 건국대학교 정보통신대학원 정보보호학과 석사
2012년 3월 : 고려대학교 정보보호대학원 정보보호학과 박사수료
2014년 3월~현재 : 서울호서전문학교 사이버해킹보안과 전임교수
관심분야 : 시큐어코딩, 지능형 차량 보안, 정형기법 등

한 근 희 (Keun-hee Han)
종신회원

서울과학기술대학교 컴퓨터공학과 졸업
한양대학교 과학대학원 공학석사
고려대학교 대학원 이학박사
현재 : 고려대학교 융합소프트웨어전문대학원 산학교수
〈관심분야〉 소프트웨어 보증, 시큐어 코딩, 정보보호 관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 자동차 보안 등