Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.4, Aug. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.4.793

자동차 공급망 위험관리(A-SCRM) 방안 연구*

김 동 원,[1†] 한 근 희,[2] 전 인 석,[1] 최 진 영[2‡]
[1]고려대학교 정보보호대학원, [2]고려대학교 융합SW대학원

A Study on Supply Chain Risk Management of Automotive*

Dong-won Kim,[1†] Keun-hee Han,[2] In-seok Jeon,[1] Jin-yung Choi[2‡]
[1]Graduate School of Information Security, Korea University,
[2]Graduate School of Convergence Software, Korea University

요 약

현대의 자동차는 안전필수(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 방안과 공급망에서 발생할 수 있는 위험을 식별, 평가 및 통제하기 위한 위험관리 방안이 필요하다. 본 논문에서는 자동차 Life-Cycle 내에서 이해관계자 별 위험관리(A-SCRM, Automotive Supply Chain Risk Management) 방법을 연구 제안한다.

ABSTRACT

Due to the rise of automotive security problems following automotive safety and the progress of the internet technology leading to a hyper-connected society, guaranteeing the safety of automotive requires security plans in the supply chain assurance and automotive software, and risk management plans for identifying, evaluating, and controlling the risks that may occur from the supply chain since the modern automotive is a Safety Critical system. In this paper, we propose a study on Automotive Supply Chain Risk Management (A-SCRM) procedures by person interested within the automotive Life-Cycle.

Keywords: Automotive Supply Chain Risk Management, A-SCRM, SSCA

I. 서 론

1.1 연구배경 및 목적

현대의 자동차는 사람에게 상해나 사망을 유발할 수 있는 안전필수(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[26], 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 프

접수일(2015년 3월 25일), 수정일(1차: 2015년 6월 4일, 2차: 2015년 7월 23일), 게재확정일(2015년 7월 24일)
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2015-H8501-15-1012)
† 주저자, blast.kim@gmail.com.
‡ 교신저자, choi@formal.korea.ac.kr(Corresponding author)

로세스를 구축하고, 안전관련 소프트웨어가 가지고 있어야 할 안전성 특성(Safety Property)을 이해하는 것은 자동차 전반의 안전성 보장을 위해 필수적인 일이다.[1]

이에 본 논문은 자동차 안전성과 관련된 국제표준 동향을 살펴보고, E/E/PE시스템의 안전성 관리 및 인증을 위한 국제표준인 IEC 61508[4]과 이를 기반으로 자동차 산업영역의 기능안전성 표준인 ISO 26262[5]가 제시하고 있는 안전성 관리 개념, 안전성 수준 평가방법, 소프트웨어 안전성 수준 보장을 위해 표준에서 권고하는 기술과 방법을 살펴본다. ISO 26262는 차량 E/E(Electrical/Electronic) 시스템의 잠재적인 재난요인 분석과 위험 평가(HARA, Hazard Analysis Risk Assessment)를 실시하고 이에 따른 안전목표(Safety Goal)와 기능 안전 요구사항(Safety Requirement)을 식별하여 관련 위험를 최소화하거나 제거하여 차량의 기능이 용인할 수 없는 위험한 상태를 초래하지 않도록 하는 일련의 안전프로세스 이다.[2] 또한 차량용 소프트웨어 개발 플랫폼인 AUTOSAR[6][7]와 ISO 26262에서 정하고 있는 차량용 소프트웨어 및 운영체제가 가지고 있어야 할 기능적 안전성 요구사항을 파악해 보고[1] 이를 통해 자동차의 안전한 공급망 보증을 위한 방안을 연구하고자 한다.

1.2 연구방법 및 구성

본 연구에서는 초 연결사회를 지향하는 사물인터넷 기술의 발전과 자동차의 스마트화 됨에 따른 자동차 보안문제가 대두됨에 따라 자동차 소프트웨어와 공급망에서의 보증 방안을 제시함으로써 효율적인 접근이 될 수 있도록 제안하고자 한다. 본 논문의 II장에서는 자동차 보안사고 사례 및 관련 표준에 대해서, III장에서는 자동차 보안위협 분석 실험을 통해 연구대상인 자동차 공급망 위험관리(A-SCRM)방안을 제시하고, 마지막으로 IV장에서는 본 논문의 결론으로 끝을 맺는다.

II. 관련 연구

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 다루어지고 있다.

Table 1. Vehicle of security incidents

Year	Descriptions	Ref
2010	Influence the control of brakes or wipers	[9]
2010	Raises the vulnerabilities of tire air pressure monitoring system	[10]
2010	ECU operation via WLAN receiver at OBD-II	[11]
2011	Hacking of Telematics Services that uses smart phones and SMS	[12]
2011	Malfunction in the vehicles occurred when the dealers' websystem (Webtech Plus) was hacked	[13]
2011	Using the Android Smart Phone, the password transmitted on mobile communication network was siezed and this was used to turn-on the ignition of the vehicle	[14]
2012	Hacking was done using Mobile Car Diagnostics App	[15]
2013	Neutralization of electronically controlled brake system	[16]
2013	Car theft through hacking	[17]

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

2.2 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, 제

품개발 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 요구사항이 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.

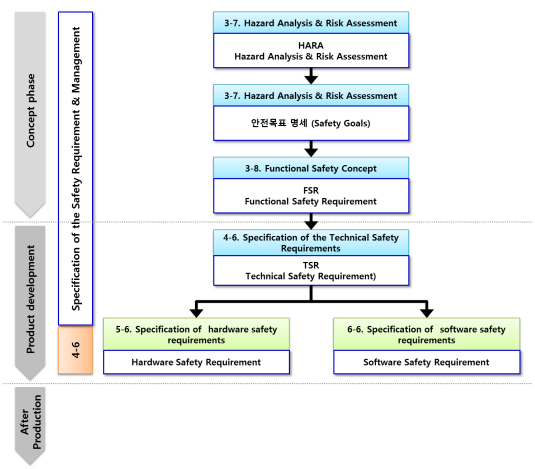

Fig. 1. Structure of the safety requirements

Table 2. Functional safety standards

Sectors	Standards
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

Table 3. RAMS

Attributes	Descriptions
Reliability	The ability to perform a required function without breaking down for a period of time according to the determined conditions of usage.
Availability	The ability to operate a system at any point
Maintainability	The ability to complete a goal within a predetermined time under specified conditions.
Safety	Design that guarantees minimization of accidents and damages in personel or equipment for a specified period in a limited condition

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 보안위협이 지속적으로 증가되고 있는 추세이다. ISO 26262의 기능안전에 보안(Confidentiality, Availability, Integrity)을 위한 방안의 필수적용이 필요할 것이다.

2.3 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 신뢰가능한지를 나타낸다. 소프트웨어는 "원하는 동작을 하는 신뢰 가능한 소프트웨어" 와 "보안취약점과 악의적 코드로부터 자유로운 소프트웨어"로 구분할 수 있다.[20] 소프트웨어 보증의 주요 역할은 과정, 절차, 그리고 제품에 대해 모든 표준과 요구사항을 만족하는 소프트웨어를 개발 또는 유지하기 위함이다.[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 공급망에서 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.

ISO 26262에 따르면 자동차 소프트웨어의 안전성을 확보하기 위한 방법으로서 MISRA-C 안전성 코딩규칙을 적용하도록 권고하고는 있으나[5], 보안

Table 4. CIA

Attributes	Descriptions
Confidentiality	Guarantees that no secret information has been leaked
Availability	Guarantees that an authorized person can use a service whenever needed
Integrity	Guarantees perfection of the information without omission or alteration

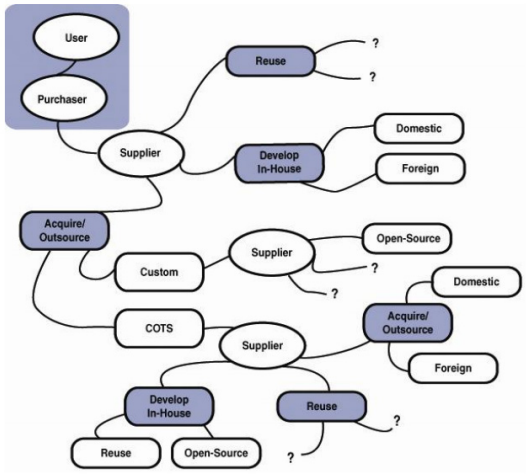

Fig. 2. Potential Software Supply Paths

성에 대한 부분은 언급되고 있지 않다. 자동차는 고장이 발생할 경우 안전하게 대처할 수 있는 기능안전은 ISO 26262를 통해 대처할 수 있지만, 외부 공격으로부터 시스템을 보호하는 보안기능 적용방안은 개발이 필요한 실정이다.

2.4 소프트웨어 & 공급망 보증 (SSCA, Software and 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, 정시납품과 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 제품 뿐만이 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.

III. 자동차 기능 분석

3.1 자동차 기능 분석

자동차에 있어서의 보안을 고려할 때에는 자동차 본체뿐만 아니라 자동차에 탑재되는 기기나 자동차와 통신을 수행하는 기기 및 제공되는 서비스의 전체를 대상으로 하여야 한다. 현대의 자동차는 Power Train, Chassis, Body, Infotainment(Head Unit/Telematics, etc)로 구분할 수 있다. 각 부분은 차량 네트워크(CAN, LIN, FlexRay, MOST, etc)를 통해 연결된다.

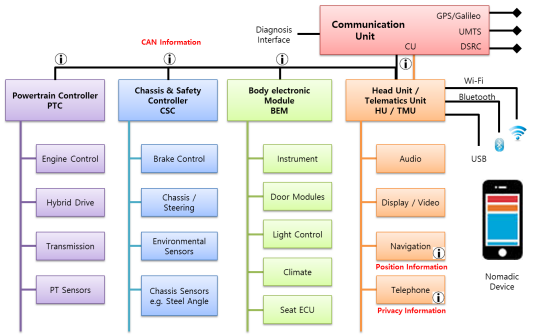

Fig. 3. Automotive on-board Network Architecture [24]

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]

Table 5. Functional classification of Vehicles[8]

Category	Classification of Function	Function
Vehicle control	Power Train	Function of the engine control, such as an automobile transmission station
	Chassis	Basic features, such as power generation, power transmission, steering, brake lights, for operating a car
	Body	Functions for operating body electrical component, typical device, lamp type, chair type, etc.
Uncontrolled Vehicle	Check/ Reuse	Using vehicle scanner and OBD-II, to be able to give fault diagnosis according to the vehicle's condition and to repair it

		accordingly
	Telematics Unit	A unit that provides various remote services such as internet and location tracking using mobile communication and broadcasting network.
	Head Unit	A unit that provides audio, video and navigation functions.
	ITS/V2X	Funtion that provides different application services such as automatic fare collection, automatic control, accident prevention using the facilities surrounding the vehicles and communication among vehicles
in vehicle N/W	Vehicle Networks	Vehicle internal networks, like CAN, CAN FD, LIN, for the implementation of functions within the vehicle
	X by Wire	Techniques for electronically controlling devices such as existing machine or steering wheel, brake.

자동차의 공격지점은 크게 직접적인 물리적 공격 지점, 간접적인 물리적 공격 지점, 근거리 원격/무선 공격 지점으로 분류할 수 있다.[8,9,18]

IV. 자동차 공급망 위험관리 방안

4.1 자동차 자산 및 보안위협 분석 실험

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[25], EVITA(E-safety Vehicle Intrusion protected Applications)의 Attack Tree를 참조하였다.[24]

자동차에서 보호해야할 정보 등의 자산에는 크게

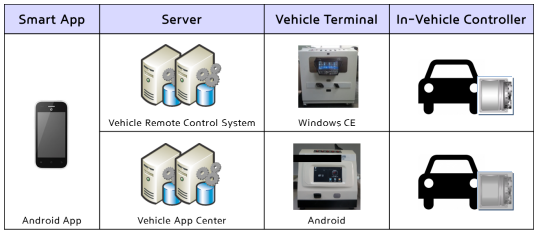

Fig. 4. Vehicle penetration test experiment environment

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

Table 6. Information and Other Assets Vehicles Should Protect[25]

Objects that should be protected	Descriptions
Operation of "Basic control functions"	Coherence and availability of "Basic control functions", execution environment of "Basic control functions", communications for the operation.
Information unique to the vehicle	Information which is unique to the car body(vehicle ID, device ID, etc), authentication code, and accumulated information such as running history and operation history.
Vehicle status information	Data representing the vehicle's stratus such as location, running speed, and destination.
User information	Personal information, authentication information, billing information, usage history and operation history of the user (driver/passengers).
Software	Software which is related to vehicles' "Basic control functions" and "Expanded functions". Examples include firmware for ECU.
Controls	Data for applications for video, music, map, etc.
Configuration information	Setting data for the behavior of hardware, software, etc.

실수(이용자에 의한 조작) 등에 의한 위협도 포함하여야 한다. 이용자에 의한 조작은 크게 2가지로 분류할 수 있다.[25]

Table 7. Threats Posed by User Operation[25]

Threat	Description
Incorrect settings	Threats caused by incorrect operations or settings by users, done through the user interface within the vehicle. Examples include: accidentally sending personally identifiable information to an unintended service provider while using infotainment feature; and disabling cryptic functionality of telematics communication, allowing the communications to be sniffed
Virus infection	Threats caused by the infection of viruses or malicious software (malware etc.) to the in-vehicle systems, via a devices or storage medium brought into by the user. Examples include: a virus which infected an infotainment device spreads to the other in-vehicle equipments via the in-vehicle LAN.

공격자에 의한 간섭은 크게 8가지로 분류할 수 있다.[25]

Table 8. Threats Posed by Attackers' Interference[25]

Threat	Description
Unauthorized use	The automotive system's functions may be used by an unauthorized individual, such as through spoofing or an attack to vulnerability within the equipment. Examples include: an attacker unlocking the vehicle by spoofing as the driver and performing the communication to unlock the vehicle
Unauthorized setting	The automotive system's setting values may be altered by an unauthorized individual, such as through spoofing or an attack to vulnerability within the equipment. Examples include: an attacker altering network settings to make normal communication impossible
Information leakage	The information that the automotive system should protect may be obtained by an unauthorized individual. Examples include: an attacker accessing accumulated contents or user information for various services, through the intrusion to the equipment or communication sniffing.
Sniffing	Communications between the in-vehicle equipments within the vehicle or communications between the vehicle and the peripheral systems may be sniffed or intercepted. Examples include: an attacker sniffing the vehicle's status information (running speed, location information etc.), while it is on the way from the vehicle to the peripheral systems for services such as navigation and traffic jam forecast.
DoS/DDoS	The system may go down or the service may be denied due to unauthorized or excessive connection requests Examples include: an attacker performing excessive communications with the smart key to make a request for door lock and unlock by the user unaccepted.
Tampered message	A tampered message may be sent by an attacker to cause false move/display of the vehicle. Examples include: an attacker tampering a TPMS (Tire Pressure Monitoring System) message, so that the caution-advisory indicator of a normal vehicle blinks.
Loss of logs	The operation history may be deleted or altered by an attacker to make after-the-fact inspection impossible. Examples include: an attacker altering logs to destroy the evidence of the attack.
Unauthorized relay	The communication path may be manipulated by an attacker to hijack legitimate communications or to improper communications. Examples include: an attacker relying the smart key's electric wave and unlocking the vehicle from a remote site

실제 자동차 모의해킹과 관련 자료 분석을 통해 자동차의 보안위협을 분석하였다. 이러한 자동차의 보안위협을 제거하고 정보자산을 보호하기 위한 방안이 필요하다. 본 논문에서는 자동차 보안위협 분석 실험결과를 참고하여 자동차 공급망 위험관리 프로세스

모델을 연구 제안한다.

4.2 자동차 시스템의 라이프 사이클

자동차 보안을 향상시키기 위해서는 자동차에 연관되는 다양한 정보자산을 대상으로 하여 그 가치에 맞는 적절한 보안 대책을 수행해야 할 필요가 있다.[25] 본 논문에서는 자동차 시스템의 라이프 사이클을 [기획], [개발], [운용], [폐기]의 4개의 과정으로 분류하여 연구한다.

자동차의 라이프 사이클의 각 과정에서 관여하는 조직과 관계자 들은 다음과 같다.

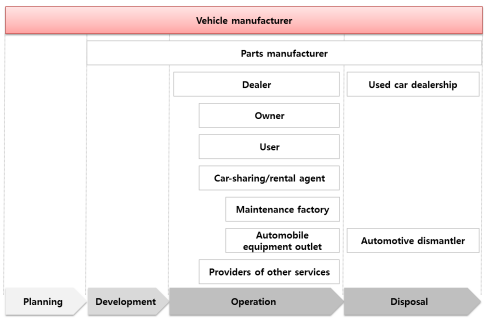

Fig. 5. Life-cycle of Automotive Systems

Table 9. Those Involved in a vehicle during its Life-cycle[25]

Those involved in vehicles	Description
Vehicle manufacturer	The vehicle's manufacturer. It engages in planning and development(design, implementation and manufacturing), sales, maintenance of the vehicle. Vehicle manufacturer is responsible for the manufacturing of the vehicle.
Vehicle parts manufacturer	Upon receiving commission from a vehicle manufacture, it develops and delivers the components of the in -vehicle systems.
Dealer	Sells the vehicle to a customer. It may have a maintenance factory.
Owner	The ne who owns the vehicles (excluding car-sharing/rental agent)
User	The one who drivers/uses the vehicle (may be identical to the owner)
Car-sharing/ rental agent	A business entity that rents the vehicles to a customer.
Maintenance factory	Conducts car inspection, maintenance and repair, etc.
Vehicle equipment outlet	A business entity that sells/installs add-on in-vehicle equipments or vehicle parts.
Providers of other services	A business entity that develops and distributes software for in-vehicle equipments or brought-in devices, such as for telematics and contents delivery, and that provides services for vehicles.
Used car dealership	Takes the vehicle whose use is terminated and resells it.
Automotive dismantler	Takes the vehicle whose use is terminated and dismantles it.

자동차 시스템의 라이프 사이클 및 관여하는 조직 및 관계자 연구결과는 자동차 공급망 위험관리 프로세스(A-SCRM)의 Frame 연구에 사용된다.

4.3 자동차 공급망 위험 관리 프로세스(A-SCRM, Automotive-Supply Chain Risk Management) 제안

현재 자동차는 ISO 26262를 준수함으로써 안전성에 대한 보증이 가능하다. 하지만 보안성에 대한 보증 방안을 마련하기 위한 절차와 방법이 필요한 실정이다. 이에

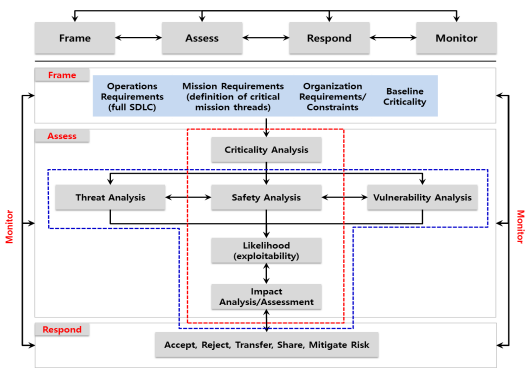

Fig. 6. Automotive SCRM Risk Assessment Process

본 논문에서는 NIST SP800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"[22]을 참조하여 자동차 공급망 위험관리 프로세스를 연구하여 다음과 같이 [Fig. 5 Automotive SCRM Risk Assessment Process]를 제안한다. 각 프로세스는 [입력(Input)] → [단계(Step)] → [출력(Output)] 으로 구성되어 SCRM을 수행한다.

4.4 기준 정의 단계

기준 정의 단계는 3계층(평가단계(Assess), 처리단계(Respond), 확인단계(Monitor))에 대한 Context를 설정하는 단계이다. 즉, 범위와 조직, 전반적인 위험관리 전략뿐만 아니라 프로그램, 프로젝트 또는 개별 정보시스템 요구사항 등을 정의한다. 이는 3계층의 입력으로 사용된다. Frame 단계에서의 입력으로는 조직의 정책, 전략, Governance, 적용 가능한 법률 및 규정, 사업 목표와 조직의 위협, 취약성, 위험, 안전 요구사항 및 보안 요구사항 등을 가정해 볼 수 있을 것이다. 이것들은 Frame 단계에서 정의되거나 식별 된 후 자동차 공급망 위험관리를 위한 기준으로 다음단계의 입력으로서 활용된다.

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 식별이 가능할 것이다.

Table 10. Automotive in the Frame Step

Inputs	- Polices, strategies, governance - Business goals - Customer requirements - Safety requirements - Security requirements - Threat, vulnerabilities, risk - etc
↓	
Frame	- Define Automotive SCRM requirements - Define Baseline Automotive SCRM policy - Integrate Automotive SCRM
↓	
Outputs	- Baseline criticality - Automotive SCRM policy - Automotive SCRM requirements

4.5 평가 단계

평가 단계는 수집된 모든 데이터를 이용하여 위험평가를 수행하는 단계이다. 입력된 데이터에 따라 가능성(Likelihood)과 영향도(Impact), 위협 및 취약성, 안전성(ASIL) 분석 결과를 포함 한다.

본 논문에서 제안하는 A-SCRM 프로세스는 ① 안전경로(Safety Path)와 ②보안경로(Securtiy Path)로 구분할 수 있다. 안전 경로는 ISO 26262의 ASIL 분석 및 평가를 통해 확보할 수 있다. 하지만 보안경로는 현재 그 방법과 기준이 불분명하다.

자동차 모의해킹을 통한 자동차 보안위협 분석 결과와 자동차 보안사고 사례를 기초로 자동차 전장소프트웨어 개발 시 보안약점(Security Weakness)을 제거하고 취약점을 사전에 예방하기 위한 활동이 필요하다. [Fig.8 Assess example]과 같이 자동차 정보자산에서의 보안위협 및 취약점이 자동차 Life-Cycle 내에서 이해관계자 별 보안대상과 방법

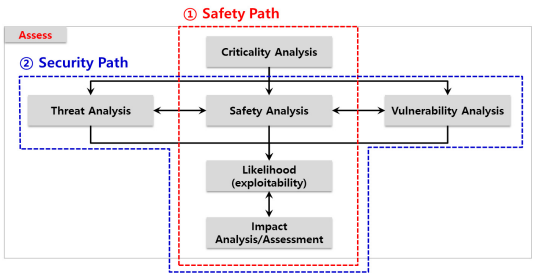

Fig. 7. Safety & Security Path

Table 11. Automotive in the Assess Step

Inputs	- Frame Outputs - Automotive Assets - Automotive Threats and Vulnerability
↓	
Assess	- Threat analysis - Safety analysis - Vulnerability analysis - Risk Assessment
↓	
Outputs	- Mission risks - Identification of critical components - Automotive supply chain risk assessment for individual systems

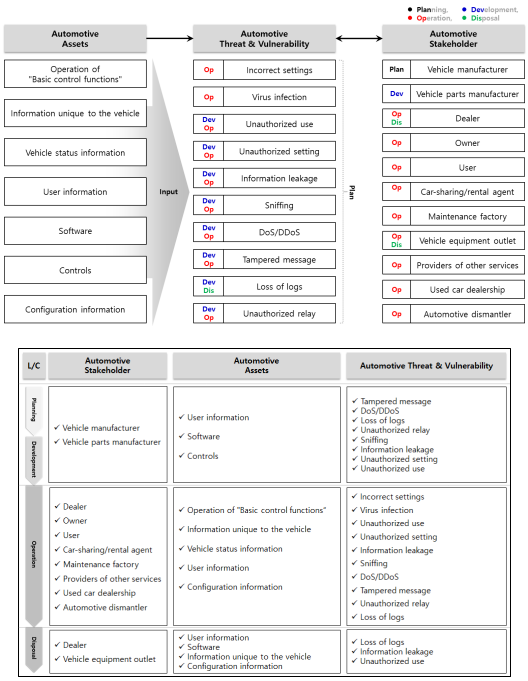

Fig. 8. Assess example

등을 분석한다.

4.6 실행 단계

실행 단계는 안전경로와 보안경로에서 분석하고 평가된 위험을 통제하기 위한 수단을 결정한다.

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 구성하였다.

Table 12. Automotive in the Respond Step

Inputs	- Assess Outputs
↓	
Respond	-Make mission/business-level risk decisions to avoid, mitigate, share, or transfer risk - Select, tailor, and implement appropriate system-level controls - Document ICT SCRM controls in System Security Plan
↓	
Outputs	- Risk decisions - Implemented controls - Updated System Security Plan

4.7 모니터링 단계

모니터링 단계는 위험수준이 허용가능 한 범위에서 유지되기 위하여 위험수준을 조정하기 위해 평가되는 단계이다. 조직의 공급망에 대한 변경은 전체적인 자동차 공급망 프로세스에 영향을 미칠 수 있기 때문에 이러한 변경을 추적하고 평가하여 그 영향에 대한 평가가 이루어지고 있음을 보장하는 단계이다. 이를 통해 자동차 공급망에서의 위험관리 방안을 보완하고 갱신하여 주기적인 관리가 될 수 있도록 도와준다.

4.8 자동차 공급망 위험 관리 프로세스 적용

국내 자동차 제조사에서 본 연구 A-SCRM에서 제시한 프로세스를 기초로 하여 〔기준정의 단계〕에서 제시한 자동차 보안정책으로 자동차용 텔레매틱스 단말기 개발시 필요한 개발보안 가이드와 Application 가이드라인을 개발하여 적용하였으며, 자체점검을 통해 개발보안을 적용할 수 있도록 개발프로세스를 변경하였다. 자동차의 품질을 책임지고 있는 품질본부는 〔평가단계〕에서 제시한 보안위협 및 취약점 분석과 확인 및 보완을 위하여 "자동차 IT 보안 프로세스"를 수립하여 품질관리 프로세스에 2015년부터 적용 준비중이다.

또한, 정비공장 및 정비소, 정비원의 인증을 위한 절차를 수립하고 있으며, 시스템을 구축하기 위한 활동을 진행하고 있다. 자동차용 소프트웨어는 타 소프트웨어와는 다르게 개발기간이 평균 4년, 시장수명 평균 7년 이상의 생명주기를 갖고 있다. 개발 시 최신기술을 적용하고 있으나 출시까지 약 4년이 소요되기 때문에 본 연구에서 제안하는 자동차 IT 보안 프로세스의 효과성을 측정하기에는 한계가 있다.

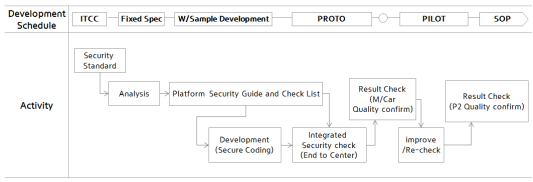

Fig. 9. Security Quality Confirm Process for vehicle development

Table 13. Risk control example[25]

Level	Management policy	Planning / Development
L1	No security effort is done.	Security is not taken into account when planning and designing a product
L2	Security effort is relegated to the on-the-spot personnel (such as planner, or developer). Issues are dealt with separately at each project.	Security consideration is relegated to the on-the-spot personnel (such as planner, or developer).
L3	Security effort is considered as an organizational issue. A security policy is drawn up and enforced.	Secure development based on the organization's policy is done.
L4	Security effort is considered as an organizational issue. A security policy is drawn up and enforced, and an audit is also conducted.	Secure development based on the organization's policy is done. And the contents are evaluated objectively.
Level	**Operation policy**	**Disposal policy**
L1	No considered that how to respond to security problems arising after the product is shipped.	No Considered that how to handle residual information.
L2	It is determined by on-the-spot personnel (such as customer representative, or developer) that how to respond to security problems arising after the product is shipped.	It is mentioned in the specification documents that how to remove residual information.
L3	It is established as an organizational policy that how to respond to security problems arising after the product is shipped.	A disposal procedure that mitigates the security risk is available.
L4	It is established as an organizational policy that how to respond to security problems arising after the product is shipped. The organization has a contact point for external parties, which handle	A disposal procedure that mitigates security risks, which is recommended by an official body, is available.

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. 자동차 소프트웨어의 안전성을 확보하기 위한 방법으로서 MISRA-C 안전성 코딩규칙에 보안성을 고려한 Secure MISRA-C에 관한 연구와 더불어서, 안전분석(ASIL) 시 보안을 고려하여 자동차 전장소프트웨어의 안전성과 보안성을 확보하기 위한 연구가 필요할 것이다.

References

[1] Seonghyun Yun, "A study on international standards and safety requirements for the development of automotive safety-related software," KSAE, pp. 1884-1890, Sep. 2009.

[2] Younho Kim, "A Method of System Requirements Specification Corresponding to ISO 26262 Functional Safety," KSAE, pp. 1548-1553, Sep. 2011.

[3] Automotive SPICE, www.automotivespice.com, Introduction, 2013.

[4] IEC 61508, "Functional safety of E/E/PE safety-related systems," IEC, Part 1~7, 1999.

[5] ISO CD 26262, "Road vehicles Functional Safety," ISO, Part 1~9, Nov. 2011.

〔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〕 Kang-suk Kim, "Analysis of potential external threats vehicle ECU via CAN communications eavesdropping and manipulation," Master. Thesis, 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#.VcB3YvntlBc," 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/wor ld/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〕 Won-jong Kim, "Car Securtiy Technology," NIPA, Week Technology Trends, vol. 1601, pp. 10-20, Jun. 2013.
〔19〕 Guan-tak Lim, "On the Improvement and Application of the FMEA Process in ISO 26262," Ph.D. Thesis, AJOU University, Dec. 2013.
〔20〕 Software Assurance, "Software Assurance in Acquisition and Contract Language," buildsecurityin.us-cert.gov, Acquisition & Outsourcing, Vol. 1, May. 2012.
〔21〕 Rome, NY: Data and Analysis Center for Software, "Software Development Security: A Risk Management 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)." NIST, June. 2014.
〔23〕 IPA "Approaches for Embedded System Information Security(2010 revised Edition)," IPA, Sep. 2010.
〔24〕 EVITA, "Security requirements for automotive on-board networks based on dark-side scenarios," EVITA, July. 2008.
〔25〕 IPA, "Approaches for Vehicle Information Security," IPA, Aug. 2013.
〔26〕 Young-Hun Ki, "Implementation of the Integrated ESP and ACC in a CAN-Based Control System," KSAE, pp. 2231-2236, Jun. 2007.

〈저자소개〉

김 동 원 (Dong-Won Kim) 종신회원
2009년 2월: 서울과학기술대학교 컴퓨터공학과 졸업
2012년 2월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 2월: 고려대학교 정보보호대학원 정보보호학과 박사 수료
2014년 2월: 현대오토에버 정보보안기술팀 과장
2014년 3월~현재: 서울호서전문학교 사이버해킹보안과 전임교수
〈관심분야〉 시큐어코딩, 정보보호, 모바일 보안, 지능형 차량 보안, SSCA, 정형기법 등

한 근 희 (Keun-Hee Han) 종신회원
서울과학기술대학교 컴퓨터공학과 졸업
한양대학교 공학대학원 공학석사
고려대학교 대학원 이학박사
현재: 고려대학교 융합소프트웨어전문대학원 산학교수
〈관심분야〉 소프트웨어 보증, 시큐어 코딩, 정보보호관리 체계, 개인정보보호, 클라우드 컴퓨팅 보안, 스마트 의료 보안, 스마트 자동차 보안 등

전 인 석 (In-seok Jeon) 종신회원
2009년 8월: 건국대학교 정보통신대학원 정보보호학과 석사
2014년 9월: 고려대학교 정보보호대학원 정보보호학과 박사 과정
2009년 9월~현재: Ahnlab CERT팀 주임 연구원
〈관심분야〉 네트워크보안, 정보보호관리체계, 정형기법 등

최 진 영 (Jin-Young Choi) 종신회원
1982년 서울대학교 컴퓨터공학과 (학사)
1986년 미국 Drexel University, Dept. of Mathematics and Computer Science (석사)
1993년 미국 Univ. of Pennsylvania, Dept. of Computer and Information Science (박사)
1996년~현재 고려대학교 컴퓨터·전파통신공학부 교수
〈관심분야〉 정형기법, 임베디드 실시간시스템, 프로그래밍언어, 프로세스 대수, 소프트웨어 공학