(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0013872
(43) 공개일자 2022년02월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/57 (2013.01) *G06F 21/55* (2013.01)
(52) CPC특허분류
G06F 21/57 (2013.01)
G06F 21/55 (2013.01)
(21) 출원번호 10-2020-0135754
(22) 출원일자 2020년10월20일
심사청구일자 2020년10월20일
(30) 우선권주장
1020200092969 2020년07월27일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
김승주
서울특별시 강남구 도곡로57길 12, 103동 503호(역삼동, 역삼2차아이파크)
정승연
서울특별시 양천구 목동동로 130, 1410동 102호(신정동, 목동신시가지아파트14단지)
강수영
서울특별시 성북구 월곡로14길 26, 108동 1302호(하월곡동, 월곡래미안루나밸리)
(74) 대리인
이대호, 박건홍

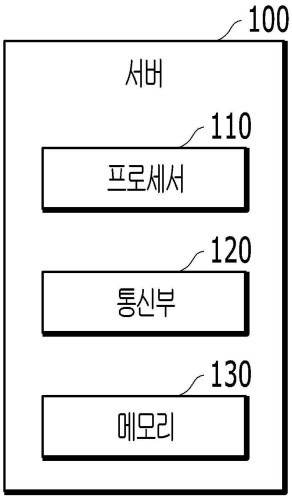
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **자동차 개발 프로세스에서의 보안 내재화 방법론**

(57) 요 약

본 개시의 몇몇 실시예에 따라, 컴퓨팅 장치의 프로세서를 이용한 자동차 보안내재화 방법이 개시된다. 상기 방법은: 기업체의 안전(Safety) 개발 방법론에 대응하는 보안(cybersecurity) 수준을 획득하는 단계; 상기 보안 수준에 기초하여, 보안내재화 방법론을 획득하는 단계; 상기 보안내재화 방법론 및 상기 안전 개발 방법론을 통합하는 단계; 및 상기 통합의 결과물을 데이터베이스에 저장하는 단계;를 포함할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업

과제고유번호	1711102808
과제번호	20170001840042004
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보보호핵심원천기술개발
연구과제명	자기학습형 사이버 면역 기술 개발
기 여 율	1/1
과제수행기관명	고려대학교
연구기간	2020.01.01 ~ 2020.12.31

명 세 서

청구범위

청구항 1

컴퓨팅 장치의 프로세서를 이용한 자동차 보안내재화 방법으로서, 상기 방법은:

기업체의 안전(Safety) 개발 방법론에 대응하는 보안(cybersecurity) 수준을 획득하는 단계;

상기 보안 수준에 기초하여, 보안내재화 방법론을 획득하는 단계;

상기 보안내재화 방법론 및 상기 안전 개발 방법론을 통합하는 단계; 및

상기 통합의 결과물을 데이터베이스에 저장하는 단계;

를 포함하는,

자동차 보안내재화 방법.

청구항 2

제 1 항에 있어서,

상기 결과물은,

맞춤형 신뢰 보안 개발 프로세스, 적어도 하나의 맞춤형 보안 개발 수행 활동 및 산출물을 포함하는,

자동차 보안내재화 방법.

청구항 3

제 2 항에 있어서,

상기 맞춤형 신뢰 보안 개발 프로세스는,

보안 교육과 관련된 제 1 단계, 착수 및 계획과 관련된 제 2 단계, 요구사항 분석과 관련된 제 3 단계, 획득과 관련된 제 4 단계, 설계와 관련된 제 5 단계, 구현과 관련된 제 6 단계, 검증과 관련된 제 7 단계, 배포와 관련된 제 8 단계, 운영과 관련된 제 9 단계 및 폐기와 관련된 제 10 단계 중 적어도 하나를 포함하는,

자동차 보안내재화 방법.

청구항 4

제 1 항에 있어서,

상기 기업체의 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계는,

상기 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득하는 단계;

상기 안전 수준이 기 설정된 최소 안전 수준 미만인 경우, 상기 기 설정된 최소 안전 수준에 대응하는 기초 안전 개발 방법론을 획득하는 단계; 및

상기 기초 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계;

를 포함하는,

자동차 보안내재화 방법.

청구항 5

제 1 항에 있어서,

상기 기업체의 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계는,

상기 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득하는 단계; 및

상기 안전 수준이 기 설정된 최소 안전 수준 이상인 경우, 상기 기업체의 상기 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계;

를 포함하는,

자동차 보안내재화 방법.

청구항 6

제 1 항에 있어서,

상기 보안 수준에 기초하여, 보안내재화 방법론을 획득하는 단계는,

상기 보안내재화 방법론과 증거 기반 보안 방법론이 매핑되어 저장된 상기 데이터베이스에서 상기 보안 수준에 대응하는 상기 보안내재화 방법론을 획득하는 단계;

를 포함하는,

자동차 보안내재화 방법.

청구항 7

제 1 항에 있어서,

상기 보안내재화 방법론 및 상기 안전 개발 방법론을 통합하는 단계는,

상기 보안내재화 방법론에서 자동차 개발과 관련된 적어도 하나의 특정 표준을 선정하는 단계;

상기 적어도 하나의 특정 표준에서 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출하는 단계; 및

상기 적어도 하나의 수행 활동에 증거 기반 표준 중 적어도 하나를 매핑하여, 자동차 보안개발 프로세스 표준을 생성하는 단계;

를 포함하는,

자동차 보안내재화 방법.

청구항 8

제 7 항에 있어서,

상기 적어도 하나의 특정 표준은,

소프트웨어 개발과 관련된 표준, 시스템 개발과 관련된 표준, 기업의 모범 사례와 관련된 표준 및 자동차 보안과 관련된 표준 중 적어도 하나를 포함하는,

자동차 보안 내재화 방법.

청구항 9

제 7 항에 있어서,

상기 적어도 하나의 특정 표준에서 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출하는 단계는,

상기 적어도 하나의 특정 표준에 포함된 적어도 하나의 자동차 관련 키워드를 이용하여, 상기 자동차 개발과 관련된 상기 적어도 하나의 수행 활동을 추출하는 단계;

를 포함하는,

자동차 보안 내재화 방법.

청구항 10

제 7 항에 있어서,

상기 적어도 하나의 수행 활동에 증거 기반 표준 중 적어도 하나를 매핑하여, 자동차 보안개발 프로세스 표준을 생성하는 단계는,

상기 적어도 하나의 수행 활동과 관련된 적어도 하나의 제 1 키워드와 정보 보호 제품의 보안성 표준, 기업 보안과 관련된 표준, 개인 정보 보안과 관련된 표준 및 자동차 기능 안정성과 관련된 표준 각각과 관련된 적어도 하나의 제 2 키워드에 기초하여, 상기 적어도 하나의 수행 활동에 상기 정보 보호 제품의 보안성 표준, 상기 기업 보안과 관련된 표준, 상기 개인 정보 보안과 관련된 표준 및 상기 자동차 기능 안정성과 관련된 표준 중 적어도 하나를 매핑하는 단계;

를 포함하는,

자동차 보안내재화 방법.

발명의 설명

기 술 분 야

[0001] 본 개시는 보안 내재화 방법론에 관한 것으로, 구체적으로 자동차 시스템에서 활용 가능한 자동차 보안 내재화 방법론에 관한 것이다.

배 경 기 술

[0002] 전통적으로 자동차 산업에서 개발은 기능 안전성 (Functional Safety)에 초점을 맞추어 왔다. 기능 안전성은 제품이 설계된 대로 정확하게 동작하는지를 판단하는 정확성과 제품 내부에서 발생한 오류가 외부로 표출되어 사용자에게 피해를 줄 수 있는지를 판단하는 안전성을 포함하는 개념이다. 기능 안전성이 보장되지 않으면 이는 단순한 시스템 동작 오류뿐만 아니라 인명 피해 사고로 이어질 수 있다. 따라서, 국제 표준화 기구 ISO(International Organization for Standardization)에서는 ISO 26262라는 자동차 기능 안전성 관련 표준을 제정하여 자동차 개발 프로세스 전반에 걸쳐 기능 안전성을 고려할 수 있도록 하였다.

[0003] 이러한 기능 안전성과 다르게 보안성은 자동차 개발에서 아직까지 중점적으로 다루어지지 않았다. 여기서, 보안성은 인가된 사용자만이 시스템의 정보 자산에 접근할 수 있도록 보장하는 기밀성(Confidentiality), 부적절한 정보의 변경이나 파기 없이 시스템이 완전하게 보존됨을 보장하는 무결성(Integrity), 시스템 정보에 대한 접근과 사용을 항상 보장하는 가용성(Availability)을 포함할 수 있다. 이러한 보안성이 보장되지 않으면 인명 피해나 프라이버시 유출 등의 다양한 사고로 이어질 수 있다. 최근 커넥티드 카의 등장과 함께 자동차의 소프트웨어 비중 및 인터넷 연결성이 높아지면서 자동차가 보안 위협에 노출될 가능성이 커지고 있다. 이에 따라 자동차 해킹 사례 또한 증가하고 있다. 따라서, 보안성이 확보된 자동차 개발에 대한 필요성이 높아지고 있으며, 여러 국제기관에서도 자동차 사이버보안 규제를 제정함으로써 이를 강조하려는 노력을 보이고 있다. 특히, UNECE(United Nations Economic Commission for Europe)가 제정 중인 자동차 사이버보안 규제의 경우 신차를 기준으로 2022년부터 적용되는데, 이에 따르면 해당 규제에서 정한 기준에 맞춰 평가 및 인증을 받지 못한 자동

차는 유럽에 수출할 수 없게 된다. 따라서, 보안성이 확보된 자동차 개발은 다양한 보안 위협뿐만 아니라 당장 직면하게 될 자동차 수출 및 수입 경제에도 중요한 쟁점이 될 수 있다.

[0004] UNECE 자동차 사이버보안 규제에서는 핵심 요구사항으로 보안 내재화를 제시하고 있다. 여기서, 보안 내재화란 개발 초기부터 제품의 정확성, 안전성, 보안성 등의 요소를 모두 고려하여 신뢰 가능한 제품을 구현하는 개념이다. 특히, 자동차 개발은 생명주기가 길고 공급망이 복잡하므로 개발 이후에 아키텍처를 변경하는 것이 매우 어렵다. 따라서, 자동차 개발에 있어 보안 내재화는 더욱 중요하게 다루어져야 하는데, 이러한 보안 내재화는 Secure SDLC(Software Development Life Cycle)를 통해 달성할 수 있다. Secure SDLC는 제품 개발 생명주기 전반에 적용되는 체계적인 보안 개발 프레임워크로 Microsoft와 같은 기업 또는 NIST와 같은 표준 기관 등에서 활용하고 있으며, 관련 연구 또한 활발하게 이루어지고 있다.

[0005] 하지만, 기존 Secure SDLC 표준은 주로 소프트웨어를 대상으로 할 뿐만 아니라 체계적인 요구사항 도출, Third-party 구성요소에 대한 획득과 같은 서로 다른 측면의 활동을 강조하고 있다. 즉, 기존의 보안 내재화와 관련된 표준은 자동차 보안 내재화에 대한 전반적이고 구체적인 방법론을 제시하지 못하는 경우가 대부분인 실정이다. 또한, 상술한 UNECE 자동차 사이버보안 규제에서도 보안 내재화를 달성하기 위한 구체적인 방법론을 제시하지 않는 실정이다.

[0006] 따라서, 자동차 보안 내재화 방법론에 대한 연구의 필요성이 당업계에 존재할 수 있다.

선행기술문헌

특허문헌

[0007] (특허문헌 0001) 미국 공개특허 US2013-0019315

발명의 내용

해결하려는 과제

[0008] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 자동차 보안 내재화 방법론을 제공하고자 한다.

[0009] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 컴퓨팅 장치의 프로세서를 이용한 자동차 보안내재화 방법을 개시한다. 상기 방법은: 기업체의 안전(Safety) 개발 방법론에 대응하는 보안(cybersecurity) 수준을 획득하는 단계; 상기 보안 수준에 기초하여, 보안내재화 방법론을 획득하는 단계; 상기 보안내재화 방법론 및 상기 안전 개발 방법론을 통합하는 단계; 및 상기 통합의 결과물을 데이터베이스에 저장하는 단계;를 포함할 수 있다.

[0011] 또한, 상기 결과물은, 맞춤형 신뢰 보안 개발 프로세스, 적어도 하나의 맞춤형 보안 개발 수행 활동 및 산출물을 포함할 수 있다.

[0012] 또한, 상기 맞춤형 신뢰 보안 개발 프로세스는, 보안 교육과 관련된 제 1 단계, 착수 및 계획과 관련된 제 2 단계, 요구사항 분석과 관련된 제 3 단계, 획득과 관련된 제 4 단계, 설계와 관련된 제 5 단계, 구현과 관련된 제 6 단계, 검증과 관련된 제 7 단계, 배포와 관련된 제 8 단계, 운영과 관련된 제 9 단계 및 폐기와 관련된 제 10 단계 중 적어도 하나를 포함할 수 있다.

[0013] 또한, 상기 기업체의 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계는, 상기 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득하는 단계; 상기 안전 수준이 기 설정된 최소 안전 수준 미만인 경우, 상기 기 설정된 최소 안전 수준에 대응하는 기초 안전 개발 방법론을 획득하는 단계; 및 상기 기초 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계;를 포함할 수 있다.

[0014] 또한, 상기 기업체의 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계는, 상기 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득하는 단계; 및 상기 안전 수준이 기 설정된 최소 안전 수준

이상인 경우, 상기 기업체의 상기 안전 개발 방법론에 대응하는 보안 수준을 획득하는 단계;를 포함할 수 있다.

[0015] 또한, 상기 보안 수준에 기초하여, 보안내재화 방법론을 획득하는 단계는, 상기 보안내재화 방법론과 증거 기반 보안 방법론이 매핑되어 저장된 상기 데이터베이스에서 상기 보안 수준에 대응하는 상기 보안내재화 방법론을 획득하는 단계;를 포함할 수 있다.

[0016] 또한, 상기 보안내재화 방법론 및 상기 안전 개발 방법론을 통합하는 단계는, 상기 보안내재화 방법론에서 자동차 개발과 관련된 적어도 하나의 특정 표준을 선정하는 단계; 상기 적어도 하나의 특정 표준에서 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출하는 단계; 및 상기 적어도 하나의 수행 활동에 증거 기반 표준 중 적어도 하나를 매핑하여, 자동차 보안개발 프로세스 표준을 생성하는 단계;를 포함할 수 있다.

[0017] 또한, 상기 적어도 하나의 특정 표준은, 소프트웨어 개발과 관련된 표준, 시스템 개발과 관련된 표준, 기업의 모범 사례와 관련된 표준 및 자동차 보안과 관련된 표준 중 적어도 하나를 포함할 수 있다.

[0018] 또한, 상기 적어도 하나의 특정 표준에서 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출하는 단계는, 상기 적어도 하나의 특정 표준에 포함된 적어도 하나의 자동차 관련 키워드를 이용하여, 상기 자동차 개발과 관련된 상기 적어도 하나의 수행 활동을 추출하는 단계;를 포함할 수 있다.

[0019] 또한, 상기 적어도 하나의 수행 활동에 증거 기반 표준 중 적어도 하나를 매핑하여, 자동차 보안개발 프로세스 표준을 생성하는 단계는, 상기 적어도 하나의 수행 활동과 관련된 적어도 하나의 제 1 키워드와 정보 보호 제품의 보안성 표준, 기업 보안과 관련된 표준, 개인 정보 보안과 관련된 표준 및 자동차 기능 안정성과 관련된 표준 각각과 관련된 적어도 하나의 제 2 키워드에 기초하여, 상기 적어도 하나의 수행 활동에 상기 정보 보호 제품의 보안성 표준, 상기 기업 보안과 관련된 표준, 상기 개인 정보 보안과 관련된 표준 및 상기 자동차 기능 안정성과 관련된 표준 중 적어도 하나를 매핑하는 단계;를 포함할 수 있다.

[0020] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0021] 본 개시는 자동차 보안 내재화 방법론을 통해 자동차 시스템이 예상대로 동작할 것이라는 신뢰를 사용자에게 제공할 수 있다.

[0022] 구체적으로, 본 개시의 본 개시는 자동차 보안 내재화 방법론은 ISO 26262의 기능 안전성 프로세스를 기반으로 하기 때문에 기존 자동차 기능 안전성 개발 프로세스에 대한 활동 접목이 용이하며, 자동차 개발에서 요구되는 정확성, 안전성, 보안성의 측면을 모두 고려할 수 있다.

[0023] 또한, 본 개시의 자동차 보안 내재화 방법론인 Trustworthy Automotive SDLC는 자동차 개발에서 요구되는 충분한 보안 수준을 제공함으로써 보안 위협에 대한 경쟁력을 확보하고, 상세화된 활동을 제시함으로써 다가오는 UNECE 자동차 사이버보안 규제에 활용될 수 있다.

[0024] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0025] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 것이다. 다른 예시들에서, 공지의 구조들 및 장치들이 하나 이상의 양상들의 기재를 용이하게 하기 위해 블록도 형태로 도시된다.

도 1은 본 개시의 몇몇 실시예에 따른 자동차 보안 내재화를 수행하기 위한 서버의 블록 구성도이다.

도 2는 본 개시의 몇몇 실시예에 따른 자동차 보안내재화 방법의 일례를 설명하기 위한 도면이다.

도 3는 본 개시의 몇몇 실시예에 따른 자동차 보안 내재화 방법론을 설명하기 위한 도면이다.

도 4는 본 개시의 몇몇 실시예에 따른 주요 Secure SDLC 표준과 관련된 표이다.

도 5는 본 개시의 몇몇 실시예에 따른 증명 기반 표준(Evidence-based standards)와 관련된 표이다.

도 6a 내지 도6e는 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 활동의 일례에 대한 흐름도이다.

도 7은 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 활동과 증명 기반 표준을 매핑하는 일례를 설명하기 위한 도면이다.

도 8은 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 산출물의 일례를 설명하기 위한 도면이다.

도 9는 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 요구사항 만족도를 설명하기 위한 도면이다.

도 10은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0026] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0027] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0028] 비록 제 1, 제 2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제 1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제 2 소자나 구성요소 일 수도 있음은 물론이다.

[0029] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0030] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0031] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0032] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.

[0033] 어떤 구성 요소가 다른 구성 요소에 “연결되어” 있다거나 “접속되어” 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 “직접 연결되어” 있다거나 “직접 접속되어”있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0034] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 “모듈” 및 “부”는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0035] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

[0036] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0038] 도 1은 본 개시의 몇몇 실시예에 따른 자동차 보안 내재화를 수행하기 위한 서버의 블록 구성도이다.

[0039] 도 1을 참조하면, 서버(100)는 프로세서(110), 통신부(120) 및 메모리(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 서버(100)를 구현하는데 있어서 필수적인 것은 아니어서, 서버(100)는 위에서 열거된 구성요소들보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0040] 서버(300)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0041] 서버(100)의 프로세서(110)는 통상적으로 서버(100)의 전반적인 동작을 제어한다. 프로세서(110)는 서버(100)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(130)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0042] 또한, 프로세서(110)는 메모리(130)에 저장된 응용 프로그램을 구동하기 위하여, 서버(100)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(110)는 상기 응용 프로그램의 구동을 위하여, 서버(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.

[0043] 서버(100)의 통신부(120)는, 서버(100)와 사용자 단말 사이 및 서버(100)와 외부 서버들 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 상기 통신부(120)는, 서버(100)를 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.

[0044] 서버(100)와 사용자 단말 사이 및 서버(100)와 외부 서버들 사이의 통신을 연결하는 네트워크는 공중전화 교환망(PSTN:Public Switched Telephone Network), xDSL(x Digital Subscriber Line), RADSL(Rate Adaptive DSL), MDSL(Multi Rate DSL), VDSL(Very High Speed DSL), UADSL(Universal Asymmetric DSL), HDSL(High Bit Rate DSL) 및 근거리 통신망(LAN) 등과 같은 다양한 유선 통신 시스템들을 사용할 수 있다.

[0045] 또한, 여기서 제시되는 네트워크(600)는 CDMA(Code Division Multi Access), TDMA(Time Division Multi Access), FDMA(Frequency Division Multi Access), OFDMA(Orthogonal Frequency Division Multi Access), SC-FDMA(Single Carrier-FDMA) 및 다른 시스템들과 같은 다양한 무선 통신 시스템들을 사용할 수 있다.

[0046] 본 개시의 실시예들에 따른 네트워크는 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있으며, 단거리 통신망(LAN: Local Area Network), 원거리 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다. 또한, 상기 네트워크는 공지의 월드와이드웹(WWW:World Wide Web)일 수 있으며, 적외선(IrDA:Infrared Data Association) 또는 블루투스(Bluetooth)와 같이 단거리 통신에 이용되는 무선 전송 기술을 이용할 수도 있다.

[0047] 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.

[0048] 서버(100)의 메모리(130)는 프로세서(110)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적 어도 하나의 타입의 저장매체를 포함할 수 있다. 이러한 메모리(130)는 프로세서(110)에 제어에 의하여 동작 될 수 있다.

[0049] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 서버(100)의 메모리(130)에 저장되고, 서버(100)의 프로세서(110)에 의해 실행될 수 있다.

[0051] 도 2는 본 개시의 몇몇 실시예에 따른 자동차 보안내재화 방법의 일례를 설명하기 위한 도면이다.

[0052] 도 2를 참조하면, 서버(100)의 프로세서(110)는 기업체의 안전(Safety) 개발 방법론에 대응하는 보안(cybersecurity) 수준을 획득할 수 있다(S110).

[0053] 일례로, 서버(100)의 프로세서(110)는 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득할 수 있다. 또한, 프로세서(110)는 안전 수준이 기 설정된 최소 안전 수준 미만인 경우, 기 설정된 최소 안전 수준에 대응하는 기초 안전 개발 방법론을 획득할 수 있다. 그리고, 프로세서(110)는 기초 안전 개발 방법론에 대응하는 보안 수준을 획득할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0054] 다른 일례로, 서버(100)의 프로세서(110)는 기업체의 안전 개발 방법론을 이용하여, 상기 기업체의 안전 수준을 획득할 수 있다. 그리고, 프로세서(110)는 안전 수준이 기 설정된 최소 안전 수준 이상인 경우, 기업체의 상기 안전 개발 방법론에 대응하는 보안 수준을 획득할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0055] 서버(100)의 프로세서(110)는 보안 수준에 기초하여, 보안내재화 방법론을 획득할 수 있다(S120).

[0056] 구체적으로, 서버(100)의 프로세서(110)는 보안내재화 방법론과 증거 기반 보안 방법론이 매핑되어 저장된 데이터베이스에서 보안 수준에 대응하는 보안내재화 방법론을 획득할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0057] 서버(100)의 프로세서(110)는 보안내재화 방법론 및 안전 개발 방법론을 통합할 수 있다(S130).

[0058] 구체적으로, 서버(100)의 프로세서(110)는 상기 보안내재화 방법론에서 자동차 개발과 관련된 적어도 하나의 특정 표준을 선정할 수 있다. 또한, 프로세서(110)는 적어도 하나의 특정 표준에서 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출할 수 있다. 그리고, 프로세서(110)는 적어도 하나의 수행 활동에 증거 기반 표준 중 적어도 하나를 매핑하여, 자동차 보안개발 프로세스 표준을 생성할 수 있다.

[0059] 좀더 구체적으로, 프로세서(110)는 자동차 개발과 관련된 적어도 하나의 수행 활동을 추출할 때, 적어도 하나의 특정 표준에 포함된 적어도 하나의 자동차 관련 키워드를 이용하여, 자동차 개발과 관련된 상기 적어도 하나의 수행 활동을 추출할 수 있다. 또한, 프로세서(110)는 자동차 보안개발 프로세스 표준을 생성할 때, 적어도 하나의 수행 활동과 관련된 적어도 하나의 제 1 키워드와 정보 보호 제품의 보안성 표준, 기업 보안과 관련된 표준, 개인 정보 보안과 관련된 표준 및 자동차 기능 안정성과 관련된 표준 각각과 관련된 적어도 하나의 제 2 키워드에 기초하여, 적어도 하나의 수행 활동에 상기 정보 보호 제품의 보안성 표준, 기업 보안과 관련된 표준, 개인 정보 보안과 관련된 표준 및 자동차 기능 안정성과 관련된 표준 중 적어도 하나를 매핑할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0060] 여기서, 적어도 하나의 특정 표준은 소프트웨어 개발과 관련된 표준, 시스템 개발과 관련된 표준, 기업의 모범 사례와 관련된 표준 및 자동차 보안과 관련된 표준 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0061] 한편, 서버(100)의 프로세서(110)는 통합의 결과물을 데이터베이스(또는, 메모리(130))에 저장할 수 있다(S140). 여기서, 결과물은 맞춤형 신뢰 보안 개발 프로세스, 적어도 하나의 맞춤형 보안 개발 수행 활동 및 산

출물을 포함할 수 있다. 또한, 맞춤형 신뢰 보안 개발 프로세스는, 보안 교육과 관련된 제 1 단계, 착수 및 계획과 관련된 제 2 단계, 요구사항 분석과 관련된 제 3 단계, 획득과 관련된 제 4 단계, 설계와 관련된 제 5 단계, 구현과 관련된 제 6 단계, 검증과 관련된 제 7 단계, 배포와 관련된 제 8 단계, 운영과 관련된 제 9 단계 및 폐기와 관련된 제 10 단계 중 적어도 하나를 포함할 수 있다.

[0062] 이하, 맞춤형 신뢰 보안 개발 프로세스는 도 6을 참조하여 후술한다.

[0064] 도 3은 본 개시의 몇몇 실시예에 따른 자동차 보안 내재화 방법론을 설명하기 위한 도면이다. 도 4는 본 개시의 몇몇 실시예에 따른 주요 Secure SDLC 표준과 관련된 표이다. 도 5는 본 개시의 몇몇 실시예에 따른 증명 기반 표준(Evidence-based standards)와 관련된 표이다.

[0065] 도 3을 참조하면, 서버(100)의 프로세서(110)는 주요 Secure SDLC 표준으로부터 자동차 개발 프로세스 관련 수행 활동을 획득할 수 있다. 여기서, 주요 Secure SDLC 표준은 도 4의 표에 도시된 바와 같이, Microsoft SDL, NIST SSDLC, OWASP CLASP 및 SAE J3061 각각의 표준을 포함할 수 있다.

[0066] 구체적으로, 프로세서(110)는 Trustworthy Automotive SDLC(신뢰 보안 개발)를 획득하기 위해 4 가지 주요 Secure SDLC 표준에서 자동차 개발과 관련이 있는 활동들을 도출할 수 있다. 여기서, Trustworthy는 개발 시 시스템에 대한 보안성, 안전성, 정확성을 모두 고려함으로써 시스템이 예상대로 동작할 것이라는 신뢰를 제공한다는 의미를 포함할 수 있다.

[0067] 한편, 서버(100)의 프로세서(110)는 증거 기반 표준으로부터 분야별 표준 세부 항목 및 Trustworthy Automotive SDLC의 요구사항을 획득할 수 있다. 여기서, 증거 기반 표준은 도 5의 표에 도시된 바와 같이, 기능 안전성과 관련된 CC, ISMS, PIMS 및 FSMS 각각의 세부 항목을 포함할 수 있다.

[0068] 구체적으로, 프로세서(110)는 주요 Secure SDLC 표준에서 자동차 개발과 관련이 있는 활동들을 도출한 이후 도출된 각 활동을 IT제품의 보안성 평가 관련 국제 표준인 CC(Common Criteria, ISO/IEC 15408), 정보보호 관리체계 관련 국제 표준인 ISMS(Information Security Management System, ISO/IEC 27001), 프라이버시 관련 국제 표준인 PIMS(Privacy Impact Management System, ISO/IEC 27701)와 자동차 기능 안전성 관련 국제 표준인 FSMS(Functional Safety Management System, ISO 26262)의 세부 요구사항(산출물(output), 세부 활동 등)에 매핑할 수 있다.

[0069] 추가로, 서버(100)의 프로세서(110)는 자동차 사이버보안 규제 및 자동차 기능 안전성 관련 표준(ISO/SAE 21434)으로부터 Trustworthy Automotive SDLC의 요구사항을 획득할 수 있다. 여기서, 자동차 사이버보안 규제는 UNECE(United Nations Economic Commission for Europe)에서 제정된 자동차 사이버보안 규제를 포함할 수 있다.

[0070] 여기서, 요구사항은 시스템(하드웨어 및 소프트웨어) 대상의 프로세스와 관련된 제 1 요구사항, Third-party 구성요소를 획득하는 과정을 포함하는 것과 관련된 제 2 요구사항, Trustworthy 관점을 고려하는 것과 관련된 제 3 요구사항, 자동차가 필요로 하는 안전성 및 보안성 수준을 충족하는 것과 관련된 제 4 요구사항, 단계 수행에 따른 추적성을 확보하는 것과 관련된 제 5 요구사항 및 프로세스의 모든 단계에 대해 상세화된 활동을 구성하는 것과 관련된 제 6 요구사항 중 적어도 하나를 포함할 수 있다.

[0071] 즉, 프로세서(110)는 자동차 사이버보안 규제 및 자동차 기능 안전성 관련 표준으로부터 상술한 제 1 요구사항 내지 제 6 요구사항 중 적어도 하나를 도출할 수 있다. 그리고, 프로세서(110)는 도출된 적어도 하나의 요구사항을 Trustworthy Automotive SDLC에 반영할 수 있다.

[0072] 그리고, 프로세서(110)는 요구사항이 반영된 Trustworthy Automotive SDLC를 사용자에게 제공할 수 있다.

[0073] 따라서, 본 개시의 Trustworthy Automotive SDLC는 ISO 26262의 기능 안전성 프로세스를 기반으로 하기 때문에 기존 자동차 기능 안전성 개발 프로세스에 대한 활동 접목이 용이할 수 있다.

[0074] 또한, 본 개시의 Trustworthy Automotive SDLC는 자동차 개발에서 요구되는 정확성, 안전성, 보안성의 측면을 모두 고려할 수 있다.

[0075] 또한, 본 개시의 Trustworthy Automotive SDLC는 자동차 개발에서 요구되는 충분한 보안 수준을 제공함으로써 보안 위협에 대한 경쟁력을 확보할 수 있을 뿐만 아니라, 상세화된 활동을 제시함으로써 자동차 사이버보안 규제에 활용될 수도 있다.

[0076] 한편, 이러한 Trustworthy Automotive SDLC는 총 10개의 활동을 포함할 수 있다. 이에 대한 설명은 도 6을 참조하여 후술한다.

[0077] 본 개시의 몇몇 실시예에 따르면, 자동차는 소프트웨어와 하드웨어를 포함하는 시스템의 형태로 개발된다. 따라서, 본 개시의 Trustworthy Automotive SDLC는 시스템 기반의 프로세스로 구축될 수 있다.

[0078] 추가적으로, 자동차 제조사는 자동차의 모든 구성요소를 자체적으로 개발하지 않고, 1-Tier, 2-Tier와 같은 협력 업체를 통해 획득한 구성요소를 활용한다. 따라서, 본 개시의 Trustworthy Automotive SDLC는 Third-party 구성요소에 대한 Trustworthiness를 확보하기 위해 Third-party 구성요소 획득에 대한 활동을 포함할 수 있다.

[0079] 본 개시의 몇몇 실시예에 따르면, 자동차 개발에서는 정확성, 안전성, 보안성의 측면이 모두 포함된 Trustworthy 관점이 고려되어야 한다. 이때 정확성과 안전성 관점은 기존 자동차 기능 안전 개발 표준인 ISO 26262가 제안하는 안전 개발 생명주기와 안전성 수준인 ASIL(Automotive Safety Integrity Level)을 통해 고려되어 왔다. 따라서, 본 개시의 Trustworthy Automotive SDLC는 이를 기반으로 보안성을 접목할 수 있도록 설계될 수 있다.

[0080] 여기서, ISO 26262에서 요구하는 ASIL 등급은 자동차의 주요 기능에 따라 다르게 선정되며, 자동차 기능 안전 개발 프로세스에서는 각 기능에 부여된 ASIL 등급을 기반으로 자동차를 개발한다.

[0081] 한편, 자동차에 대한 보안성 확보를 위해서는 두 가지 측면을 고려해야 한다. 먼저, 자동차 시스템에서 요구하는 EAL 수준을 충족해야 하는데, EAL 수준이란 제품의 보안성 평가 관련 국제 표준인 CC의 보증 수준을 의미한다. ISO 26262의 ASIL C 수준은 CC의 EAL5 수준에 해당한다. 따라서, 본 개시의 Trustworthy Automotive SDLC는 자동차 개발에 대해 충분한 보안성을 확보하기 위해서 기능 안전성 측면의 ASIL C 수준에 해당하는 EAL5의 보증 수준을 충족할 수 있다.

[0083] 도 6a 내지 도6e는 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 활동의 일례에 대한 흐름도이다. 도 7은 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 활동과 증명 기반 표준을 매핑하는 일례를 설명하기 위한 도면이다. 도 8은 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 산출물의 일례를 설명하기 위한 도면이다.

[0084] 먼저, 도 6a를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 교육(Training)단계(S1)를 포함할 수 있다.

[0085] 본 개시의 Trustworthy Automotive SDLC는 교육 단계에서 조직 구성원을 대상으로 안전성, 보안성 및 프라이버시에 대한 인식을 확보하고 개발 프로세스를 수행하면서 필요한 관련 지식을 교육할 수 있다.

[0086] 또한, 본 개시의 Trustworthy Automotive SDLC는 교육 단계에서 보안성이나 안전성과 관련된 기능을 개발하거나 관리하는 일부 팀의 경우 이에 대한 배경지식을 가지고 있지만, 개발팀과 같은 그 외의 구성원은 Trustworthiness에 관한 지식이 부재한 경우가 많기 때문에 분야별 교육을 통해 프로세스 수행에 요구되는 주제를 교육할 수 있다.

[0087] 구체적으로, 교육 단계는 안전성, 보안성 및 프라이버시에 대한 인식 확보를 위한 주제를 교육하는 것과 관련된 기본 교육을 포함할 수 있다. 또한, 교육 단계는 조직의 구성원들이 프로세스를 수행하는데 위화감이 없도록 위험분석과 같은 개발 프로세스 내에서 다뤄지는 주제에 대한 기본 지식 교육을 포함할 수 있다. 또한, 교육 단계는 보안의 측면에서 보면 개발팀 대상의 보안 설계 및 시큐어 코딩, 평가팀 대상의 정적 및 동적 분석, 보안팀 대상의 보안 및 프라이버시 관련 규제 인증과 같은 주제를 통해 각 실무자가 담당한 Trustworthy Automotive SDLC의 세부 활동을 수행하는 방법을 교육하는 것과 관련된 심화 교육을 포함할 수 있다. 여기서, 심화 교육은 직무에 따라 부여되는 별도의 교육일 수 있다. 다만, 이에 한정되는 것은 아니다.

[0088] 추가로, 교육 단계에 포함된 모든 교육들은 로드맵을 통해 관리될 수 있다. 또한, 교육 단계에 포함된 모든 교육들은 교육 대상자에 각각의 교육 준수 여부를 관리하여, 교육 수강 여부에 대한 추적성을 확보할 수 있다.

[0089] 도 7을 참조하면, Trustworthy Automotive SDLC의 교육 단계는 예를 들어, ISMS의 Leadership과 매핑 될 수 있다. 또한, 교육 단계의 Trustworthy Automotive SDLC는 FSMS의 Management of functional safety와 매핑 될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0090] 한편, 도 8을 참조하면, Trustworthy Automotive SDLC의 교육 단계는 분야별 기본 교육 주제 및 심화 교육 주제

와 교육 일정 및 로드맵을 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0091] 다시 도 6a를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 착수 및 계획(Initiation)단계(S2)를 포함할 수 있다.

[0092] 본 개시의 Trustworthy Automotive SDLC는 착수 및 계획 단계에서 프로젝트에 대한 개발 환경을 구축하고 프로젝트의 전반적인 계획을 수립할 수 있다. 또한, Trustworthy Automotive SDLC는 착수 및 계획 단계에서 분야별 목표를 설정할 수 있다.

[0093] 구체적으로, 착수 및 계획 단계는 프로젝트에서 취급하는 정보 자산과 제품 유형, 프로젝트 특성을 고려하여 프로젝트 범주화를 수행하는 것과 관련된 세부 단계를 포함할 수 있다. 또한, 착수 및 계획 단계는 이를 기반으로 역할 및 도구, 최소 품질 수준 등을 포함한 프로젝트 전반에 대한 계획을 수립하는 것과 관련된 세부 단계를 포함할 수 있다. 여기서, 최소 품질 수준은 프로젝트를 수행하면서 반드시 충족시켜야 할 최소한의 보안성, 안전성 및 프라이버시 수준을 의미할 수 있다. 또한, 최소 품질 수준을 충족하지 못하면 다음 단계를 수행할 수 없다.

[0094] 또한, 착수 및 계획 단계는 프로젝트에 대한 분야별 목표를 설정하고, 서로 다른 목표 간 일관성 및 완전성을 검증함으로써 이후 단계 수행에 대한 추적성을 확보할 수 있다.

[0095] 한편, 자동차 개발의 경우 시스템, 소프트웨어, 하드웨어 수준에 따라 개발이 별도로 수행되기 때문에 해당 단계를 각 수준에 맞춰 진행하게 된다. 이때 시스템 수준의 착수 및 계획 단계에서는 소프트웨어 및 하드웨어 수준을 아우르는 프로젝트 전반의 환경 및 계획을 수립함으로써 소프트웨어 및 하드웨어 개발에 대한 일관성을 확보해야 한다.

[0096] 따라서, 도 7에 도시된 바와 같이, Trustworthy Automotive SDLC의 착수 및 계획(Initiation)단계는 이러한 구조는 초기 단계부터 배포 단계(S8)까지 동일하게 적용되도록 매핑 될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0097] 도 8을 참조하면, Trustworthy Automotive SDLC의 착수 및 계획단계는 개발 및 개발 환경 관련 계획, 분야별 프로젝트 목표, 프로젝트 목표에 대한 일관성 및 완전성 검증 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0098] 도 6b를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 요구사항 분석(Requirements)단계(S3)를 포함할 수 있다.

[0099] 본 개시의 Trustworthy Automotive SDLC는 요구사항 분석 단계에서 프로젝트의 보안성, 안전성 및 프라이버시 관련 자산에 대한 영향평가를 수행하고 그 결과를 기반으로 분야별 요구사항을 도출하는 세부 단계를 포함할 수 있다. 또한, 요구사항 분석 단계는 목표와 요구사항 간 일관성 및 완전성을 검증함으로써 착수 및 계획 단계와 요구사항 분석 단계 간의 추적성을 확보할 수 있다.

[0100] 여기서, 기능 안전성과 보안성의 목표는 충돌할 수 있다. 이 경우, 요구사항 분석 단계는 기 설정된 분야별 영향평가 결과에 대한 적합성 및 충돌 여부 판단을 통해 안전성 및 보안성 영향 수준에 대한 우선순위를 식별하는 세부 단계를 더 포함할 수 있다. 추가로, 요구사항 분석 단계는 기존 시스템을 재사용하는 경우, 재사용 시스템에 대한 보안성 및 안전성 영향 또한 평가하는 세부 단계를 포함할 수 있다.

[0101] 요구사항 분석 단계는 앞서 도출한 목표에 따른 요구사항의 일관성 및 완전성을 검증함으로써 착수 및 계획 단계와 요구사항 분석 단계 간의 추적성을 확보할 수 있다.

[0102] 도 7을 참조하면, 요구사항 분석(Requirements)단계는 예를 들어, CC의 General mode과 매핑 될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0103] 한편, 도 8을 참조하면, 요구사항 분석(Requirements)단계는 분야별 영향평가 결과, 기존 시스템 평가 결과, 분야별 요구사항, 요구사항 간 적합성 및 충돌 여부 판단 결과, 목표에 따른 요구사항의 일관성 및 완전성 검증 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0104] 다시 도 6b를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 획득(Acquisition)단계(S4)를 포함할 수 있다.

[0105] 본 개시의 Trustworthy Automotive SDLC는 획득 단계에서 Third-party 구성요소 획득에 대한 범위 및 계획을

수립하고 관련 요구사항을 정의할 수 있다.

[0106] 구체적으로, 획득 단계는 정의한 요구사항을 기반으로 대상 업체가 제출한 명세에 대해 평가 및 테스트를 수행하는 세부 단계를 포함할 수 있다. 여기서, Third-party 구성요소는 1-Tier, 2-Tier 등의 협력 업체를 통해 획득한 구성요소를 의미할 수 있다. 또한, 획득 단계는 자동차 제조사의 요구사항에 맞추어 제출한 Third-party 구성요소의 명세를 기반으로 자동차 제조사가 독립적인 평가 및 테스트를 수행하는 세부 단계를 포함할 수 있다.

[0107] 본 개시의 몇몇 실시예에 따른 획득 단계는 자동차 개발의 경우 협력 업체를 통한 서브 시스템 개발이 전체 개발에 큰 비중을 차지하기 때문에 필수적으로 수행되어야 하는 단계일 수 있다.

[0108] 도 8을 참조하면, 획득(Acquisition)단계는 획득 계획 및 요구사항과 Third-party 구성요소에 대한 평가 및 테스트 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0109] 도 6c를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 설계(Design)단계(S5)를 포함할 수 있다.

[0110] 본 개시의 Trustworthy Automotive SDLC는 설계 단계에서 아키텍처를 설계하고 이를 기반으로 한 분야별 위험분석을 수행할 수 있다. 일반적으로 자동차 개발의 경우 서브 시스템을 기반으로 하나의 통합 시스템을 구성하기 때문에, 설계 단계는 시스템 통합 과정에 대한 아키텍처 설계를 고려할 수 있다.

[0111] 구체적으로, 설계 단계는 도출된 아키텍처를 기반으로 분야별 위험분석을 수행하여 시스템 내에 발생 가능한 위협에 대해 완화방안을 도출하는 세부 단계를 포함할 수 있다. 또한, 설계 단계는 요구사항 분석 단계(S3)와 같은 방식으로 분야별 완화방안에 대한 적합성 및 충돌 여부를 판단함으로써 이후 기능 안전 개발 프로세스와 보안 개발 프로세스 간의 충돌이 발생하지 않도록 하는 세부 단계를 포함할 수 있다. 또한, 설계 단계는 요구사항에 따라 아키텍처의 일관성 및 완전성을 검증함으로써 요구사항 분석 단계와 설계 단계 간의 추적성을 확보할 수 있다.

[0112] 도 8을 참조하면, 설계(Design)단계는 단위 및 통합 아키텍처, 분야별 위험분석 결과 및 완화방안, 분야별 완화방안 간 적합성 및 충돌 여부 판단 결과, 요구사항에 따른 설계의 일관성 및 완전성 검증 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0113] 다시 도 6c를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 구현(Implementation)단계(S6)를 포함할 수 있다.

[0114] 본 개시의 Trustworthy Automotive SDLC는 구현 단계에서 앞선 단계들(S1 내지 S5)에서 도출한 요구사항 및 아키텍처를 기반으로 시스템을 구현할 수 있다. 이 경우, 개발자는 코딩 가이드라인을 통해 시스템을 구현할 수 있다. 여기서, 코딩 가이드라인에는 기존에 확립된 MISRA C 등의 코딩 표준이 포함될 수 있다. 또한, 개발자는 배포된 시스템을 사용자가 사용할 때 Trustworthiness가 확보된 운영 환경을 구축할 수 있도록 배포 가이드라인 또는 도구를 생성할 수 있다.

[0115] 한편, 구현 단계는 아키텍처와 구현체 간의 일관성 및 완전성을 검증함으로써 설계 단계와 구현 단계 간의 추적성을 확보할 수 있다.

[0116] 도 8을 참조하면, 구현(Implementation)단계는 시스템 구현 결과, 사용자 가이드 문서 및 도구, 설계에 따른 구현의 일관성 및 완전성 검증 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0117] 도 6d를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 검증(Verification)단계(S7)를 포함할 수 있다.

[0118] 본 개시의 Trustworthy Automotive SDLC는 검증 단계에서 구현된 시스템을 기반으로 테스트 및 검토를 수행할 수 있다. 여기서, 테스트는 정적 및 동적 분석, 인수 테스트를 포함할 수 있다.

[0119] 일반적으로 자동차는 서브 시스템을 기반으로 구성되는 통합 시스템이므로 검증 단계는 시스템을 통합하는 과정에서 문제가 발생하지 않는지를 판단하는 통합 테스트를 수행하는 세부 단계를 포함할 수 있다. 여기서, 통합은 서브 시스템 기반의 통합을 의미할 수 있다. 다만, 이에 한정되는 것은 아니고, 하드웨어와 소프트웨어 기반의 시스템 통합을 의미할 수도 있다.

[0120] 검증 단계는 통합된 시스템에 대해 보안 위협이 존재하는지를 판단하기 위해 침투 테스트를 수행하는 세부 단계를 포함할 수 있다. 또한, 검증 단계는 시스템을 구현하면서 기존에 설계한 내용과 변경된 사항이 있는지 여부나 변경사항이 보안성, 안전성 및 프라이버시 관련 문제를 발생시키지는 않는지를 검토하기 위해 프로젝트 최소

품질 수준이나 산출된 문서 측면에서 검토하는 세부 단계를 포함할 수 있다.

[0121] 도 8을 참조하면, 검증(Verification)단계는 테스트 수행 결과, 독립적인 침투 테스트 수행 결과, 시스템 구현에 따른 변경사항에 대한 분야별 최종 검토 결과를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0122] 다시 도 6d을 참조하면, 본 개시의 Trustworthy Automotive SDLC는 생산 및 배포(Production & Release)단계(S8)를 포함할 수 있다.

[0123] 본 개시의 Trustworthy Automotive SDLC는 생산 및 배포 단계에서 시스템을 생산하고, 배포 후 시스템에서 발생 가능한 사고에 대해 대응계획을 수립할 수 있다. 여기서, 생산은 시스템 생산 공정을 의미하는데, 자동차의 경우 복잡하고 긴 생산 공정을 통해 생산하는 과정을 거치기 때문에 해당 과정에 대한 보안성을 반드시 확보해야 한다.

[0124] 한편, 생산 및 배포 단계는 생산이 완료된 시스템을 배포하는 과정에서도 보안 문제가 발생하는지를 검토하는 세부 단계를 포함할 수 있다.

[0125] 도 7을 참조하면, 생산 및 배포(Production & Release)단계는 예를 들어, FSMS의 Product development at the system level(Part 4) 및 Product development at the software level(Part 6)과 매핑 될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0126] 한편, 도 8을 참조하면, 생산 및 배포(Production & Release)단계는 시스템 생산 계획 및 절차, 생산된 시스템에 대한 검증 수행 결과, 시스템 배포 이후 대응계획을 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0127] 도 6e를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 운영(Operation)단계(S9)를 포함할 수 있다.

[0128] 본 개시의 Trustworthy Automotive SDLC는 운영 단계에서 배포 이후에 시스템에서 발생할 수 있는 취약점을 모니터링하고 발견된 취약점에 대해 대응할 수 있다.

[0129] 구체적으로, 운영 단계는 모니터링 계획을 수립하고, 이를 기반으로 시스템에 대한 지속적인 모니터링을 수행하는 세부 단계를 포함할 수 있다. 또한, 운영 단계는 사고 발생에 대한 취약점 리포트를 수집하고 이를 평가하여 대응 방안을 도출하는 세부 단계를 포함할 수 있다. 이후 상기 대응 방안은 패치 또는 업데이트를 통해 공개 및 배포될 수 있다.

[0130] 일반적으로 자동차의 경우 문제 발생이 인명 피해와 직접 연결될 수 있으므로 24시간 대응 가능한 담당팀을 배치하는 것이 중요할 수 있다. 운영 단계는 운영 중인 시스템에 변경사항이 생겼을 경우, 해당 변경사항에 대해서 형상을 관리함으로써 시스템에 대한 추적성을 확보할 수 있다.

[0131] 도 7을 참조하면, 운영(Operation)단계는 예를 들어, ISMS의 Operation 및 Improvement와 매핑 될 수 있다. 또한, 운영 단계는 FSMS의 Production operation, service and decommissioning(Part 7)과 매핑 될 수 있다. 다만, 이에 한정되는 것은 아니다.

[0132] 한편, 도 8을 참조하면, 운영(Operation)단계는 모니터링 결과 문서, 사고 대응 리포트, 사고 대응 평가 및 해결방안, 사고 대응 해결방안 배포 절차를 산출할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0133] 다시 도 6e를 참조하면, 본 개시의 Trustworthy Automotive SDLC는 폐기(Disposal)단계(S10)를 포함할 수 있다.

[0134] 본 개시의 Trustworthy Automotive SDLC는 폐기 단계에서 시스템에 대한 사용을 종료하고 전이 및 폐기를 수행할 수 있다. 여기서, 시스템 전이는 소유자 이전, 시스템 폐기는 폐차의 경우를 의미할 수 있다.

[0135] 일반적으로, 자동차 제조사는 시스템 폐기에 대한 과정을 자체적으로 수행하지는 않는다. 하지만, 시스템이 전이 또는 폐기될 시 어떤 정보가 보존되거나 소거되어야 하는지에 대한 정보를 가이드 문서를 통해 관련 업체에 제공함으로써 시스템 폐기에 대한 Trustworthiness를 확보할 수 있다.

[0136] 상기 가이드 문서는 사용자 개인정보에 대한 완전한 소거 방법, 자동차 주행 거리와 같이 이후 활용 가능한 내부 정보에 대한 보존 여부 등을 포함할 수 있다.

[0137] 자동차는 활용도에 따라 중고차 판매와 같은 소유자 이전, 렌터카와 같은 다수의 사용자에 의한 활용 등의 다양한 상황이 고려될 수 있다. 따라서, 폐기 단계는 자동차 제조사는 해당 시스템의 활용도나 특성에 적합한 과정을 수행할 수 있도록 담당 업체에 정보를 제공하는 세부 단계를 포함할 수 있다.

[0139] 도 9는 본 개시의 몇몇 실시예에 따른 Trustworthy Automotive SDLC의 요구사항 만족도를 설명하기 위한 도면이다.

[0140] 본 개시의 몇몇 실시예에 따르면, 서버(100)의 프로세서(110)는 자동차 사이버보안 규제 및 자동차 기능 안전성 관련 표준으로부터 Trustworthy Automotive SDLC의 요구사항을 획득할 수 있다. 여기서, 자동차 사이버보안 규제는 UNECE(United Nations Economic Commission for Europe)에서 제정된 자동차 사이버보안 규제를 포함할 수 있다. 또한, 자동차 기능 안전성 관련 표준은 ISO/SAE 21434일 수 있다.

[0141] 여기서, 요구사항은 시스템(하드웨어 및 소프트웨어) 대상의 프로세스와 관련된 제 1 요구사항, Third-party 구성요소를 획득하는 과정을 포함하는 것과 관련된 제 2 요구사항, Trustworthy 관점을 고려하는 것과 관련된 제 3 요구사항, 자동차가 필요로 하는 안전성 및 보안성 수준을 충족하는 것과 관련된 제 4 요구사항, 단계 수행에 따른 추적성을 확보하는 것과 관련된 제 5 요구사항 및 프로세스의 모든 단계에 대해 상세화된 활동을 구성하는 것과 관련된 제 6 요구사항 중 적어도 하나를 포함할 수 있다.

[0142] 본 개시의 몇몇 실시예에 따르면, 본 개시의 Trustworthy Automotive SDLC는 6개의 요구사항을 기반으로 설계된 자동차 보안 내재화 방법일 수 있다. 즉, 6개의 요구사항을 모두 만족할 수 있다. 이러한 Trustworthy Automotive SDLC는 Secure SDLC 표준 및 기존 연구보다 상세한 활동을 제시하며 자동차 개발에 적합할 수 있다.

[0143] 도 9는 본 개시의 Trustworthy Automotive SDLC의 각 요구사항에 대해 기존 Secure SDLC 표준 및 기존 연구의 충족 여부를 비교 분석한 표가 도시되어 있다.

[0144] 비교 대상 Secure SDLC 표준으로는 Microsoft SDL, NIST SSDLC, OWASP CLASP, SAE J3061를 선정하였고, 비교대상 연구는 개발 프로세스 전체를 대상으로 하는 연구를 선정하였다.

[0145] 도 9에 도시된 표에 숫자로 기록된 연구는 이하와 같다.

[0146] [44]: Takahira, Ricardo Y., et al. "Scrum and Embedded Software development for the automotive industry." Proceedings of PICMET'14 Conference: Portland International Center for Management of Engineering and Technology; Infrastructure and Service Integration. IEEE, 2014.

[0147] [45]: Young, William, and Nancy G. Leveson. "An integrated approach to safety and security based on systems theory." Communications of the ACM 57.2 (2014): 31-35.

[0148] [48]: Schmittner, Christoph, Zhendong Ma, and Erwin Schoitsch. "Combined safety and security development lifecylce." 2015 IEEE 13th International Conference on Industrial Informatics (INDIN). IEEE, 2015.

[0149] [55]: Skoglund, Martin, Fredrik Warg, and Behrooz Sangchoolie. "In Search of Synergies in a Multi-concern Development Lifecycle: Safety and Cybersecurity." International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2018.

[0150] [66]: Koschuch, Manuel, et al. "Safety & Security in the Context of Autonomous Driving." 2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE). IEEE, 2019.

[0151] 한편, 상술한 비교 대상 Secure SDLC 표준 및 비교대상 연구와 본 개시의 Trustworthy Automotive SDLC 사이의 비교 분석을 수행한 결과, 기존 연구와 Secure SDLC 표준은 자동차에 적합한 보안 내재화 방법론을 제시함에 있어 요구사항을 만족시키지 못할 수 있다.

[0152] 특히, 모든 비교 대상이 자동차가 필요로 하는 안전성 및 보안성 수준을 충족하는 것과 관련된 제 4 요구사항을 만족하지 못하는 것으로 조사되었다.

[0153] 또한, 프로세스의 모든 단계에 대해 상세화된 활동을 구성하는 것과 관련된 제 6 요구사항 또한 모든 비교 대상이 만족시키지 못하는 요구사항인 것으로 조사되었다.

[0154] 구체적으로, 기존 Secure SDLC에서는 2의 Depth를 가지는 세부 활동이 최대 36개의 도출되었다. 하지만, 본 개시의 Trustworthy Automotive SDLC는 2의 Depth를 가지는 50개의 세부 활동으로 구성되어 있다. 따라서, 기존 표준들에 대해 본 개시의 Trustworthy Automotive SDLC의 구성 활동은 충분한 구체화가 이루어진 상태이다.

[0156] 도 10은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

[0157] 본 개시내용이 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 전술되었지만, 당업자라면 본 개시내용 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로서 구현될 수 있다는 것을 잘 알 것이다.

[0158] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시져, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.

[0159] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.

[0160] 컴퓨터는 통상적으로 다양한컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체 로서, 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.

[0161] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는 데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.

[0162] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

[0163] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.

[0164] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0165] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 섀시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브

(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.

[0166] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 집 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0167] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0168] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0169] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0170] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다. 이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0171] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0172] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순하게 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0173] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

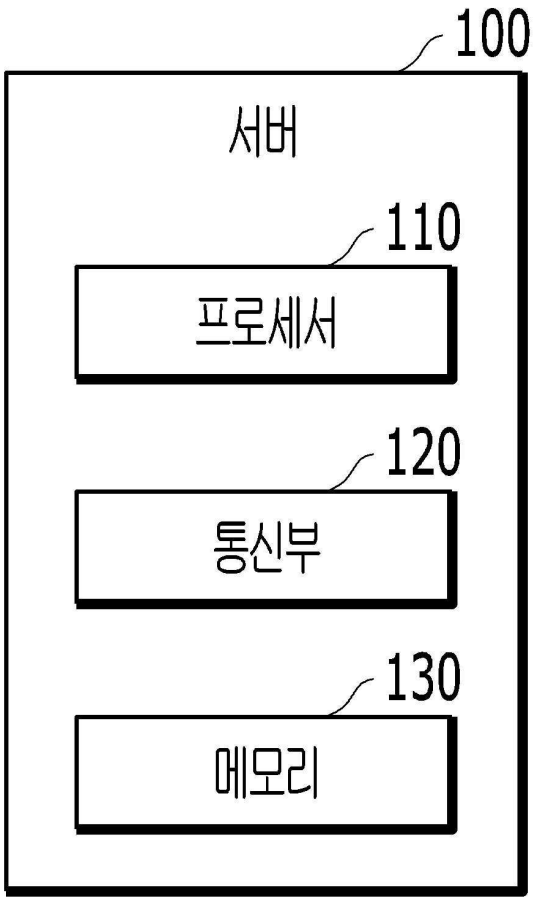
[0174] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[0175] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 "제조 물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

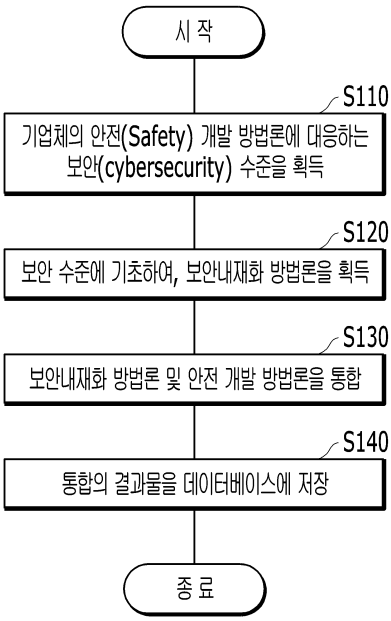
[0176] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

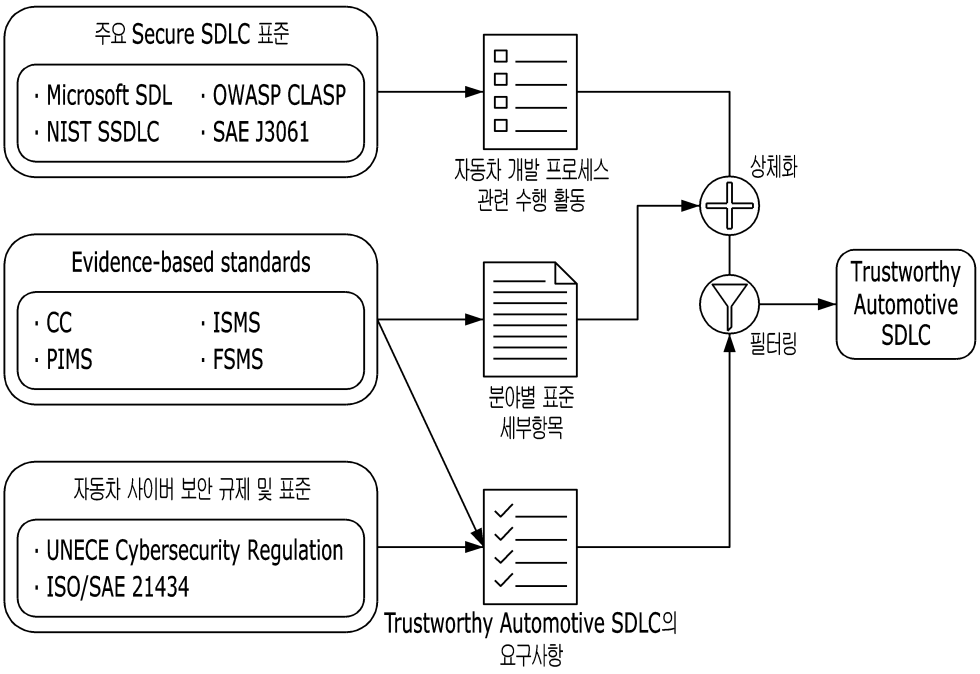
도면1


100
서버
110
프로세서
120
통신부
130
메모리

도면2


시작
S110
기업체의 안전(Safety) 개발 방법론에 대응하는 보안(cybersecurity) 수준을 획득
S120
보안 수준에 기초하여, 보안내재화 방법론을 획득
S130
보안내재화 방법론 및 안전 개발 방법론을 통합
S140
통합의 결과물을 데이터베이스에 저장
종료

도면3


주요 Secure SDLC 표준
· Microsoft SDL
· OWASP CLASP
· NIST SSDLC
· SAE J3061
자동차 개발 프로세스
관련 수행 활동
상체화
Evidence-based standards
· CC
· ISMS
· PIMS
· FSMS
분야별 표준
세부항목
Trustworthy
Automotive
SDLC
필터링
자동차 사이버 보안 규제 및 표준
· UNECE Cybersecurity Regulation
· ISO/SAE 21434
Trustworthy Automotive SDLC의
요구사항

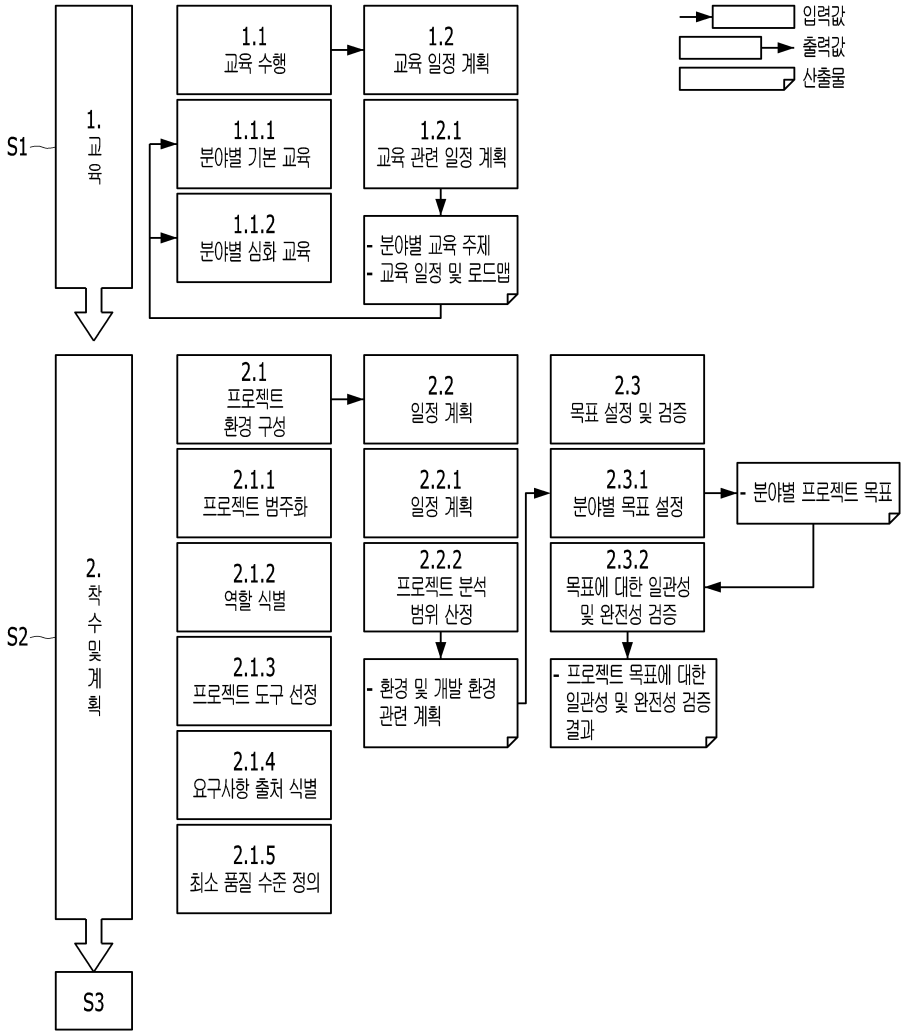
도면4

	Microsoft SDL	NIST SSDLC	OWASP CLASP	SAE J3061
Target	Software	System	Best Practice	Vehicle
Feature	Focuses on requirements and design phase	Focuses on third-party components acquisition and system disposal	Provides real-world enterprise activities in the form of best practices	Complies with the process of ISO 26262, the automotive functional safety standard
Pros & Cons (P:Pros, C:Cons)	· Provides tools for performing activities like risk analysis(P) · Not include disposal phase(C)	· Can be used to evaluate information systems that require certification when performing certification and accreditation(P) · Lack of activity for implementation phase(C)	· Identifies the role of the person in charge of each activity(P) · Lack of updates and related information(C)	· Easy to apply security-related activities according to the automotive function safety development process(P) · Not include security training and disposal phase(C)

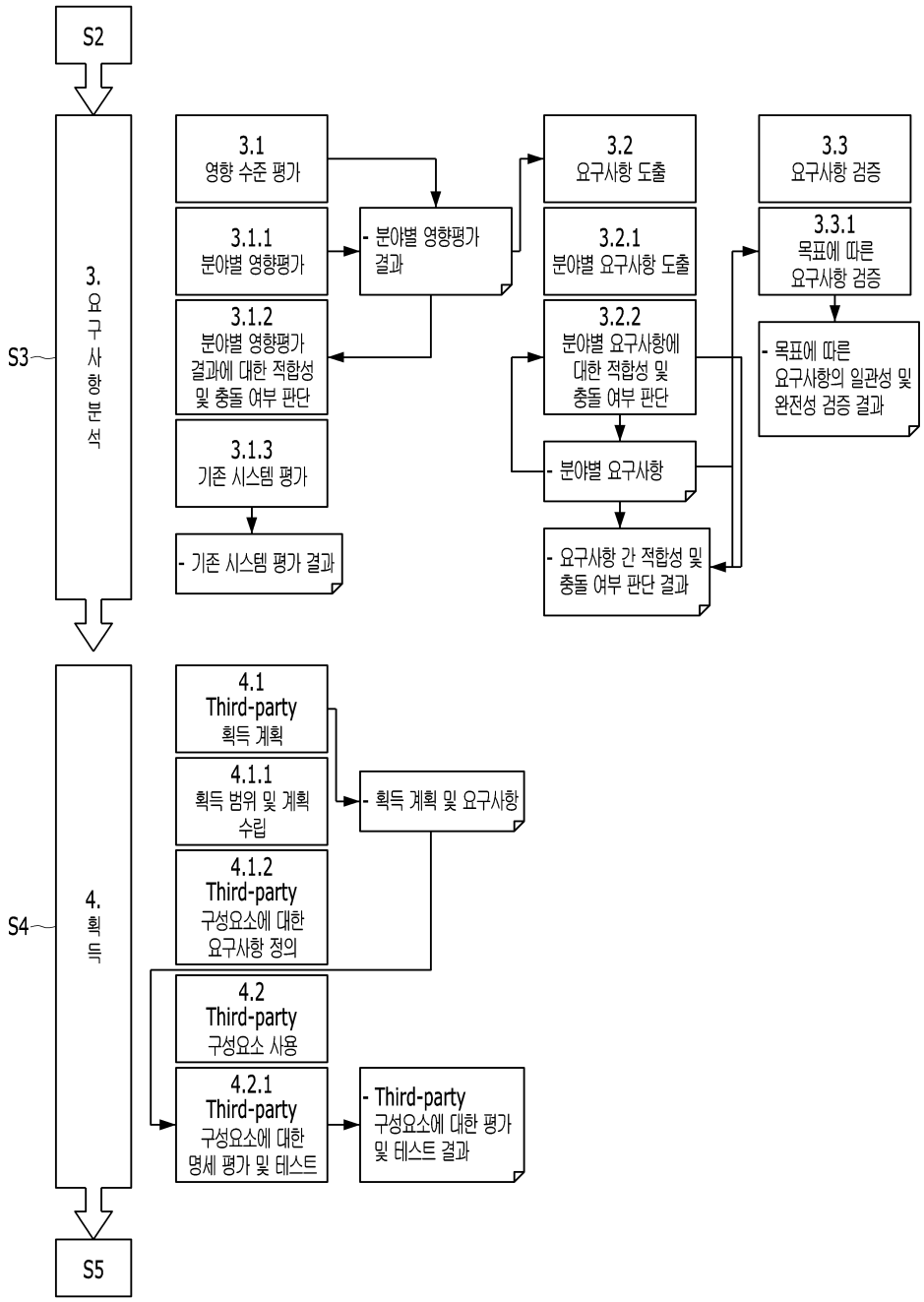
도면5

	CC	ISMS	PIMS	FSMS
Target	Product	Environment	Privacy	Functional safety
Description	Standards for evaluating the security and reliability of IT products	Standards for security and reliability certification of an organization's assets	Standards providing detailed criteria for performance of privacy impact assessment	Standards presenting processes for automotive functional safety development
Mapping phases	2,3,5-10	1-10	2,5,8,10	1-10
Source	ISO/IEC 15408	ISO/IEC 27001	ISO/IEC 27701	ISO 26262

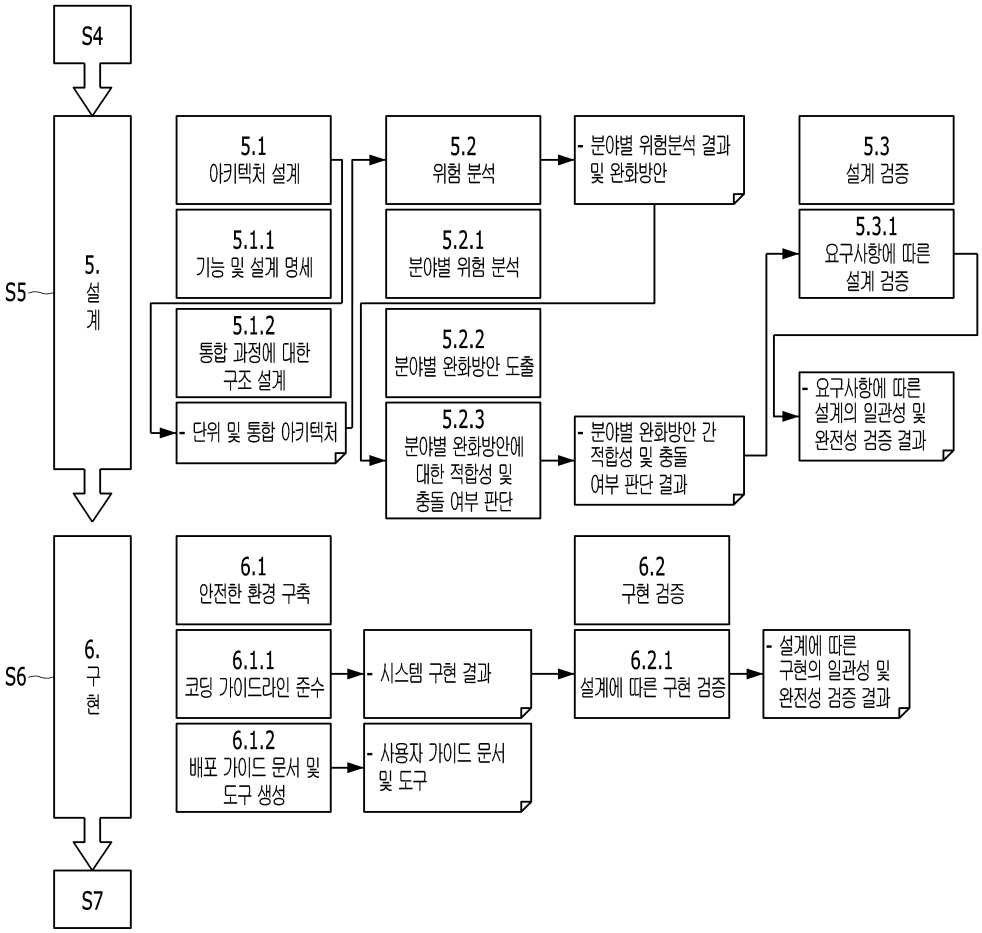
도면6a


입력값
출력값
산출물
S1
1. 교육
1.1 교육 수행
1.2 교육 일정 계획
1.1.1 분야별 기본 교육
1.1.2 분야별 심화 교육
1.2.1 교육 관련 일정 계획
- 분야별 교육 주제
- 교육 일정 및 로드맵
S2
2. 착수 및 계획
2.1 프로젝트 환경 구성
2.1.1 프로젝트 범주화
2.1.2 역할 식별
2.1.3 프로젝트 도구 선정
2.1.4 요구사항 출처 식별
2.1.5 최소 품질 수준 정의
2.2 일정 계획
2.2.1 일정 계획
2.2.2 프로젝트 분석 범위 산정
- 환경 및 개발 환경 관련 계획
2.3 목표 설정 및 검증
2.3.1 분야별 목표 설정
2.3.2 목표에 대한 일관성 및 완전성 검증
- 분야별 프로젝트 목표
- 프로젝트 목표에 대한 일관성 및 완전성 검증 결과
S3

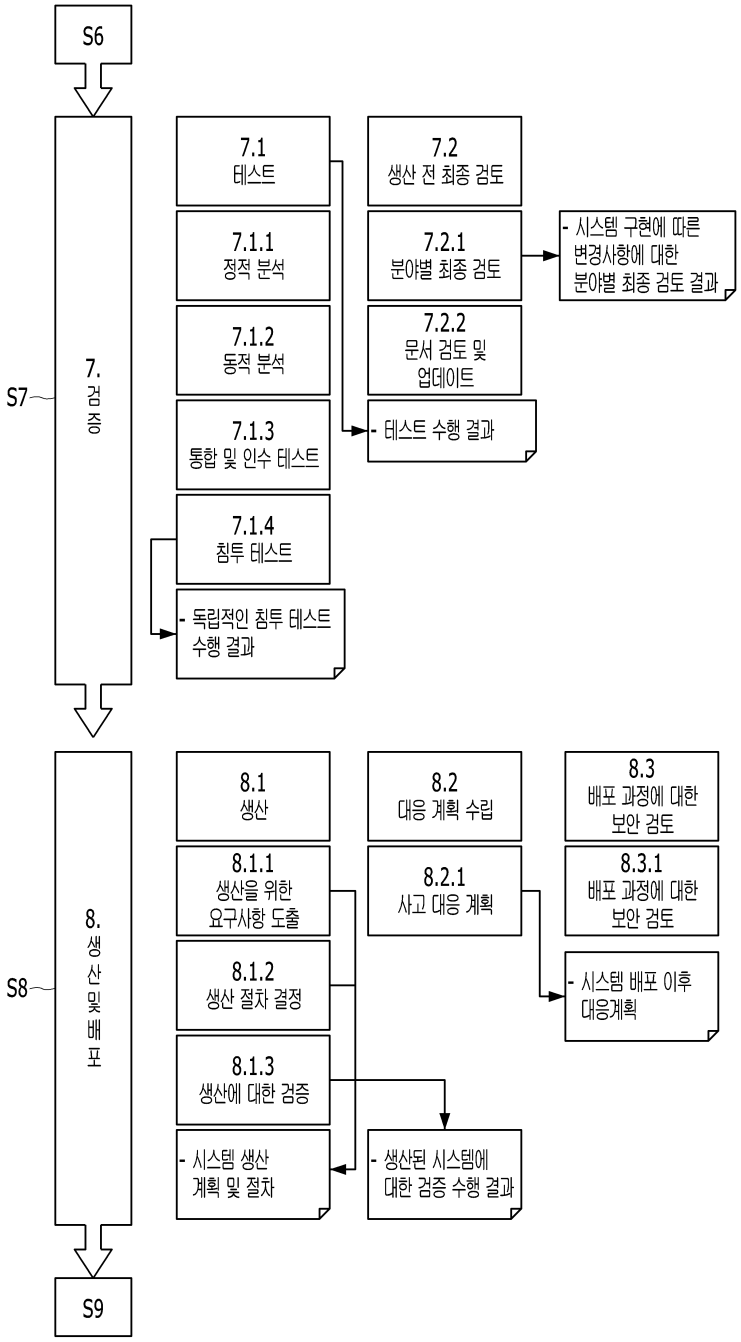
도면6b


S2
S3
3. 요구사항 분석
3.1 영향 수준 평가
3.1.1 분야별 영향평가
3.1.2 분야별 영향평가 결과에 대한 적합성 및 충돌 여부 판단
3.1.3 기존 시스템 평가
- 분야별 영향평가 결과
- 기존 시스템 평가 결과
3.2 요구사항 도출
3.2.1 분야별 요구사항 도출
3.2.2 분야별 요구사항에 대한 적합성 및 충돌 여부 판단
- 분야별 요구사항
- 요구사항 간 적합성 및 충돌 여부 판단 결과
3.3 요구사항 검증
3.3.1 목표에 따른 요구사항 검증
- 목표에 따른 요구사항의 일관성 및 완전성 검증 결과
S4
4. 획득
4.1 Third-party 획득 계획
4.1.1 획득 범위 및 계획 수립
4.1.2 Third-party 구성요소에 대한 요구사항 정의
4.2 Third-party 구성요소 사용
4.2.1 Third-party 구성요소에 대한 명세 평가 및 테스트
- 획득 계획 및 요구사항
- Third-party 구성요소에 대한 평가 및 테스트 결과
S5

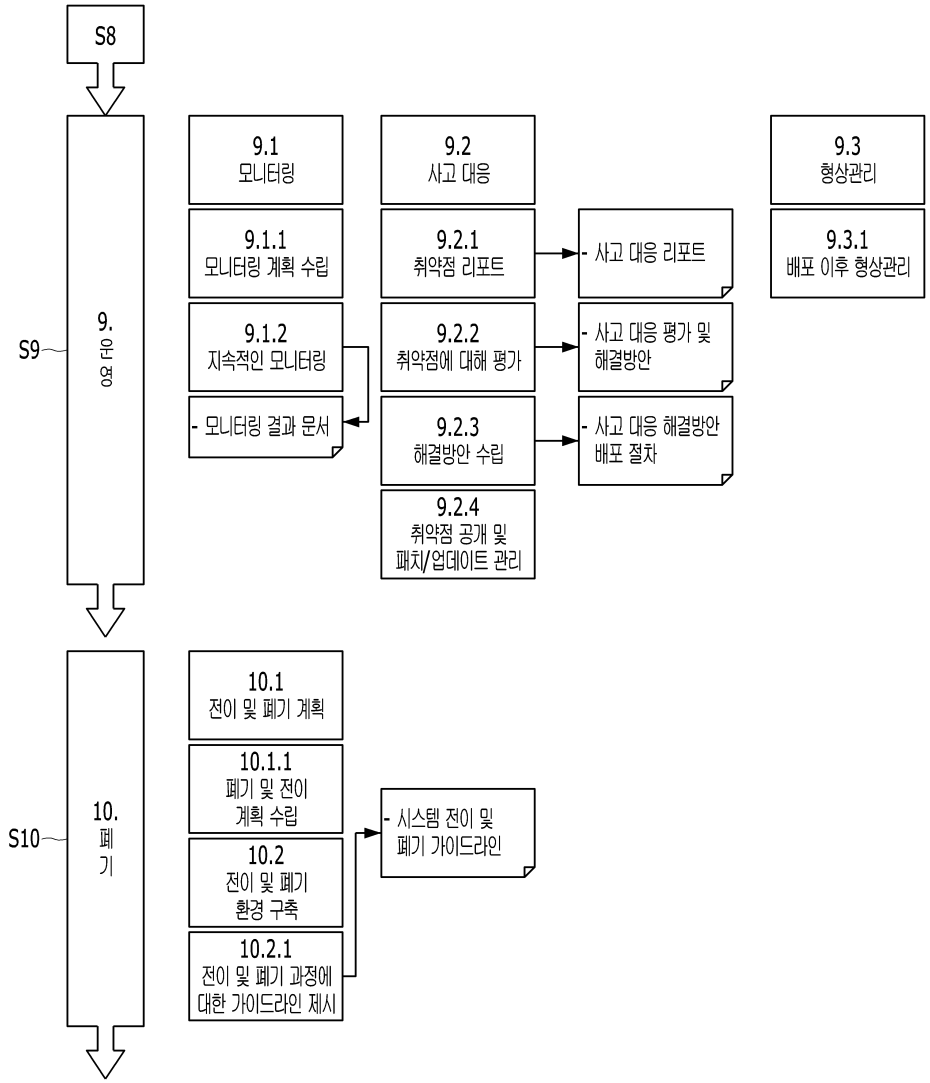
도면6c


S4
S5
5.
설
계
5.1
아키텍처 설계
5.1.1
기능 및 설계 명세
5.1.2
통합 과정에 대한
구조 설계
- 단위 및 통합 아키텍처
5.2
위험 분석
5.2.1
분야별 위험 분석
5.2.2
분야별 완화방안 도출
5.2.3
분야별 완화방안에
대한 적합성 및
충돌 여부 판단
- 분야별 위험분석 결과
및 완화방안
- 분야별 완화방안 간
적합성 및 충돌
여부 판단 결과
5.3
설계 검증
5.3.1
요구사항에 따른
설계 검증
- 요구사항에 따른
설계의 일관성 및
완전성 검증 결과
S6
6.
구
현
6.1
안전한 환경 구축
6.1.1
코딩 가이드라인 준수
6.1.2
배포 가이드 문서 및
도구 생성
- 시스템 구현 결과
- 사용자 가이드 문서
및 도구
6.2
구현 검증
6.2.1
설계에 따른 구현 검증
- 설계에 따른
구현의 일관성 및
완전성 검증 결과
S7

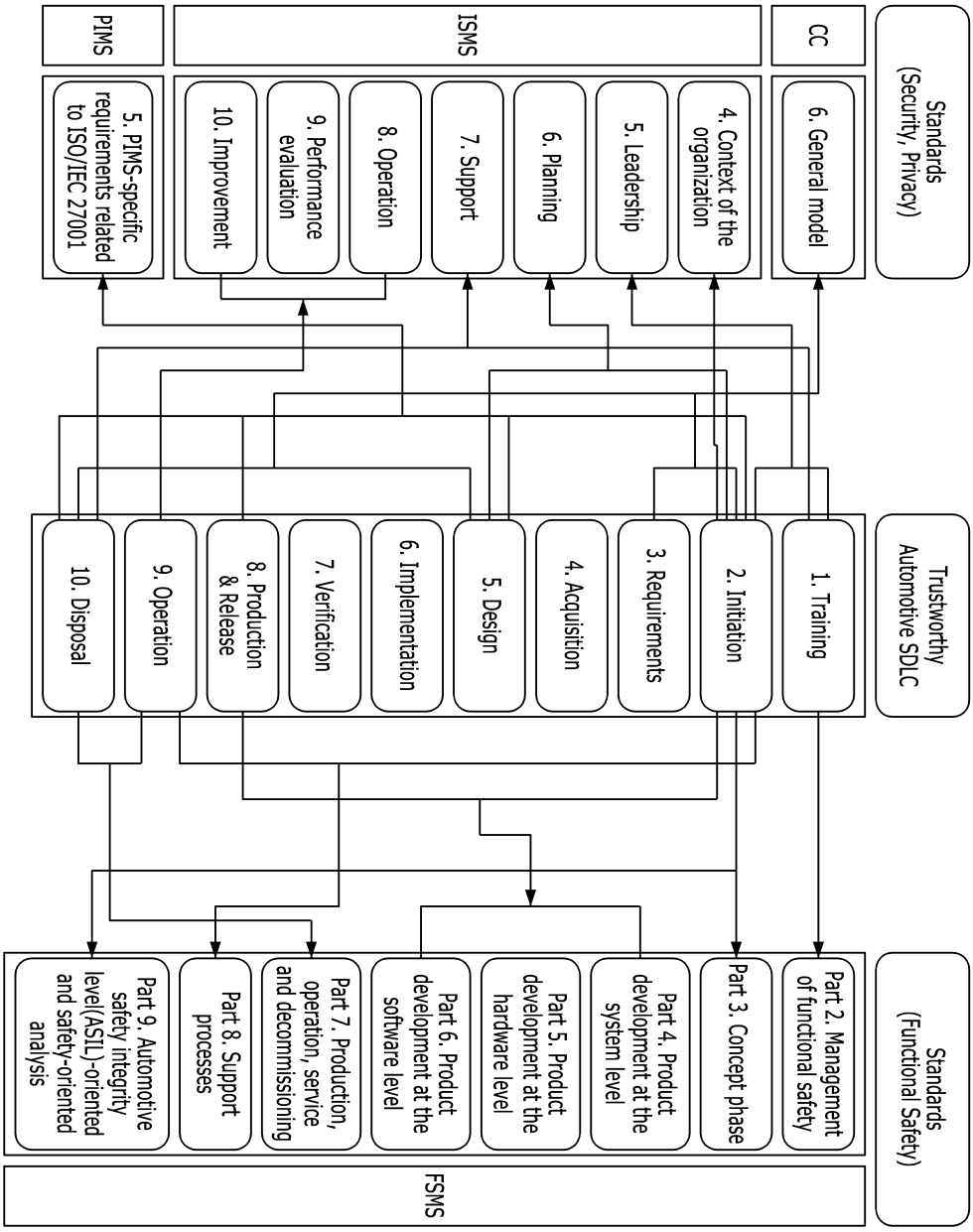
도면6d


S6
S7
7. 검증
7.1 테스트
7.1.1 정적 분석
7.1.2 동적 분석
7.1.3 통합 및 인수 테스트
7.1.4 침투 테스트
- 독립적인 침투 테스트 수행 결과
7.2 생산 전 최종 검토
7.2.1 분야별 최종 검토
- 시스템 구현에 따른 변경사항에 대한 분야별 최종 검토 결과
7.2.2 문서 검토 및 업데이트
- 테스트 수행 결과
S8
8. 생산 및 배포
8.1 생산
8.1.1 생산을 위한 요구사항 도출
8.1.2 생산 절차 결정
8.1.3 생산에 대한 검증
- 시스템 생산 계획 및 절차
8.2 대응 계획 수립
8.2.1 사고 대응 계획
- 생산된 시스템에 대한 검증 수행 결과
8.3 배포 과정에 대한 보안 검토
8.3.1 배포 과정에 대한 보안 검토
- 시스템 배포 이후 대응계획
S9

도면6e


S8
S9
9. 운영
9.1 모니터링
9.1.1 모니터링 계획 수립
9.1.2 지속적인 모니터링
- 모니터링 결과 문서
9.2 사고 대응
9.2.1 취약점 리포트
- 사고 대응 리포트
9.2.2 취약점에 대해 평가
- 사고 대응 평가 및 해결방안
9.2.3 해결방안 수립
- 사고 대응 해결방안 배포 절차
9.2.4 취약점 공개 및 패치/업데이트 관리
9.3 형상관리
9.3.1 배포 이후 형상관리
S10
10. 폐기
10.1 전이 및 폐기 계획
10.1.1 폐기 및 전이 계획 수립
10.2 전이 및 폐기 환경 구축
10.2.1 전이 및 폐기 과정에 대한 가이드라인 제시
- 시스템 전이 및 폐기 가이드라인

도면7


Standards (Security, Privacy)
CC
ISMS
PIMS
6. General model
4. Context of the organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance evaluation
10. Improvement
5. PIMS-specific requirements related to ISO/IEC 27001
Trustworthy Automotive SDLC
1. Training
2. Initiation
3. Requirements
4. Acquisition
5. Design
6. Implementation
7. Verification
8. Production & Release
9. Operation
10. Disposal
Standards (Functional Safety)
Part 2. Management of functional safety
Part 3. Concept phase
Part 4. Product development at the system level
Part 5. Product development at the hardware level
Part 6. Product development at the software level
Part 7. Production, operation, service and decommissioning
Part 8. Support processes
Part 9. Automotive safety integrity level(ASIL)-oriented and safety-oriented analysis
FSMS

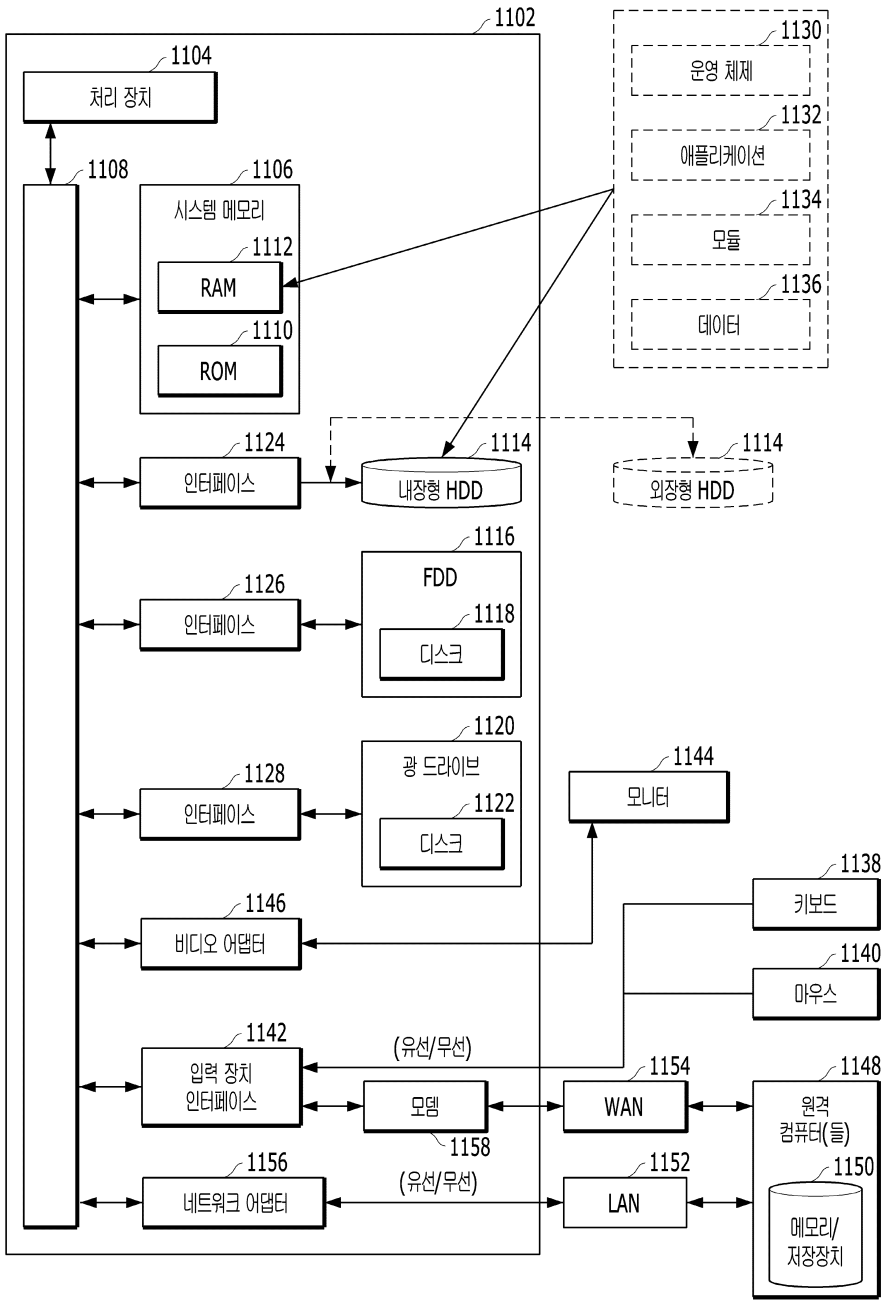
도면8

번호	단계	산출문서
1	교육 (Training)	분야별 기본 및 심화 교육 주제 교육 일정 및 로드맵
2	착수 및 계획 (Initiation)	개발 및 개발 환경 관련 계획 분야별 프로젝트 목표 프로젝트 목표에 대한 일관성 및 완전성 검증 결과
3	요구사항 분석 (Requiremenrs)	분야별 영향평가 결과 기존 시스템 평가 결과 분야별 요구사항 요구사항 간 적합성 및 충돌 여부 판단 결과 목표에 따른 요구사항의 일관성 및 완전성 검증 결과
4	획득 (Acquisition)	획득 계획 및 요구사항 Third-party 구성요소에 대한 평가 및 테스트 결과
5	설계 (Design)	단위 및 통합 아키텍처 분야별 위험분석 결과 및 완화방안 분야별 완화방안 간 적합성 및 충돌 여부 판단 결과 요구사항에 따른 설계의 일관성 및 완전성 검증 결과
6	구현 (Implementation)	시스템 구현 결과 사용자 가이드 문서 및 도구 설계에 따른 구현의 일관성 및 완전성 검증 결과
7	검증 (Verification)	테스트 수행 결과 독립적인 침투 테스트 수행 결과 시스템 구현에 따른 변경사항에 대한 분야별 최종 검토 결과
8	생산 및 배포 (Production & Release)	시스템 생산 계획 및 절차 생산된 시스템에 대한 검증 수행 결과 시스템 배포 이후 대응 계획
9	운영 (Operation)	모니터링 결과 문서 사고 대응 리포트 사고 대응 평가 및 해결방안 사고 대응 해결방안 배포 절차
10	폐기 (Disposal)	시스템 전이 및 폐기 가이드라인

도면9

	Requirement	Secure SDLC standards				Existing studies						Trustworthy Automotive SDLC
		Microsoft SDL	NIST SSDLC	OWASP CLASP	SAE J3061	[44]	[45]	[48]	[55]	[66]		
1	Targets on system	×	○	×	○	○	○	○	○	○		○
2	Includes the procedure of third-party components acquisition	×	○	○	○	×	×	×	×	×		○
3	Considers aspect of trustworthiness	×	×	×	○	○	○	○	○	○		○
4	Satisfies the level of safety and security required by automotive development	×	×	×	×	×	×	×	×	×		○
5	Ensures traceability between phases	○	○	×	○	×	×	○	×	×		○
6	Provides detailed activities for every phase of the process	×	×	×	×	×	×	×	×	×		○

도면10


1102
1104
처리 장치
1108
1106
시스템 메모리
1112
RAM
1110
ROM
1130
운영 체제
1132
애플리케이션
1134
모듈
1136
데이터
1124
인터페이스
1114
내장형 HDD
1114
외장형 HDD
1116
FDD
1126
인터페이스
1118
디스크
1120
광 드라이브
1128
인터페이스
1122
디스크
1144
모니터
1138
키보드
1146
비디오 어댑터
1140
마우스
1142
입력 장치
인터페이스
(유선/무선)
모뎀
1158
1154
WAN
1148
원격
컴퓨터(들)
1156
네트워크 어댑터
(유선/무선)
1152
LAN
1150
메모리/
저장장치