자동차 산업의 사이버보안 개요 및 SAE J3061 적용 방안

2018. 09. 13

(주)에스피아이디

spid

CMMI Institute Partner
Powered by Carnegie Mellon

Contents

I. 자동차 산업의 사이버보안 개요

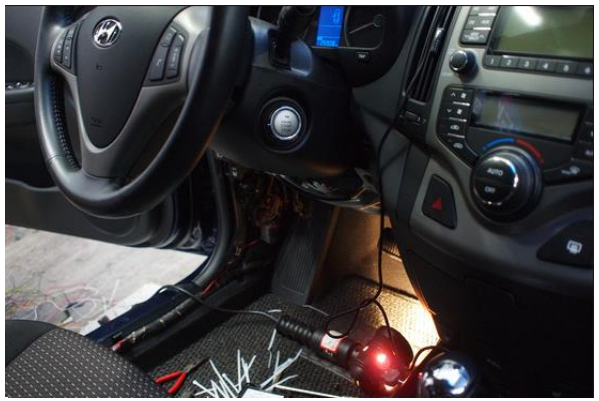
1. 산업의 변화와 자동차 산업의 변화

▣ 정보통신, 센서 기술의 발전이 제조업 공정에 혁신을 일으키고 있으며, ICT 융합을 통한 산업구조 및 사회 시스템의 혁신을 일으키는 산업의 변화를 4차 산업혁명을 이끌고 있습니다.

자동차 산업			
	▪ 전기 동력을 이용한 대량 생산 ▪ 산업용 기기 ▪ 기계 기술 중심	▪ 컴퓨터 제어 기반 부품 탑재 ▪ 개인용 기기 ▪ 전기, 전자 기술 증대	▪ 운전자. 보행자, 도로, 여러 자동차 등 모든 사물과의 연결 ▪ 자율주행, 커넥티드 카

2. 자동차 산업의 사이버보안 이슈

▣ 자동차와 ICT 기술의 접목으로 ICT 산업의 사이버보안 이슈가 이동하였습니다.



- 주로 취약한 안드로이드 어플리케이션 변경으로 차량 내부 네트워크 진입 시도
- OBD를 통한 Firmware Update 수행을 통해 차량의 제어 권한 확보
- 시험 대상에 한하여 재현이 가능함

- 셀룰러 네트워크를 통해 인터넷에 연결로 **취약점 노출 빈도의 증가**
- 내부 ECU가 상호 연결되어 전체 내부 네크워크의 노출 위험이 있으며 공격자의 전문 기술에 따라 중요 시스템 탈취 가능
- 간단한 장비를 사용하여 실험 대상이 아닌 일반 차량을 대상으로 해킹 목표를 찾고 수행 가능함

2. 자동차 산업의 사이버보안 이슈

▣ 자동차 산업에서의 주요 사이버보안 공격

Vehicle OEM	Type of Attack	Severity
Jeep Cherokee	**Cellular Network – Entertainment system** 특정 Port(6667)이 열려 있었고 Port Scan을 통해 검색 및 응답수행/ Firmware update로 권한 획득,	High
GM Chevy Impala	**Physical Access – Buffer Overflow** MP3파일을 차량 시스템에서 재생, 자동차 전체 시스템 및 중요 기능에 대한 접근 권한 부여	Low
BMW	**Spoofed Wi-Fi Hotspot** 자동차 SIM 기반 셀룰러 연결시 가짜 네트워크에 연결하여 원격잠금해제 가능, 비암호화된 통신환경	High
Corvette	**OBD dongle exploited** OBD포트에 특정 동글 부착, 원격으로 브레이크 신호 제어	Medium
Tesla S Model	**Physical Access –Trojan** 물리적 접근으로 트로이목마 설치, 원격접근 가능	Low
Nissan LEAF	**Wireless attack – Mobile app** 닛산에서 제공하는 앱 취약점을 악용, 원격으로 실내장치 on/off, GPS 위치 수집	Medium
Tesla All models	**Wireless attack – Wi-Fi** WiFi 연결 결함을 활용하여 악성웹사이트 자동 로드하여 무선 공격, 리눅스 운영체제의 결함 및 게이트웨이의 인가되지 않은 펌웨어 업데이트 가능	High

3. 자동차 산업의 사이버보안 문제

▣ 사이버보안 기술 적용의 어려움

4. 차량에 대한 사이버보안 연구

▣ ESCAR 협회 설립을 통해 자동차 도메인의 사이버보안 연구가 유럽을 중심으로 활성화 되었습니다.

2003 escar (Embedded Security in Cars)

- **ESCAR(Embedded Security in Cars)** 설립으로 자동차 사이버보안 연구 시작

2004 ~ 2010 SEVECOM

- 도로 교통관련 통신에 중점
- 보안 통신 프로토콜, 개인정보보호, 침입탐지, 보안 사용자 인터페이스 등을 위한 암호 기본 요소를 정의

2008 ~ 2011 evita

- 사이버보안 관련 컴포넌트 보호를 위하여 온보드 네트워크용 아키텍처 설계 및 프로토타입화

2010 ~ 2012 *OVERSEE*

- 개방형 표준화된 차량용 소프트웨어 및 통신 플랫폼 개발
- 차량 어플리케이션에 내부/외부 차량 통신 인터페이스 제공

2011 ~ 2014 PRESERVE (preparing secure v2x communication systems)

- V2X 사이버보안 하위 시스템 설계, 구현 및 테스트를 위하여 실제 배포 시나리오를 안전하고 확장성을 갖춰 개발

2012 ~ 2015 SESAMO (Security and Safety Modelling)

- **기능안전과 사이버보안 메커니즘 간의 상호 작용**을 위한 시스템의 체계적인 설계, 분석, 개발 및 평가 방법론 제공

2013 ~ 2016 *HEAVENS*

- 자동차 산업에서의 사이버보안 최첨단 기술을 연구하고 분석, **사이버보안 모델을 구축하고 평가 방법 및 도구 지원**
- ISO 26262, AUTOSAR 및 기타 관련 표준을 고려한 E/E 아키텍처에서 안전과 사이버보안의 상호 작용을 조사

5. 사이버보안 기술 개요

▣ 정보 보안 기술과 자동차 보안 기술

Information Security

- 보호 대상 : Asset , Privacy, DATA, Information
- 보호 대상 시스템의 주요 취약점을 분석하여 논리적, 물리적 보호 시스템 구축
- 주요 정보보안 기술 : VPN, SSL, Anti-Virus, Anti-Spam, etc.
- 주요 표준 및 관련법 : CMVP, ISO/IEC 15408, ISO 27002, etc.

Vehicle Security

- 보호 대상 : 운전자, 운전자 자산, Society Community
- 외부 기기와의 연결로 인해 기능적인 오류를 일으킬 수 있는 모든 차량 네트워크에 대해 보안 확보
- 주요 차량보안 기술 : EVITA security module
- 주요 표준 및 관련법 : EVITA Project, SAE J3061, etc

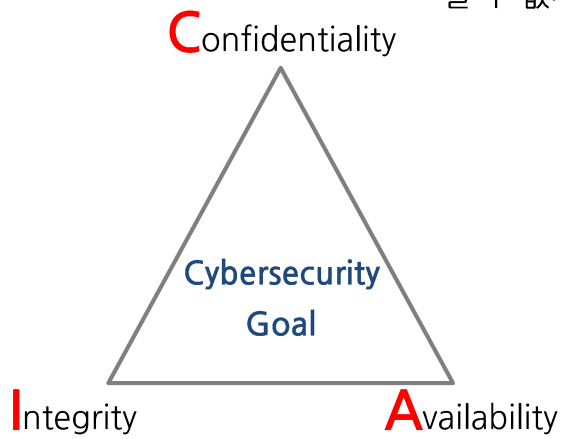
보호 대상에 대한 Threat를 분석 식별하여
허가되지 않은 공격자로부터의 보호

Ref. Denso, Safety and Security for Connected Vehicles, 2015.01

5. 사이버보안 기술 개요

▣ 사이버보안의 원칙

허가되지 않은 자에게 객체 및 교환 데이터를 알 수 없게 하는 것



정확하고 완전한 상태로 자료 또는 정보를 보존

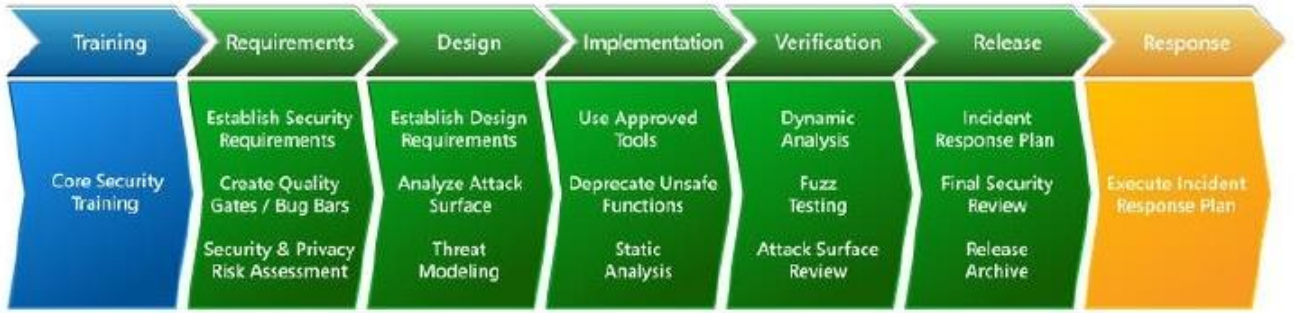
사용자가 정상적인 과정이나 절차를 통해 시스템을 사용 할 수 있도록 시스템을 준비하는 기능

- **Authentication(인증)** : 연결 성립 시 송신자 또는 수신자에 대한 인증 및 데이터의 출처 검증
- **Non-Repudiation(부인 방지)** : 활동 및 이벤트 발생을 증명, 추후 그에 대한 발생의 부인을 방지

II. SAE J3061 적용 방안

1. SAE J 3061 Overview

▣ 자동차 산업 도메인에서 제품을 개발 관리하는 자체 내부 프로세스에 적용 할 수 있도록 Tailoring 하여 SAE J3061 가이드라인 발표하였습니다.



Microsoft's Security Development Lifecycle (SDL)

▣ 적용 범위 및 주요 목적

1. Defining a complete lifecycle process framework that can be tailored and utilized within each organization's development processes to incorporate Cybersecurity into cyber-physical vehicle systems from concept phase through production, operation, service, and decommissioning. 컨셉 단계에서 생산, 운영, 서비스 및 폐기를 통해 사이버 물리적인 차량 시스템에 사이버보안을 통합하기 위해 각 조직의 개발 프로세스 내에서 조정 및 활용 할 수 있는 완벽한 수명주기 프로세스 프레임워크 정의

2. Providing information on some common existing tools and methods used when designing, verifying and validating cyber-physical vehicle systems. 사이버 물리적 차량 시스템을 설계, 검증, 확인할 때 사용되는 기존의 도구 및 방법에 대한 정보 제공

3. Providing basic guiding principles on Cybersecurity for vehicle systems. 차량 시스템에 대한 사이버보안의 기본적 가이드 지침 제공

4. Providing the foundation for further standards development activities in vehicle Cybersecurity. 차량 사이버보안에서 표준 개발 활동의 기반 제공

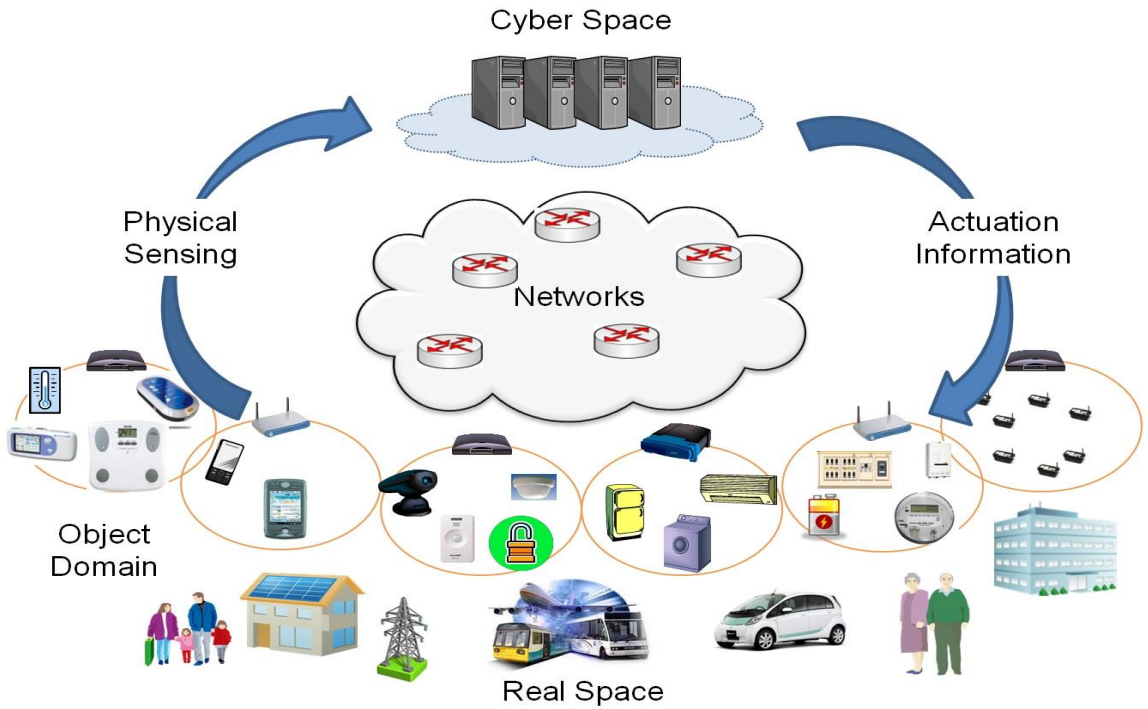
2. J3061의 주요 용어 정의

▣ CYBER-PHYSICAL SYSTEM 가상 물리 시스템

A system of collaborating computational elements controlling physical entities.

물리적 개체를 제어하는 컴퓨터 구성요소를 결합한 시스템

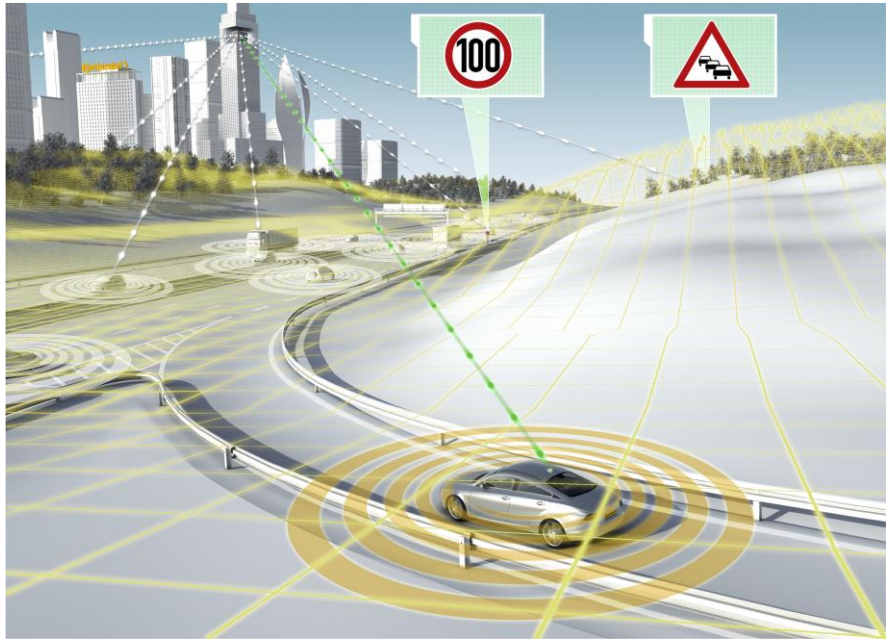
* 프로그래밍에 의해 만들어진 가상 세계, 즉, 디지털 환경과 물리적 법칙에 의해 운용되는 물리적 세계를 통합하는 개념이다. 사람의 개입 없이 사물을 직접 인터넷에 연결하고 이를 통해 데이터를 수집, 분석, 제어하는 실시간 분산제어 시스템으로 사이버상의 정보 처리 결과로 현실의 움직임을 제어할 수 있는 시스템이다.



▣ CYBER-PHYSICAL VEHICLE SYSTEM (CPVS) 가상물리 차량 시스템

Vehicle embedded control systems where there exists a tight coupling between the computational elements and the physical elements of the system and the environment around the system.

컴퓨터를 사용한 엘리먼트와 시스템의 물리적 엘리먼트 및 시스템 주변 환경 간에 긴밀하게 결합된 차량 임베디드 제어 시스템



2. J3061의 주요 용어 정의

▣ CYBER-ATTACK

An assault on system Cybersecurity that derives from an intelligent act, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade Cybersecurity services and violate the Cybersecurity policy of a system.

지능적 행위, 즉, 사이버보안 서비스를 우회하고 시스템의 사이버보안 정책을 위반하는 의도적인 시도(특히 방법이나 기법의 의미에서의)인 지적 행동으로부터 파생된 시스템 사이버보안에 대한 공격

▣ CYBERSECURITY 사이버보안

Measures taken to protect a cyber-physical system against unauthorized access or attack.

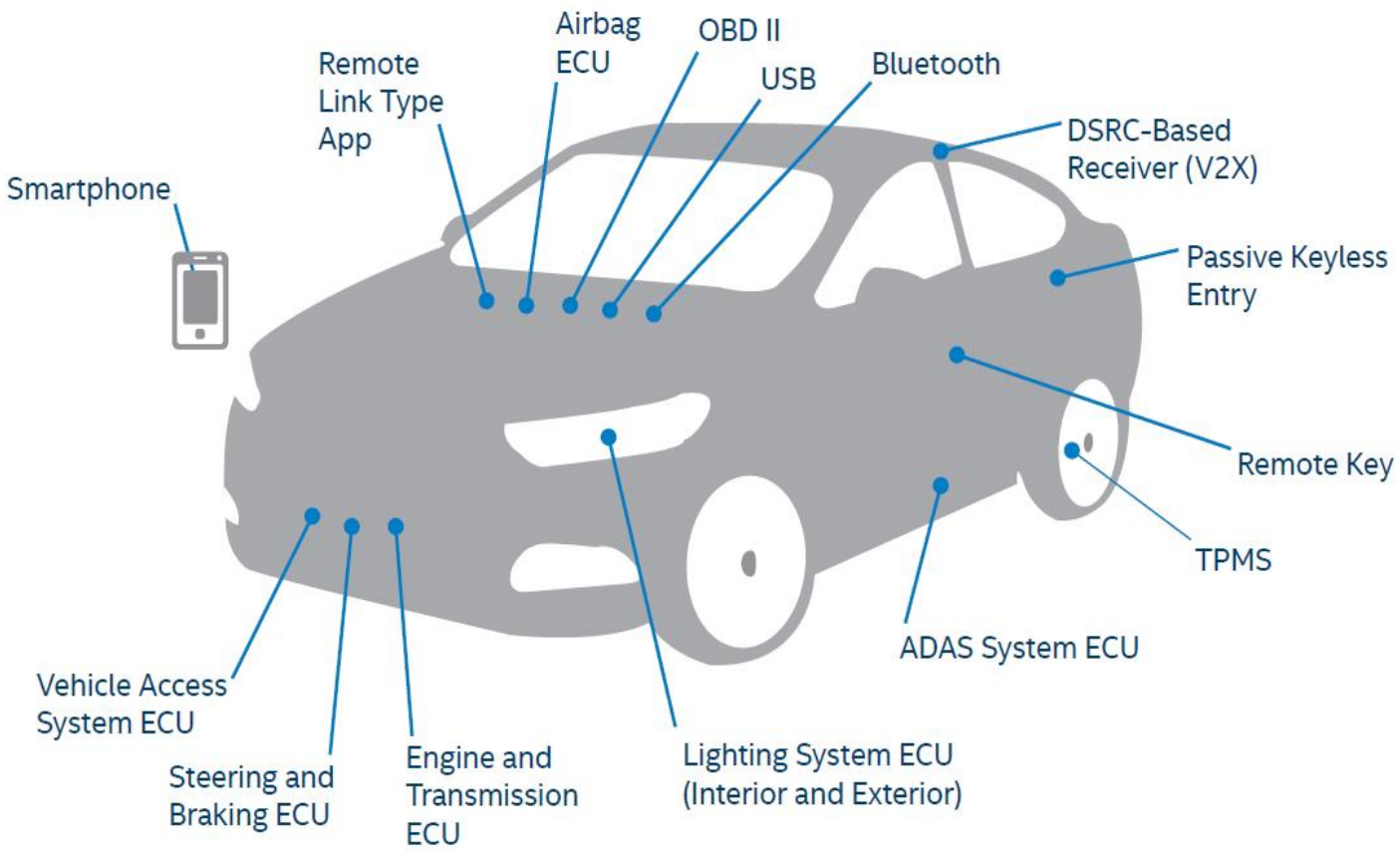
사이버물리 시스템을 비인가된 접근 또는 공격으로부터 보호하기 위해 취한 조치

2. J3061의 주요 용어 정의

▣ ATTACK SURFACE

The different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.

비인가된 사용자(공격자)가 데이터를 입력하거나 환경에서 데이터를 추출하려고 시도할 수 있는 여러 지점(공격 벡터)



Ref. The 15 weakest points of a connected car according to Intel

CF. Cybersecurity 주요 용어

▣ VUNERAVILITY (취약점)

- 하나이상의 위협에 의해 익스플로잇(exploit) 될 수 있는 자산 또는 자산 그룹의 약점

  Ref. ISO 27005

- 시스템의 설계, 구현 또는 운영 그리고 관리 중의 결함이나 약점으로 인하여 시스템의 보안 정책을 침해하기 위해 익스플로잇 될 수 있는 것

  Ref. IETF RFC 2828

- 1) 시스템의 민감성 또는 결함, 2)공격자가 결함에 대한 접근, 공격자가 결함에 대한 3)익스플로잇 가능성의 교집합으로 정의됨

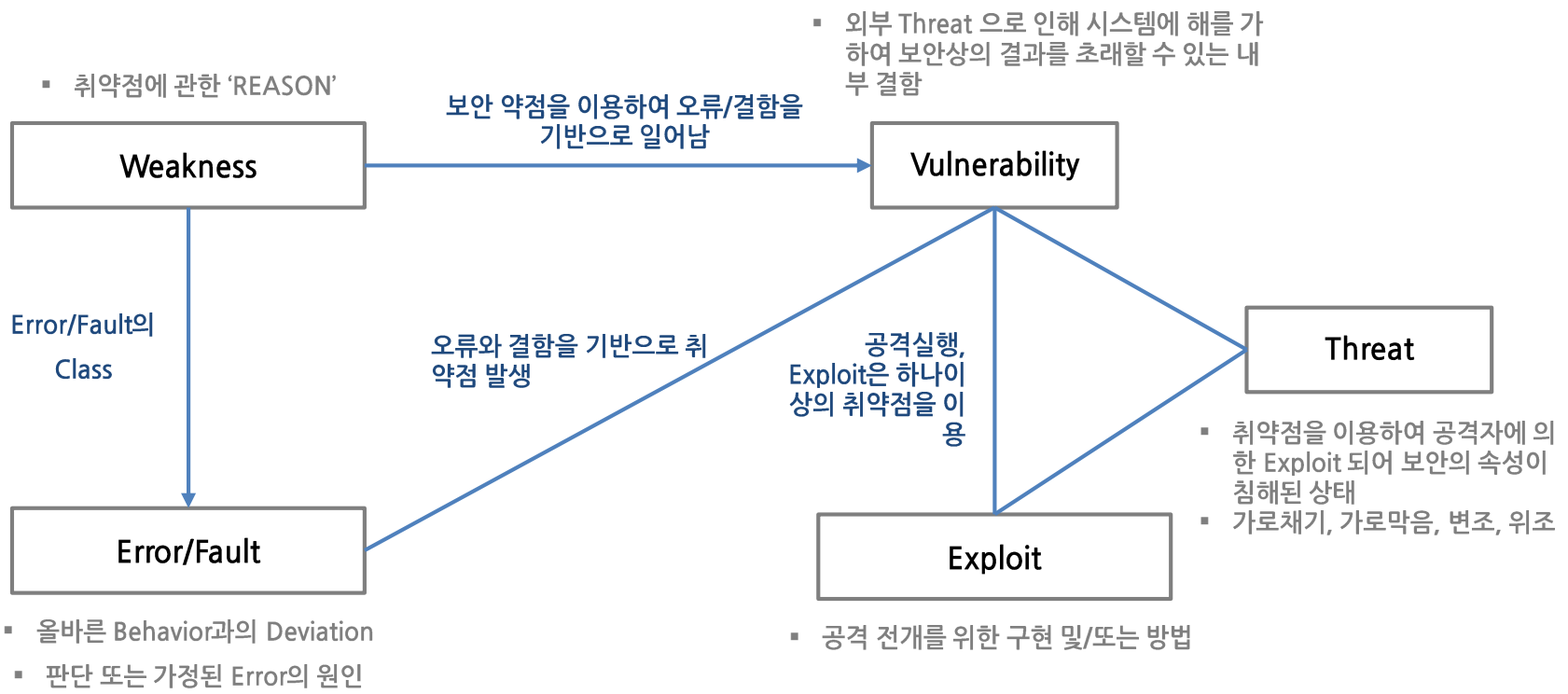
▣ THREATS (위협)

- 손실이나 손상의 원인이 될 가능성을 제공하는 환경의 집합

- Security에 해를 끼치는 행동 또는 사건

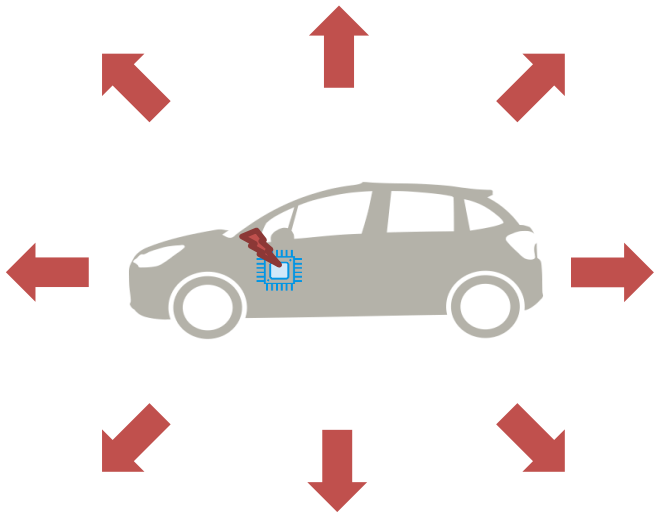
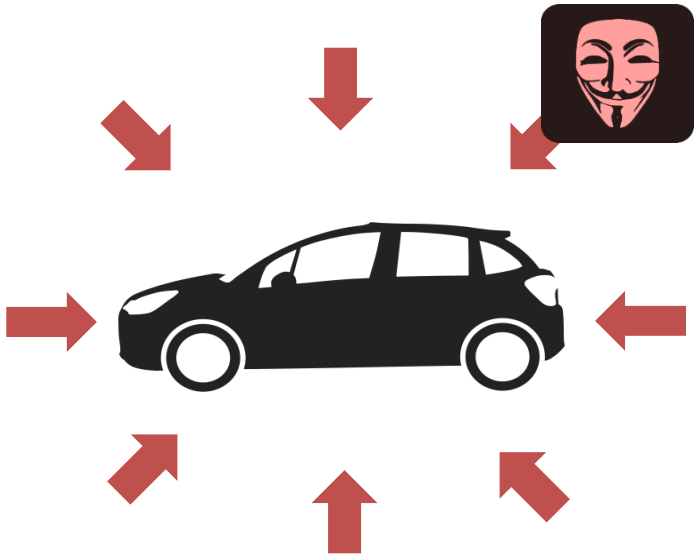
CF. Cybersecurity 주요 용어

▣ Relationships for Vulnerability and Threat



3. Safety system vs Security system

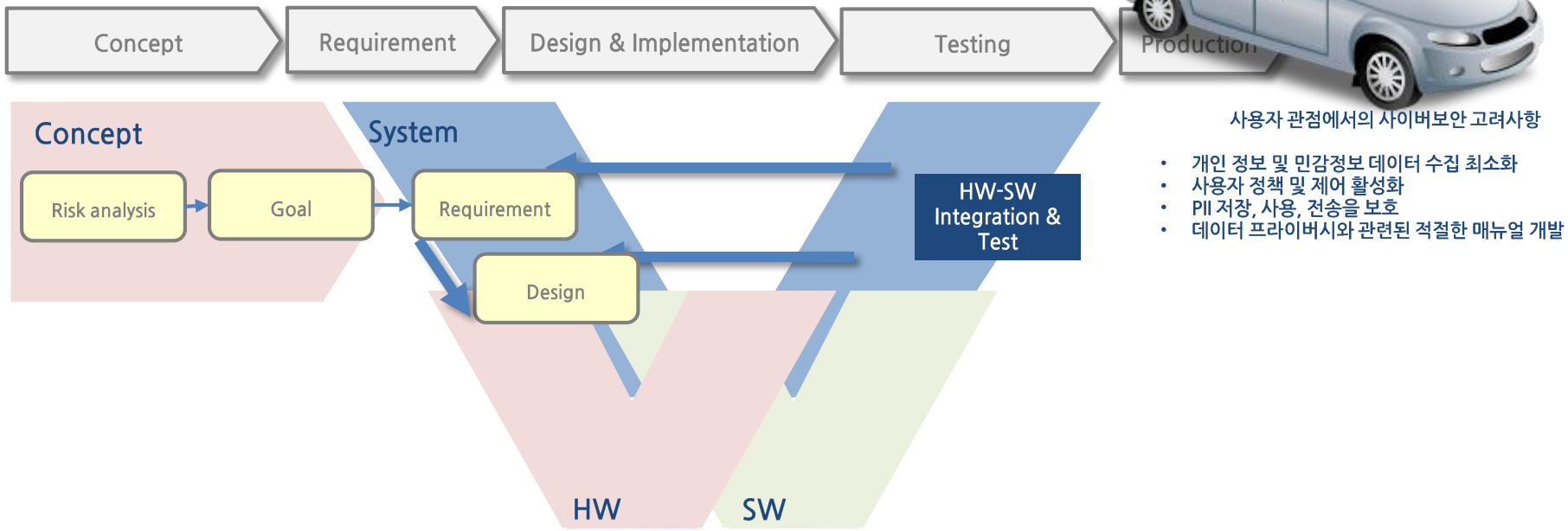
▣ Differences in Analysis Scope

Functional Safety	Cybersecurity
	
고장 (Malfunction) ▶ 재난(Hazard) ▶ 생명, 재산, 환경의 리스크(Risk)	취약점(Vulnerabilities) ▶ 위협(Treats) ▶ 자산, 운영, 개인 정보의 리스크 (Risk)

Ref. von Wedel, J.K. and Arndt, P., "Safe and Secure Development: Challenges and Opportunities," SAE Technical Paper 2018-01-0020, 2018, doi:10.4271/2018-01-0020.

4. Principle on SAE J 3061 for Cyber-physical vehicle system

▣ 차량의 전체 수명주기 단계별 사이버보안이 고려되어야 합니다.



사용자 관점에서의 사이버보안 고려사항

- 개인 정보 및 민감정보 데이터 수집 최소화
- 사용자 정책 및 제어 활성화
- PII 저장, 사용, 전송을 보호
- 데이터 프라이버시와 관련된 적절한 매뉴얼 개발

[컨셉 개발]

- 사이버보안을 고려한 Feature 설계
- Threats analysis
- Cybersecurity 수준 결정

[설계 및 검증]

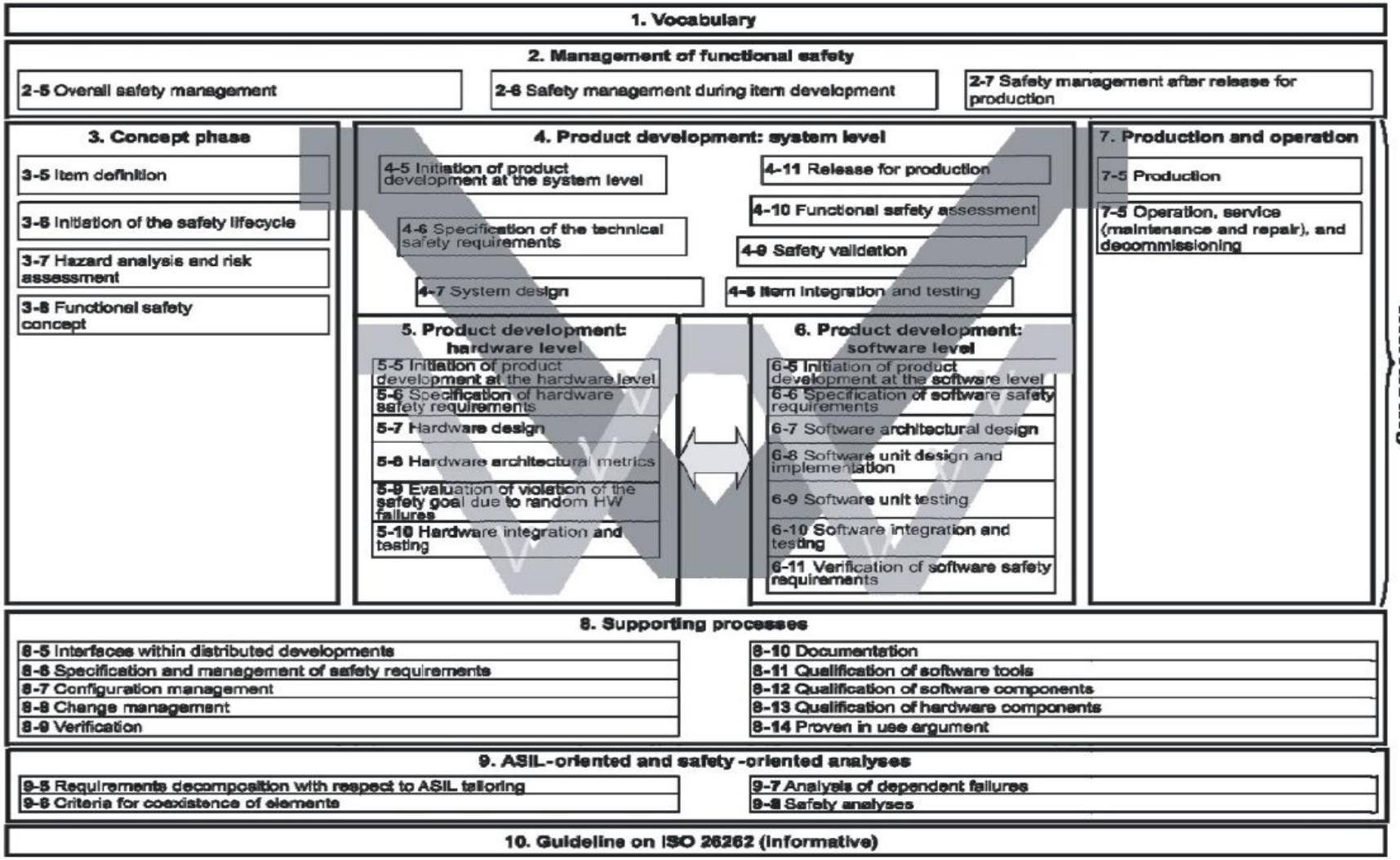
- 적절한 Cybersecurity Control (Cybersecurity Measure /Mechanism) 구현
- 단계별 사이버보안 분석 및 구현
- 설계가 사이버보안 요구사항을 충족시키는지 여부 검증 (Review/ analysis/ Testing) 수행
- 리스크 최소화 되었거나 제거 되었음을 확인

[운영 및 서비스]

- Incident Response 대응 프로세스

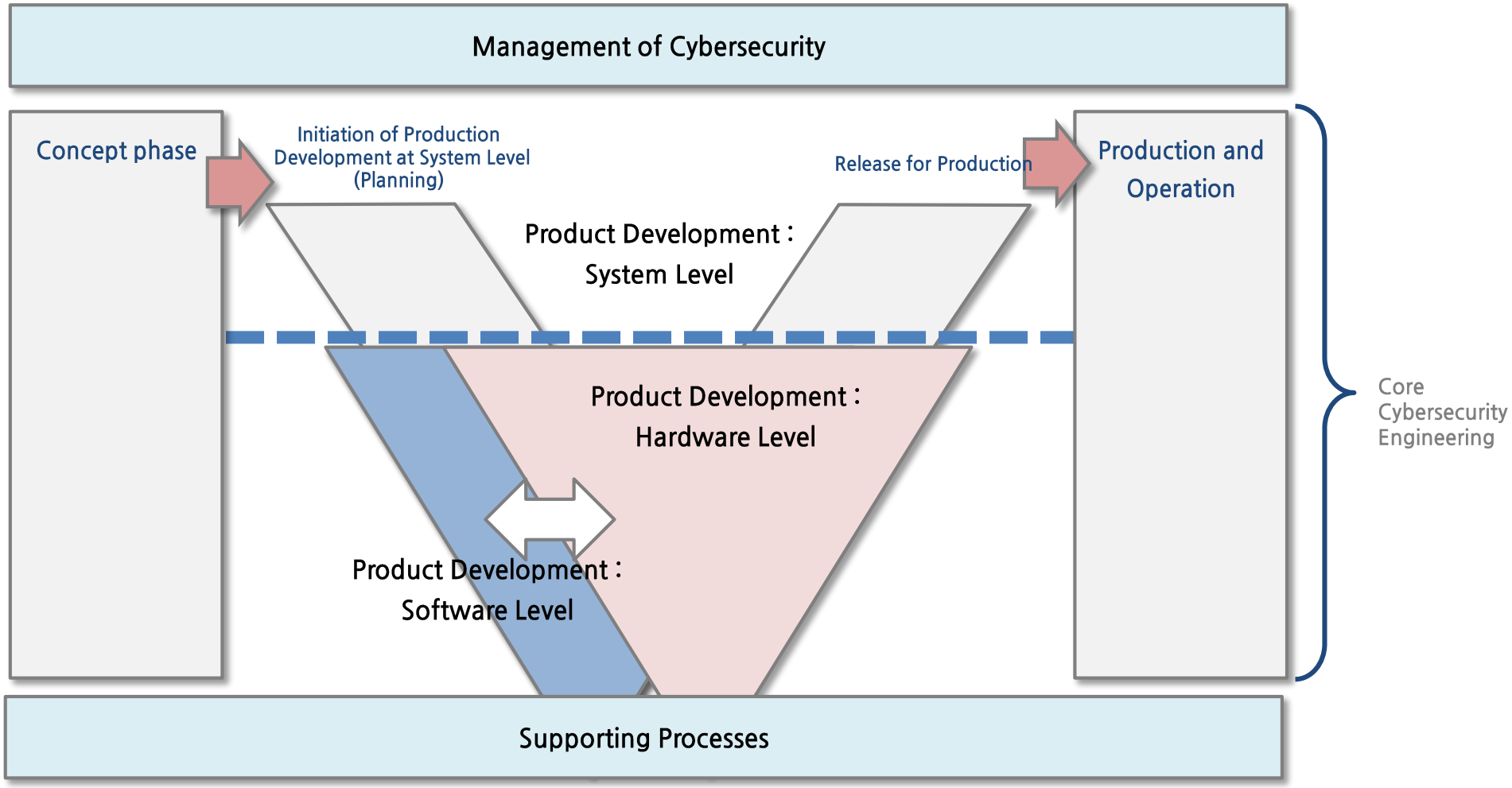
5. Cybersecurity Process Overview

▣ ISO 26262 기능안전 차량 표준에서의 프로세스 프레임워크를 선택하여 기존 안전 프로세스 측면을 활용 및 조정하여 두 영역 간의 상호 관계를 고려하여 사이버보안과 안전 간의 일관성 유지를 용이하게 할 수 있습니다.



5. Cybersecurity Process Overview

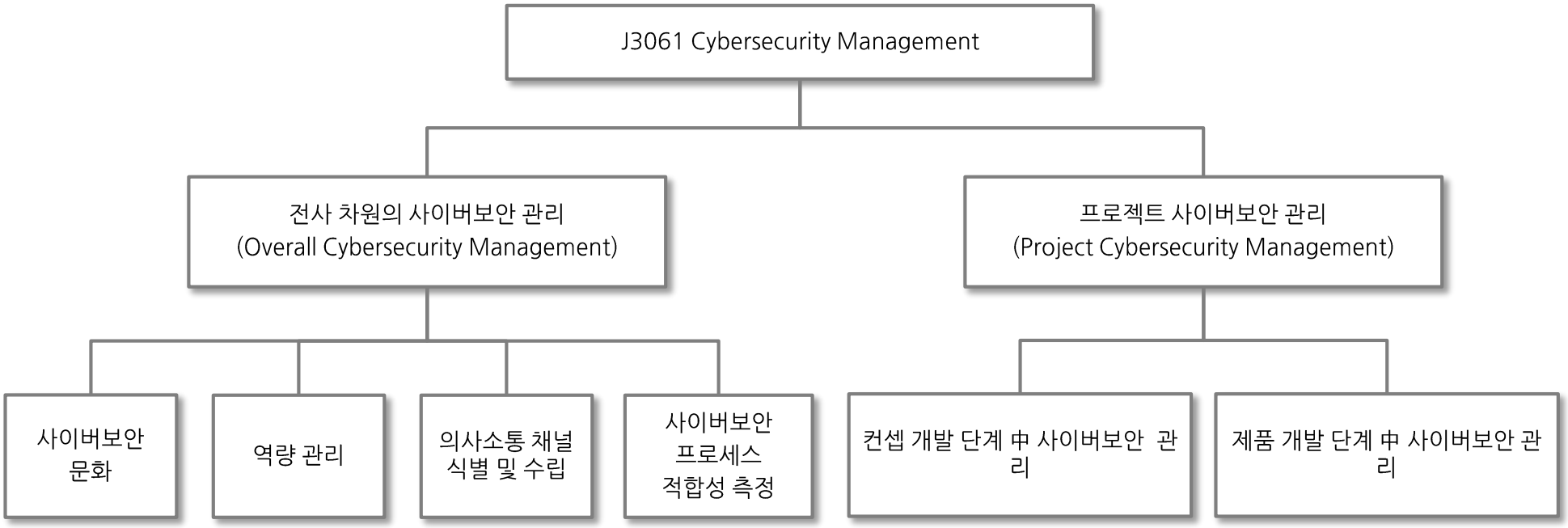
▣ ISO 26262 기능안전 차량 표준에서의 프로세스 프레임워크를 선택하여 기존 안전 프로세스 측면을 활용 및 조정하여 두 영역 간의 상호 관계를 고려하여 사이버보안과 안전 간의 일관성 유지를 용이하게 할 수 있습니다.



Ref. SAE J 3061 Figure 3 - Overall cybersecurity process framework

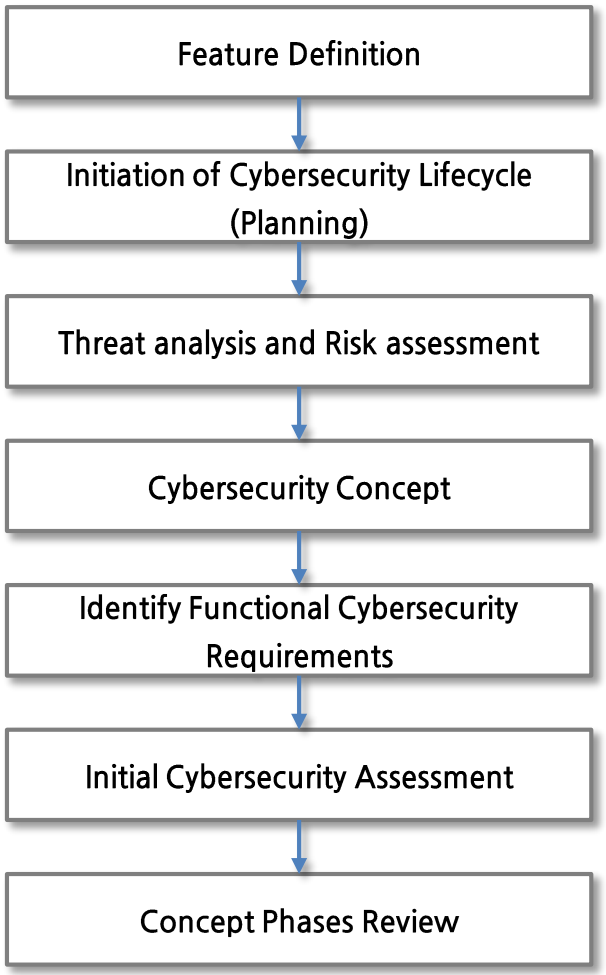
5. Cybersecurity Process Overview

▣ SAE J 3061 Cybersecurity Management Scope



5. Cybersecurity Process Overview

▣ Concept phase Overview



- 시스템의 정의
- 물리적 경계 및 신뢰구간(Trust boundary) 식별

- 사이버보안 수명주기 착수
- 사이버보안 개발 계획 수립(활동, 책임자, 시작/종료 일자 등)

- Threat identification
- Risk assessment(Threat classification)
- Cybersecurity goals identification

- Feature에 관한 사이버보안 획득을 위한 전략

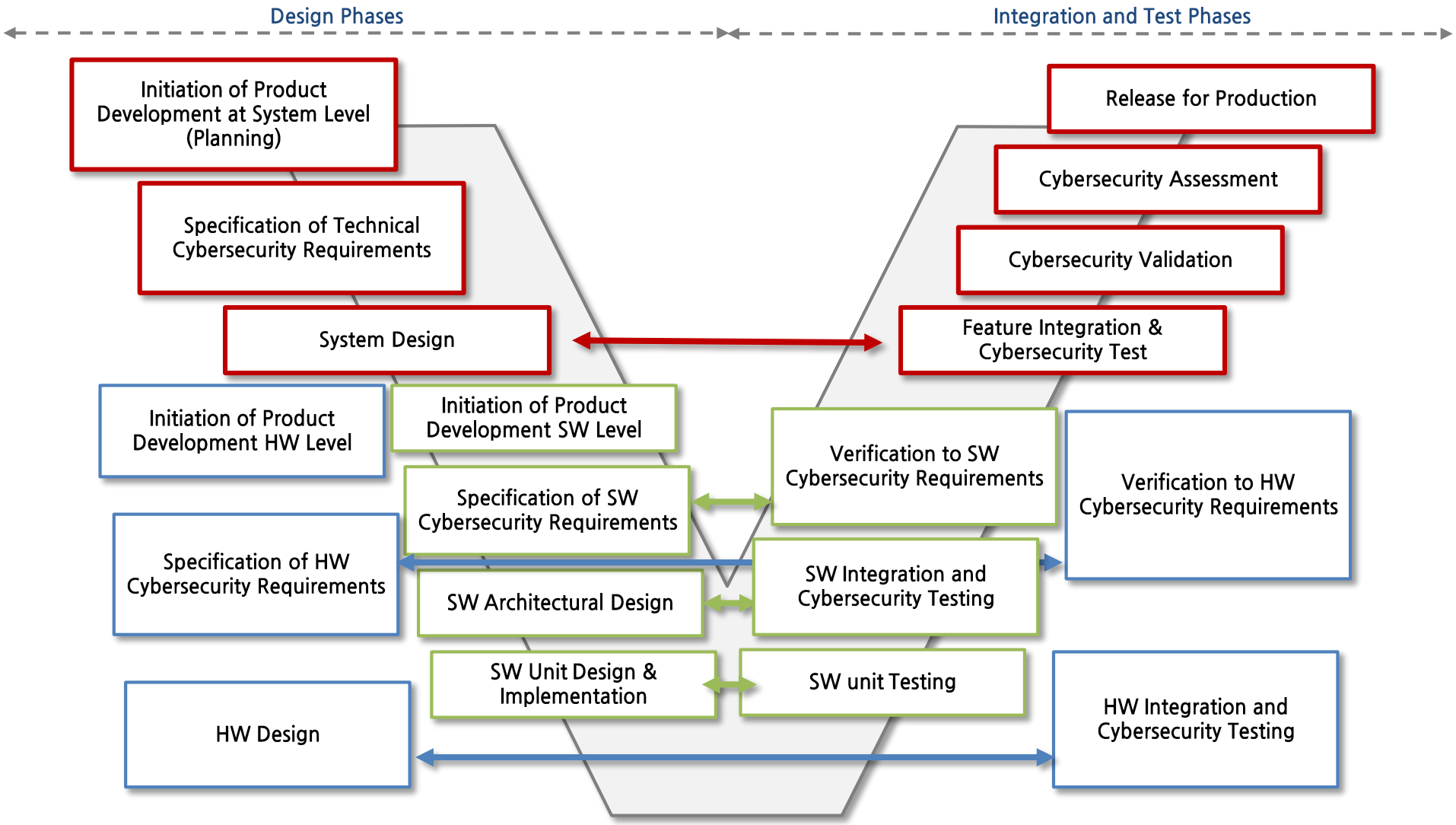
- Cybersecurity goal 달성을 위한 기능적 관점에서 기술

- Cybersecurity 달성 여부를 평가 착수
- Cybersecurity Case 개발 착수

- 마일스톤 및 게이트 리뷰

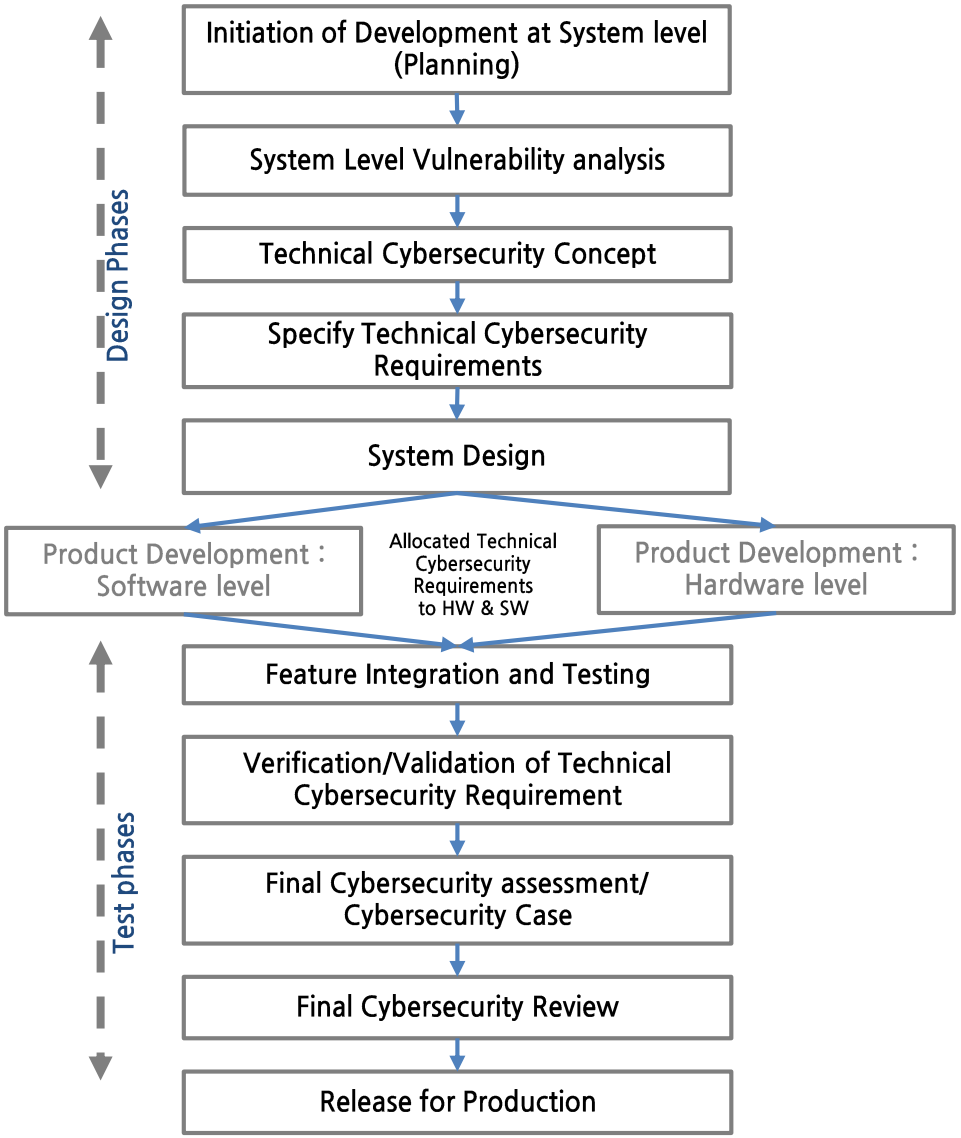
5. Cybersecurity Process Overview

▣ Relationships between product development at the system, hardware, and software levels



5. Cybersecurity Process Overview

▣ 시스템 수준에서 사이버보안 활동의 흐름



- Cybersecurity concept 상세화
- 상위수준의 cybersecurity requirements 및 Technical cybersecurity strategy으로 파생 및 상세화 수행
- Hardware-Software Interface
- Data flows, Data Storage, Data Processing
- 사이버보안 기능을 지원하는 기능

- Feature testing, testing Phase verification
- Cybersecurity를 위해 시스템의 의도된 기능에 대한 테스트
- Feature 간의 정확한 통신, 적절한 대책 기능 확인

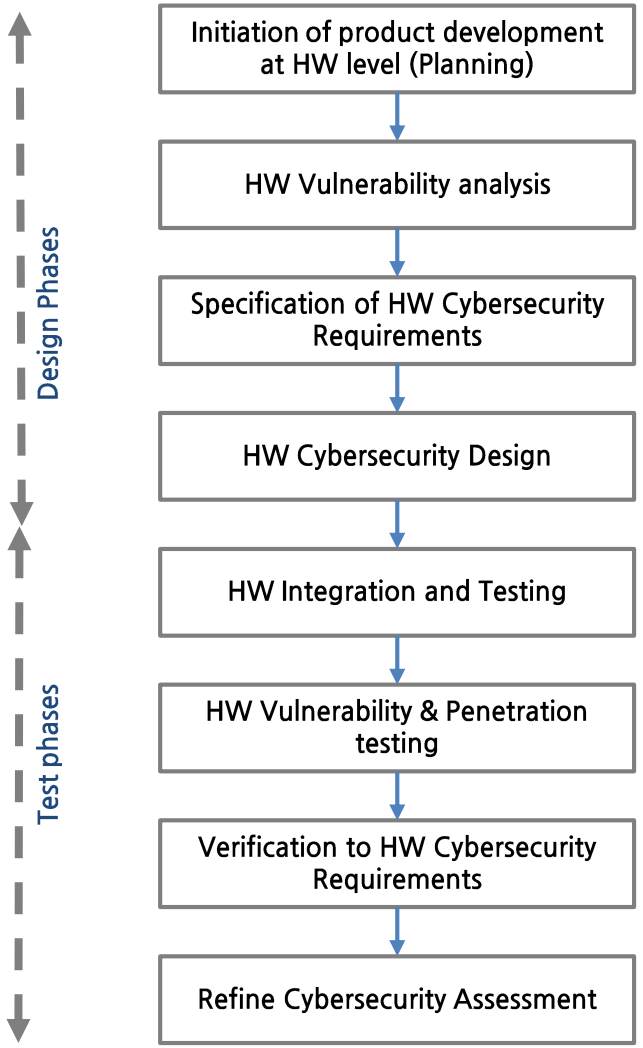
- Vulnerability Test / Penetration Test / Fuzz Test

- 개발 최종 단계에서 시스템에 의해 사이버보안 요구사항이 어떻게 부합되는지 여부를 평가
- 설계되고 개발된 시스템이 “Secure” 하다는 증거 및 논거를 제공

- 시스템 각 개발 단계별 활동의 완전성, 일관성, 정확성 검증

5. Cybersecurity Process Overview

▣ Cybersecurity activities on Hardware level



- Technical Security Concept 상세화
- HW Interface, Data Flow, Data Storage, Data Processing 등을 지원하는 Cybersecurity context 검토하여 성능, 효율성과 같은 매개변수로 정의

- Identify Cybersecurity controls to address the Vulnerability
- 변조, 허가되지 않은 물리적 접근, 리버스 엔지니어링 방지
- Trust anchors(HSM, SHE 통합)

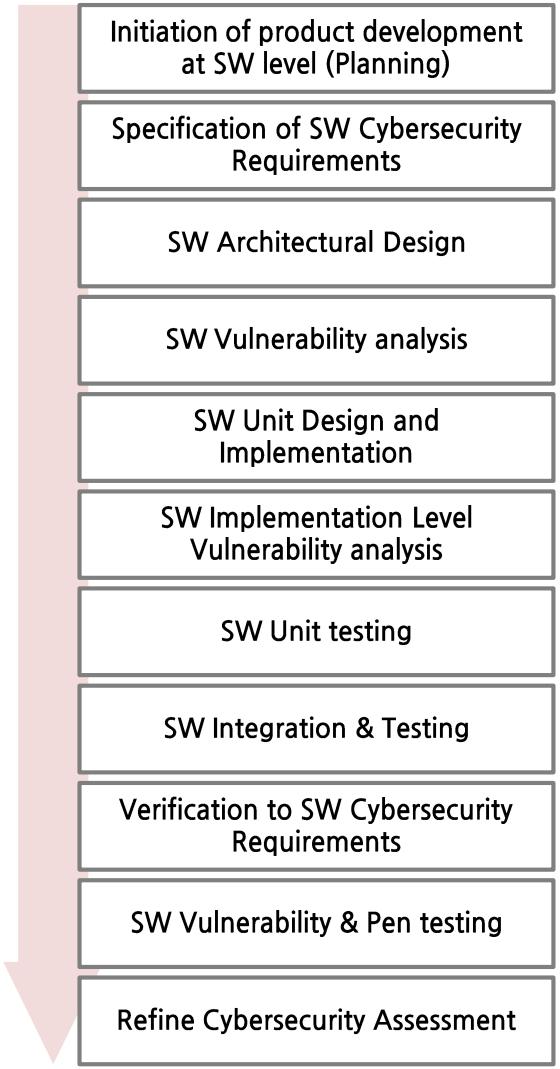
- Verification for HW Design phase
- HW 컴포넌트 기능, 성능, 및 신뢰성 요구사항 충족 여부 검증

- HW 레벨의 알려진 취약성 및 잠재 취약성 완화 여부 검증
- 사이버보안 통제의 구현 적절성여부 확인

- The preliminary Cybersecurity assessment refine

5. Cybersecurity Process Overview

▣ Cybersecurity activity on Software level



- Selection of Methods
- Programming and/or Modeling Languages
- SW 통합 및 테스트 계획

- 비인가된 접근 방지, 변조 탐지를 위한 SW의 사이버보안 기능 정의

- 데이터 유형, 데이터 흐름, SW 에러 검출 방법, SW 오류로부터 회복하는 방법 분석 설계
- 데이터가 기밀성, 무결성, 가용성을 유지

- SW Cybersecurity requirements, data flow 분석
- Identify Cybersecurity controls to address the Vulnerability

- MISRA 및 CERT C 함께 사용

- Verification for SW Unit Design phase

- Input/Output/Data Flow
- Edge cases, Error handling, Exception handling, Failure mode

- Verification for SW Architectural Design phase
- Vulnerability & Penetration testing

- Penetration testing
- Fuzzing testing

- The preliminary Cybersecurity assessment refine

5. Cybersecurity Process Overview

▣ Supporting Process

기존 제품 개발 프로세스와 통합되어 형상관리, 문서화 관리, 변경 관리 등 ISO 26262 지원 프로세스 활동이 사이버보안에 특화되어 조정 및 적용이 필요합니다.

Configuration Management	• 제품 개발 수명주기 내에서 시스템을 고유하게 식별되고 재현될 수 있도록 보장
Requirements Management	• 요구사항의 속성 및 특성을 정의 • 전체 수명주기 동안 일관된 요구사항 관리를 보장
Change Management	• 시스템/제품에 대한 변경사항 분석 및 제어 • 변경을 위한 의사결정 프로세스 도입 필요
Documentation Management	• 개발되는 시스템에 대한 문서/artifact의 문서화 관리 전략 개발
Quality Management	• QS 9000, ISO/TS 16949 또는 유사한 품질 관리 시스템을 수립
Distributed Development	• Supplier의 역량 평가 및 Customer 또는 Supplier 간의 개발 인터페이스 합의 도출

5. Cybersecurity Process Overview

▣ Production & Operation/Service

Cybersecurity requirements과 관련된 생산 프로세스의 확보 방안에 대한 요구사항과 Overall Cybersecurity Managements에서 정의된 필드 모니터링 프로세스(Field Monitoring Process) 와 사고 대응 절차(Incident Response procedure) 수행과 유지가 적용되어야 합니다.

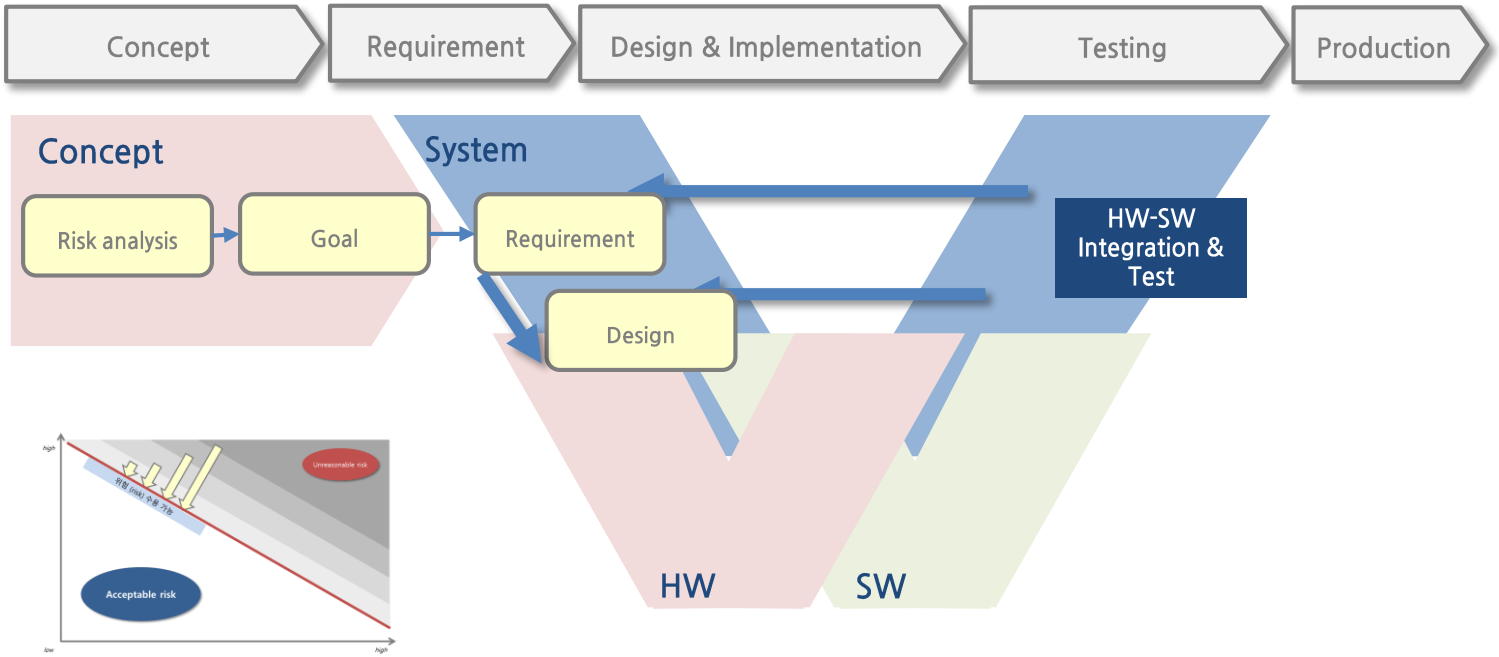
Production	
개발 시스템 공급사 관점	• 공정 능력이 제대로 충족되고 있음을 증빙 • 사이버보안 책임을 고객에게 설명 • 사이버보안 관련된 특별 특성에 대한 접근, 교환 및 생산 모니터링을 제공하는 공급자 계약서 체결 • 사이버보안 관련 사고 발생시 분석 및 이슈 보고
OEM 관점	• 수명종료 시점에서 사이버보안 고려사항(개인정보/암호 삭제 등) 관리 • 사이버보안 문제에 대한 필드 모니터링 • 사이버보안 문제에 대한 사고 대응 계획 준수

Operation and Service	
필드 모니터링	• 사이버보안 사건 정보를 수집하고 공유를 목적으로 함 • 사고 대응을 위한 전담팀이 구성되고 상시 운영됨을 보증하여야 함 • 타사 사이버보안 사건 사례, 법적 분쟁, Hacker Chat 등에서 정보 수집 및 분석
사고 대응	• 자동차 산업에서 발생하는 사이버보안 사고에 대응하기 위함 • 조직 또는 다른 조직의 사이버물리적 차량 시스템에 대한 직접적인 공격 발생시 사고의 억제 및 사고 완화 조치 이행 • Potential Incident 적시에 보고 필요

6. Communication Point between Safety Process & Cybersecurity Process

▣ Safety system과 Cybersecurity system Engineering의 유사성

기존 설계에 새로운 Feature를 추가하는 것이 아니라 설계에서 안전 또는 사이버보안 설계를 구현하는 것으로 시스템 공학 측면에서 접근이 필요합니다.



6. Communication Point between Safety Process & Cybersecurity Process

▣ Safety system과 Cybersecurity system Engineering의 차별성

System safety	System cybersecurity
considers potential **hazards** to identify safety mechanisms that can be integrated into the design to address the causes of the potential hazards	considers potential **threats** posed by a malicious attacker whose goal is to cause harm, wreak havoc, gain financial benefits, or simply to gain notoriety
- Potential hazards and causes are more readily identified - Appropriate action to mitigate the potential consequences, or to eliminate the potential hazards all together can be taken - **Causes of hazards based knowledge of system, components, and interaction** - Focus on sub-systems	- Cyber Security **threats are more difficult** to address than potential safety hazards - More difficult to try to anticipate the exact moves an attacker may take in order to add appropriate Security Controls to protect against attacker's options. - Causes maybe unknown - Additional factors in risk assessment: **attacker's experience level, attacker's access, attacker's need for special equipment** - Focus on sub-systems AND electrical architecture (i.e. possible access to safety-critical areas through non-safety-critical area, i.e. CD player)
FTA(Fault tree analysis) identifies potential causes of the top hazard event and looks for single-point and multi-point random hardware failures.	**ATA(Attack tree analysis)** we are not concerned with single-point and multi-point random hardware failures, but rather with **determining potential paths that an attacker could take through the system to lead to the top level threat.**

6. Communication Point between Safety Process & Cybersecurity Process

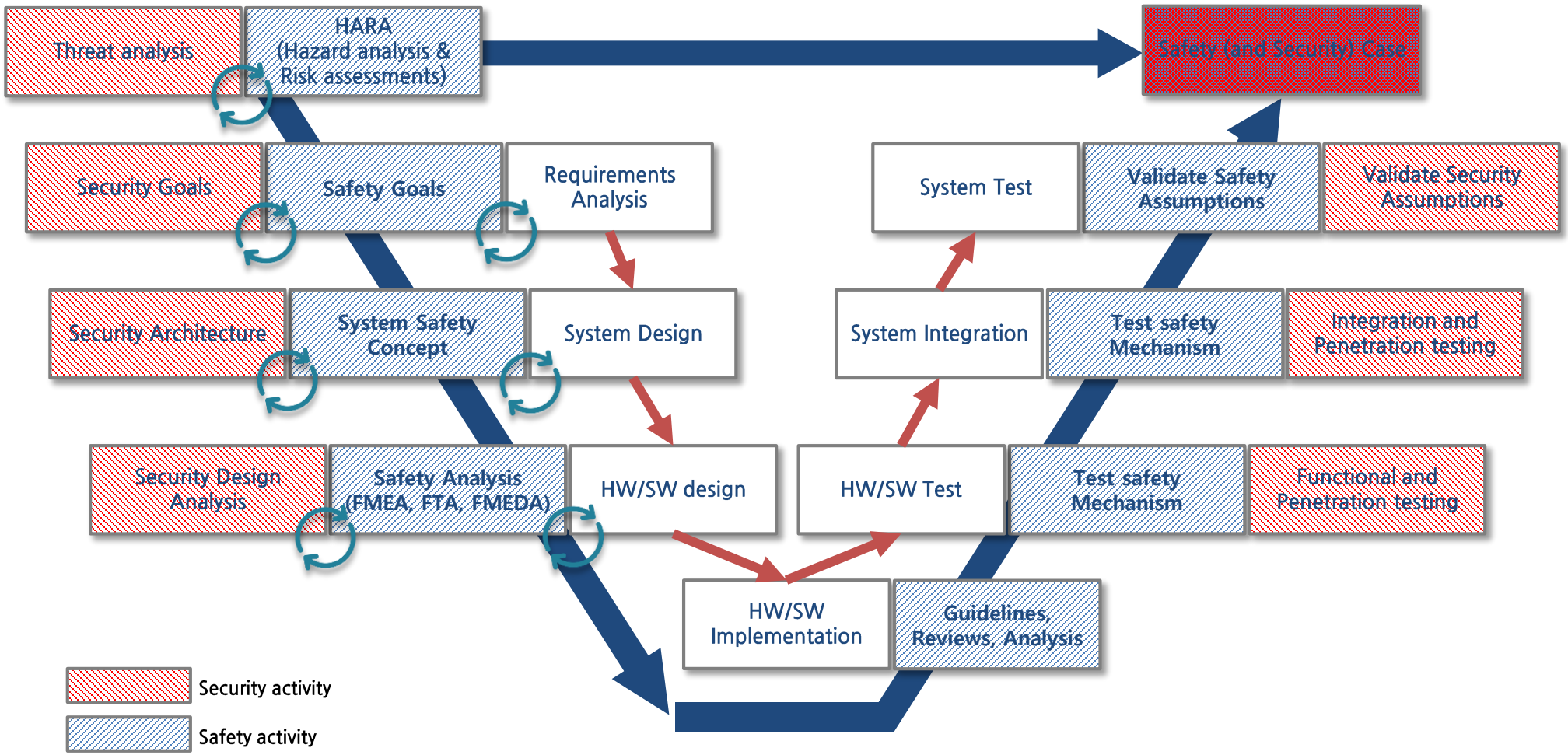
▣ Safety system과 Cybersecurity system Engineering의 차별성

Analysis		Safety Engineering	Security Engineering
Subject	Risk	Hazard	Threat
	System inherent deficiency	Malfunction	Vulnerability
	External enabling condition	Hazardous situation	Attack
Category	Impact analysis	Severity	Threat criticality
	External risk control analysis	Controllability	Attack Skills, Know-how
	Occurrence analysis	Exposure	Attack resources & Surface
Result	Design goal	Safety Goal	Security Target
	Design Goal criticality	ASIL	SecL

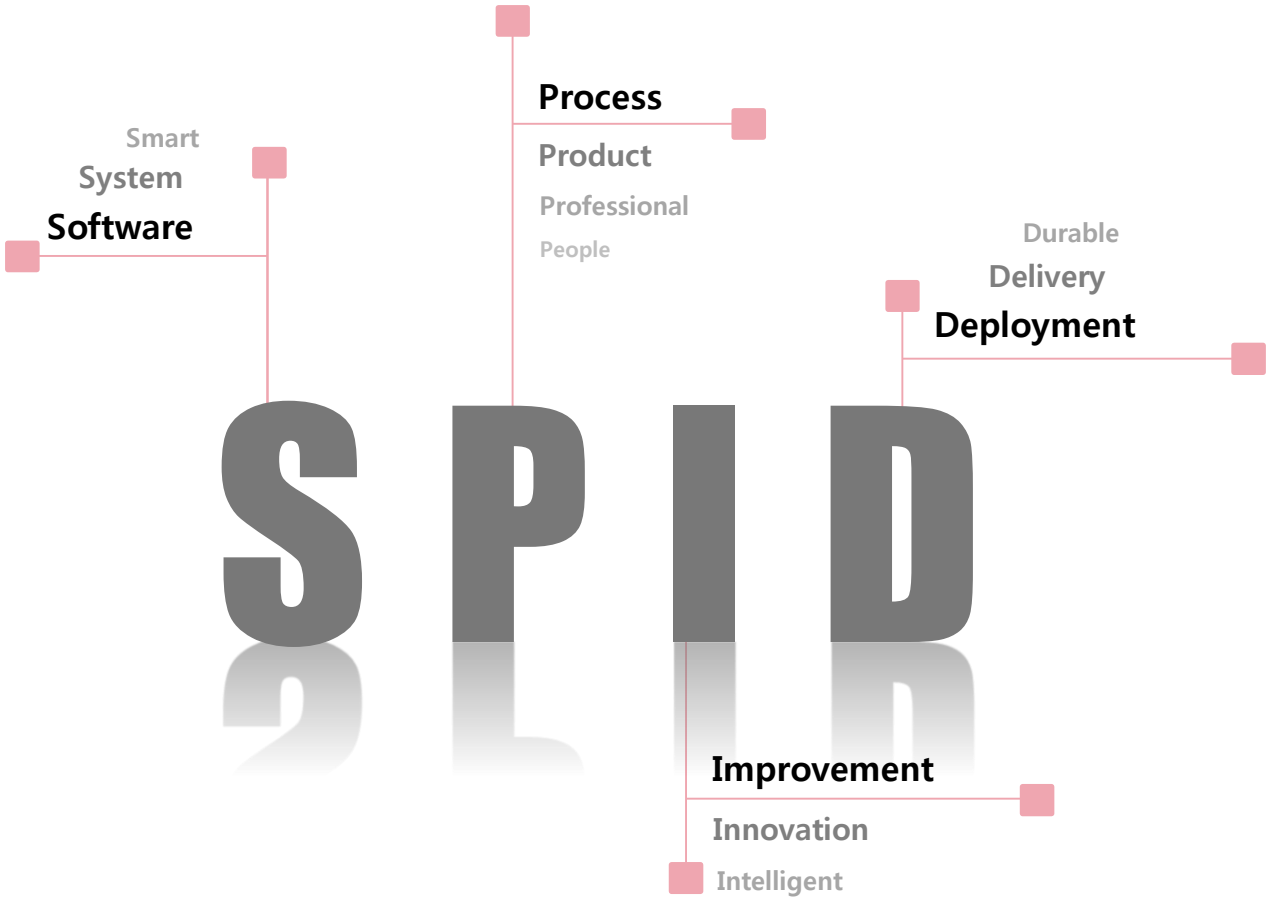
Ref. Integrated safety and security Development in the Automotive Domain, SAE Technical Paper, 2017-01-1661

6. Communication Point between Safety Process & Cybersecurity Process

▣ Integrated cybersecurity and Safety process



Ref. Automotive Functional Safety = Safety + Security, **SecurIT'12, August 17-19, 2012, Kollam, Kerala, India**



spid

㈜에스피아이디

서울시 강남구 선릉로93길 27, 아름빌딩 4층 (135-513)

02-3453-5345 / Fax: 02-3453-5346 / spid@spidconsulting.com

www.spidconsulting.com / www.spidconsulting.co.kr