중소기업 기술국산화 전략품목 상세분석

<자동차>

중소벤처기업부
TIPA 중소기업기술정보진흥원

10.EVITA secure 기반 보안 반도체 및 암호화 모듈

1. 개요

가. 개념 정의

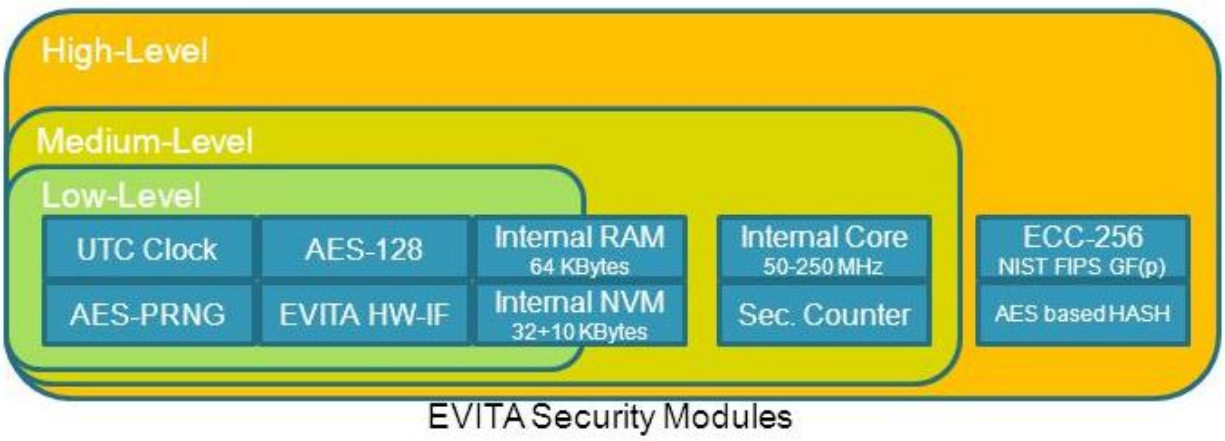
☐ 커넥트드카의 기반이 되는 V2X(Vehicle to everything)용 EVITA(E-safety Vehicle Intrusion proTected Applications)/UNECE(UNECE Automotive Cybersecurity Regulation) 등 차량용 보안규격을 만족할 수 있는 통신 반도체 핵심 제품 및 기술

- EVITA(E-safety Vehicle Intrusion proTected Applications) 프로젝트는 자동차 환경의 변화에 따라 요구되는 차량 보안을 위해 암호화 과정에서 사용되는 정보나 차량 제어, 사용자 정보 등 중요한 정보들을 해킹이나 도청 등으로부터 보호하기 위한 시스템 설계 및 인터페이스 설계 기준

- EVITA에서는 시큐리티 프레임워크 구성 기술에 네트워크 보안 기술과 호스트 기반의 보안 기술이 포함되어 있으며, 이에 대한 대응이 가능한 보안 시스템반도체 및 암호화 모듈 (HSM:Hardware Security Module) 등의 V2X 통신 반도체 기술

- 자동차 보안에서는 차량 내부 정보의 보안과 여러 기능이 안전하게 수행되는 것이 중요하기 때문에 차량 내부에서 사용되는 데이터의 무결성, 확실성, 신뢰성이 요구되며, 이러한 요구사항을 만족하기 위해서 각 기능의 보안 요구 수준에 따라 해당 프로그램을 수행하는 영역을 다르게 하는 방법, 인터페이스의 분리 등의 추상화 기능, 효율적 보안 기능 수행을 위한 하드웨어 지원 등 복합적인 기술이 통신 반도체 기술로서 적용됨

[EVITA security 기반 보안 반도체 및 암호화 모듈 구조]



☐ 차량용 ECU와 센서 사이의 통신 보안을 위해서는 각 전장부품이 공용키를 가지고 있어야 하며, 통신을 통한 정보 이동에서 암호화 기능이 내재된 사양에 따라 하드웨어 혹은 소프트웨어로 구현된 HSM 암호화 모듈 기술

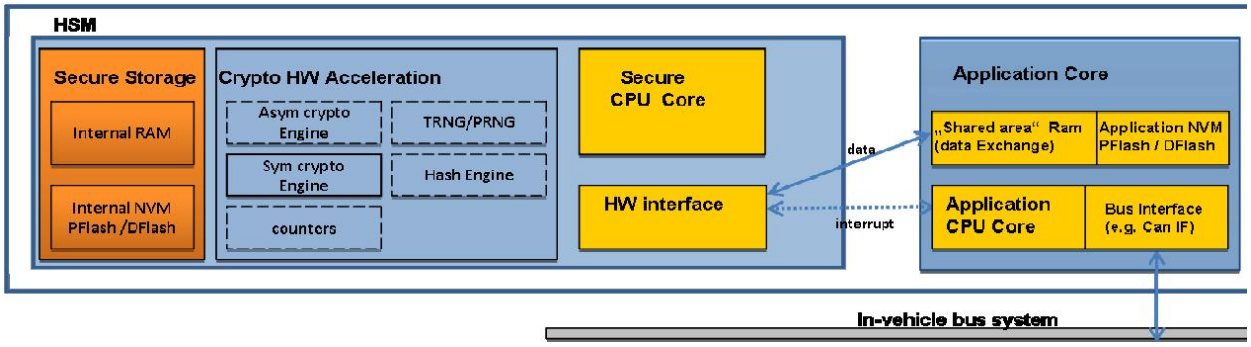
- HSM 암호화 모듈 기술에서 공용 키는 통신을 위해 계속 사용돼야 하고 비휘발성 저장매체에

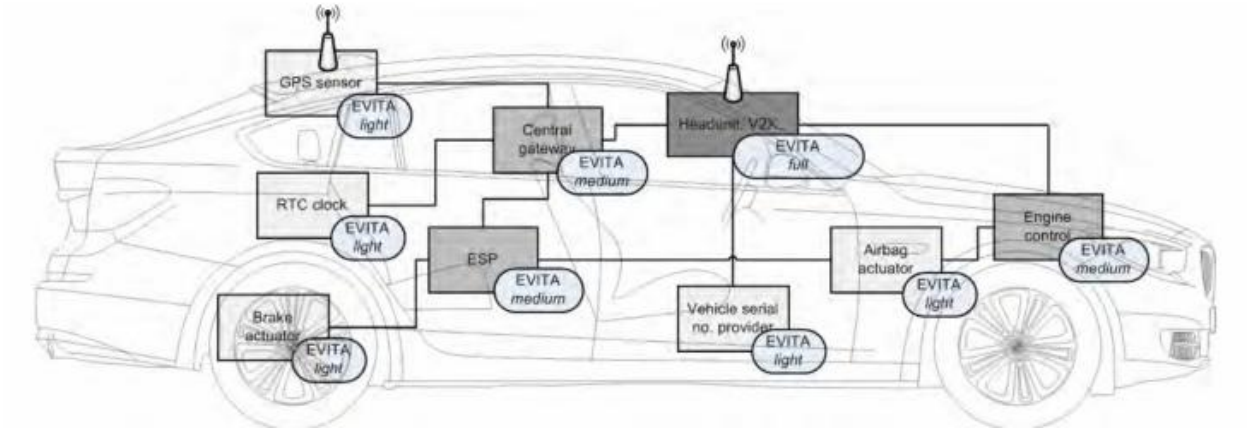
저장되어야 하기 때문에 보안기능이 있는 비휘발성 저장매체가 각 전장부품에 장착됨

☐ EVITA security 수준을 만족시킬 수 있는 암호화 기능을 포함하여 명확성을 확인하는 기능과 전자서명 기능이 포함되어 있고, 난수 발생 기능과 비대칭 암호화 엔진도 포함돼 있는 HSM 기술

- 암호화 기능 이외에 보안 저장매체 기능, 이를 동작시키기 위한 CPU, 보안 기능들을 애플리케이션에서 사용할 수 있도록 인터페이스 등이 내재화된 EVITA 시큐리티 프레임워크 설계 기술

[자동차용 온보드 보안 모듈 및 네트워크 구조 연결 예시]





☐ EVITA에서의 HSM에서는 Trusted Computing과 Cryptographic Hardware 등으로 구분함

[EVITA HSM의 기술적 특징]

분 류	기술적 특징
Trusted computing	• 보안 연산의 신뢰성을 위해 사용 • 운영체제에서 필요로 하는 보안 기술과 더불어 보안이 취약한 응용 프로그램과의 연동이나 분산화 되어 있는 환경에서 사용 등을 예로 들 수 있음
Trusted Platform Module	• 보안기능 동작을 위해 필요한 연산을 보안이 유지되는 곳에서 수행 • 하드웨어 기반의 난수 발생, 암호화 엔진, 해시 함수 엔진, 보안저장매체(ROM, RAM, EEPROM) 등을 예로 들 수 있음
Core Root of Trust for Measurement	• 전장부품의 부팅 시 변조나 허가받지 않은 소프트웨어가 동작하는 것을 방지하는 기능 • 부팅 과정에서 전장부품의 이전 저장되어 있는 상태와 비교해 변동 사항이 없음을 확인함으로써 전장부품에 대한 침입이 없음을 증명
Trusted Software Stack	• 보안 운영체제나 애플리케이션에게 제공되는 보안 기능들에 대한 소프트웨어 모듈이나 컴포넌트 • 보안을 위한 암호화 인터페이스를 제공하고 보안 동작을 위한 보안키를 관리
Cryptographic Hardware	• 암호 알고리즘의 하드웨어/소프트웨어 구현의 설계 및 제작 • 추가적인 암호화 가속 기능으로 기존의 기능처리 시간 요구사항을 만족

나. 중요성 및 의의

☐ 커넥티드카 전장부품의 통신 환경은 여러 통신 기술들의 집중화와 다양성이 커지면서 탄력적이고 여러 단계를 제공하는 보안 기술이 요구되며, 다양한 보안 기술을 제공하기 위해서 보안 하드웨어가 필수적으로 적용되어야 함

- EVITA 보안 통신의 주체에 대한 확신을 위해 Message Authentication Code와 같이 인증 기능이 요구됨
- 차량용 ECU의 경우 보안 기능들을 수행하기 위해 독립적인 타이머나 프로세서, 난수 발생 모듈 등의 기능이 필요
- 센서의 경우 ECU와 같은 고 사양의 전장부품이 아니므로 암호화모듈이 소프트웨어로 제공되거나 내부 RAM에 보안 기능이 없을 수 있으나 경량형 센서 ECU의 경우에도 기본 보안 기능 탑재 필요

☐ 응용 어플리케이션에 따라 EVITA의 요구사항을 만족하기 위해서는 Full, Medium, Light와 같은 형태의 3단계 보안수준의 HSM 구성 필요

- Full HSM: 헤드 유닛처럼 V2X 메시지를 처리하는 경우는 빠른 비대칭 암호화 처리 및 키관리, 인증 기능 등이 필요
- Medium HSM: 각 ECU의 경우 비대칭 암호의 처리는 상대적으로 덜 중요하고 대칭키 암호화 처리나 키 관리 등의 기능을 수행
- Light HSM: 센서나 액추에이터와 같이 상대적으로 저 사양 및 보안 요구사항이 낮은 경우의 보안 기능 수행

☐ 커넥티드카를 위해서는 보안 기능의 적용 용이성 및 유연성을 최대로 하기 위해, 모든 보안 모듈은 각각의 보안 정책을 준수하고 시행할 수 있도록 구성돼야 하며, 이러한 보안 정책에는 허가, 프라이버시, 인증, 침입 감지 및 대응 정책 등이 적용된 보안 모듈 기술 필요

- 차량 보안 정책은 특정 개체의 접근이나 특정 리소스 사용에 대한 허가 정도를 구체화시키고, 프라이버시 정책은 데이터 및 정보의 공개 수준을 규정함
- 커넥티드카를 위한 인증 정책은 어떠한 인증 방식을 사용할 것인지, 예를 들어 패스워드를 사용할 것인지 스마트카드를 사용할 것인지 등을 정의가 필요하며, 대응 보안 모듈 기술 개발 필요
- 커넥티드카를 위한 침입 감지 정책은 특정 공격 시나리오와 공격 학습을 정의하며, 침입 대응 정책은 감지된 공격 종류에 대해 어떠한 대응 방식을 사용할 것인지를 정의하여 이에 대한 기술 개발 필요

다. 가치사슬 구조 및 분류

(1) EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈의 가치사슬

☐ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈은 커넥티드 자동차에서 차량 보안 레벨에 대한 대응을 위해서 핵심기술로 사용됨

☐ 차량의 여러 ECU 통합화가 진행 중으로 70개가 넘는 ECU의 기능을 일부 통합하고 그 수를 줄임으로써 자동차의 중량을 줄이고 보안 관련 ECU관리를 효율적으로 할 수 있도록 하는 개발이 진행중

- 전장부품 개발을 위한 보안 표준 제정 및 보안 인터페이스 표준화를 통해 보안 기술개발을 용이하게 하고 여러 공급사들이 각 소프트웨어의 일부 보안 모듈을 개발해 생산할 수 있는 형태로 진행 중임

☐ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈은 커넥티드 자동차용 핵심부품이자 모듈로서 후방산업은 반도체 소자 및 소프트웨어로 대표되는 소재부품 산업과 전방산업은 자동차, 모빌리티 등의 기계부품 제조업으로 구성되어 있음

[EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 산업구조]

후방산업	보안 반도체 및 암호화 모듈 제조 분야	전방산업
반도체소자 등 생산/판매 소프트웨어 개발/판매	자동차용 보안 반도체 및 암호화 모듈 설계/판매 산업·가전용 보안 반도체 및 암호화 모듈 설계/판매	자동차, 모빌리티 등 제조업 로봇, 보안안전 등 제조업 스마트 홈, 스마트 팩토리 등 설비업

(2) EVITA 소프트웨어 시큐리티 모듈의 분류

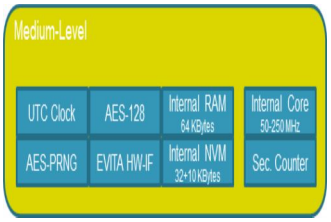
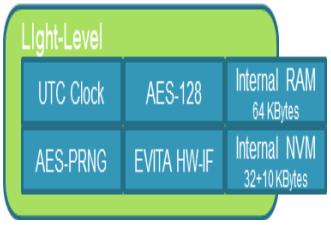
☐ EVITA 소프트웨어 시큐리티 프레임워크의 모듈들은 각 ECU들의 역할과 요구사항 및 성능에 따라 구분됨

[EVITA 소프트웨어 시큐리티 프레임워크 모듈의 분류]

분류	사용목적
EAM(Entity Authentication Module)	• 식별, 계정 관리, 싱글 사인 온(Single Sign-On, SSO)/사인 아웃 구현, 프라이버시 보호 메커니즘 등 인증 관련 태스크를 제공하며, 다양한 인증 메커니즘을 통합
CCM(Communication Control Module)	• 보안 통신을 위한 High-level 인터페이스를 제공 • 모듈은 모든 내부 프로세스 통신과 모든 차량 통신, 차량 내부 및 외부 개체들 사이의 통신을 보호하고 제어 • CCM은 상호 호출 및 통신을 위한 모든 시큐리티 모듈에서 사용
PDM(Policy Decision Module)	• 정책의 관리 및 접근과 정책 결정에 대한 인터페이스 제공 • 방화벽과 같이 특수화된 PDM에게 결정을 위임 • PEP(Policy Enforcement Points)는 리소스에 대한 접근 요청을 받고 접근 제어 결정을 시행하는 포인트로, 독립적인 모듈로 존재하는 것이 아니라 추상적인 서브 PDM으로 동작
SWD(Security Watchdog Module)	• 침입 감지 및 대응에 대한 메커니즘을 제공 • SWD는 보안 파라미터를 모니터하고 그에 상응하는 보안 응답을 발생
PIM(Platform Integrity Module)	• EVITA HSM 서비스와 관련된 보안 서비스를 제공
SSM(Secure Storage Module)	• 데이터의 보안 저장을 위한 서비스를 제공 • 공격자의 접근이 가능한 비휘발성 데이터 스토리지에 대한 보안 요구사항(기밀성, 무결성/진위성 등) 및 기능적 요구사항을 제공
CRS(Cryptographic Services Module)	• 암호화 기능 및 프리미티브에 대한 인터페이스를 제공 • 암호화 서비스를 필요로 하는 시큐리티 모듈 또는 프로그램에 통합되기 때문에 모듈 및 라이브러리

☐ 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈은 보안 수준에 따라 Full, Medium, Light으로 분류됨

[EVITA secure 기반 보안 반도체 및 암호화 모듈의 구조 및 보안 레벨에 따른 분류]

분 류	기술적 특징	개념도
HSM Full	• 암호화 기능을 담당하는 Cryptographic 빌딩블록과 애플리케이션 코어와 연결을 위한 logic 빌딩블록 구성 • Cryptographic 빌딩 블록은 ECC-256-GF, WHIRL POOL, AES-128, AESPRNG, Counter 등으로 구성 • 추가적으로 programmable CPU, 보안 저장장치, 하드웨어 인터페이스로 구성	
HSM Medium	• 대칭 암호화 기능과 이를 위한 난수 발생 모듈, Counter로 이루어진 Cryptographic 빌딩블록과 보안 저장매체(RAM, 비휘발성 메모리)와 ARM Cortex-M3 수준의 CPU, 하드웨어 인터페이스로 구성	
HSM Light	• 통신 종단 간 보안을 유지하기 위해 사용 • 복잡한 연산이나 판단이 필요하지 않고 입력받은 정보나 들어온 명령을 수행하는 동작을 하므로 단순한 정보에 대한 암호화 처리 • AES-128과 같은 대칭 암호 엔진과 부수적으로 필요한 AES-PRNG, counter 등의 모듈 • 보안 저장매체의 경우 선택적으로 포함될 수 있으나 기본적으로는 포함 않됨	

라. 기술수준과 기술격차

☐ 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈의 국내 기술은 지속적인 기술개발이 필요한 수준으로 선도국인 미국, 독일 등 상용화 기술 레벨을 확보한 선도국과는 3년 이상의 기술격차가 있으며, 선도국 대비 국내 상대적 기술수준은 50%임

■ 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈 분야는 미국 반도체 공급부족 등으로부터 많은 어려움이 도출되고 있으며, 전량 수입에 의존하고 있는 품목 및 기술로서 보안 반도체 암호화 모듈 핵심기술 개발에 의한 국내업체의 경쟁력 향상이 시급한 상황임

☐ 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈의 국내 기술은 모바일 분야에 한정되어 있어 자동차용 보안 수준을 만족하는 고안정성의 상용화 제품개발을 위한 추가적인 기술 개발이 필요함

■ 국내 차량용 보안 반도체 기술은 중소기업 중심으로 개발되고 있으나, 추가적인 자동차 응용 분야에 적합한 다품종 보안 반도체 및 암호화 모듈 기술개발이 필요함

2. 산업·시장분석

가. 산업 동향

☐ V2X 무선통신 보안에서 가장 큰 문제는 허가되지 않은 데이터가 차량 내부 네트워크로 침투되는 것과 DDoS 등의 공격을 통해 통신자원의 가용성을 침해하는 것임

- V2X의 보안위협 요소는 무선통신망 해킹, 위장 OBU/RSU 등이 있으며 보안기술로는 V2X 메시지 인증, 암호화, 차량 PKI 등이 있음
- V2X 통신에 있어서 메시지 고속처리는 매우 중요하며 보안 관점에서는 차량 간 메시지의 서명 검증 고속화가 큰 이슈

☐ 최근 자동차 통신의 보안기능을 강화하고 제품혁신에 주력하는 솔루션 제공 업체의 투자가 증가하고 있으며, OEM 업체들은 신속한 OTA 업데이트를 통해 보안 패치를 제공하는데 주력하고 있음

- 블랙베리는 2018년 차량 간의 V2X 통신을 보호하기 위한 보안 관리 프로그램을 출시
- 차량 보안 네트워크와 소프트웨어 보안 솔루션을 제공하는 스타트업 기업의 시장 진출이 증가

☐ 현재 OBU(Onboard Unit)에는 서명키의 안전한 저장 및 안전한 서명 처리를 위해 HSM(Hardware Security Module)이 들어가 있으나 HSM은 CPU에 비해 낮은 클럭 스피드와 버스 딜레이 등의 요소로 고속 서명 검증 성능 확보에 어려움

☐ 유럽 국가의 정부는 다양한 시험 및 시험 활동을 지원하여 다양한 V2X 프로젝트에 자금을 지원하고 있으며, 향후 자동차 V2X 시장의 성장은 아시아 태평양이 2020년에 자동차 V2X의 가장 큰 시장이 될 것으로 예상

[자동화 수준에 따른 레이더 장치의 추세 및 수량]

*출처 : 라닉스 기업설명자료(2019)

❑ 실시간으로 차량간 교통정보를 공유하여 충돌사고 확률을 낮추기 위해서는 V2X 통신 모듈인 CCU(Communication Control Unit)가 필요하며, 이에 자율주행 관련 글로벌 기술시장을 주도하고 있는 선도국가(미국, 유럽, 일본, 한국 등)에서는 정책적인 프로젝트(정부-완성차-부품사 협력)를 중심으로 CCU 개발기업, 보안솔루션 개발기업, 통신 서비스 기업들이 적극적으로 시장에 나서고 있음

❑ V2X 기술시장 선도국인 미국은 2022년까지 모든 신차에 V2V통신장비를 의무화하는 규정을 발표하여 차량 내 통신의 보안 모듈에 대한 수요가 크게 증가할 것으로 예상

❑ 중국은 2016년 C-V2X를 표준으로 채택하였으며, 2018년 LTE-V2X 기술에 주파수(5.9GHz 대역, 대역폭 20MHz)를 할당했고, 2025년까지 신차 출시의 50%, 2030년에는 거의 모든 신차가 LTE-V2X 장착을 목표로 함

나. 시장 동향 및 전망

(1) 시장 성장 촉진요인 및 저해요인

□ 자동차 보안 시장은 아직 초기 단계이며, 전략적 인수, 기업 간이 파트너십 체결, 지속적인 제품혁신 및 새로운 시장진입에 의한 시장 생태계의 확대는 2025년까지 시장의 성장을 이끄는 주요 요인이 될 전망

□ 국내 자동차 관련 업체들은 세계 최고수준인 IT인프라를 바탕으로 지능형 자동차 관련 기술에서 경쟁력을 확보하기 위한 기술 발전을 지속

□ 자동차의 전장화가 높아지고 커넥티드카와 전기차의 비중이 커지면서 글로벌 IT 업체들의 시장 진출이 증가되는 위협요인이 존재

■ 중국을 비롯한 신흥국의 전기차 자체 생산이 증가되면서 기존 자동차 업체에 제공되는 물량이 축소될 수 있는 우려가 존재

[시장 성장 촉진요인 및 저해요인]

촉진요인	저해요인
• 차량의 스마트화로 생성되는 방대한 양의 데이터 증가 • 전세계적인 V2X 자동차 시장의 급속한 성장 • 세계최고 수준의 국내 IT 융합기술 • 국내 차량제작사의 해외 시장 수출 마케팅 능력 보유	• 글로벌 IT 업체들의 시장 진출 가능성 증가 • 국내 완성차업체의 의존도 높음 • 선진국 대비 핵심 원천기술 수준 낮음 • 선진국 대비 기업의 연구개발 비용 낮음
기회요인	**과 제**
• 차량 보안은 스타트업 기업의 핵심 관심 영역 • 전 세계적인 V2X 차량 강제화 정책 증가 • OEM 업체들의 차량보안 투자 증가 • 글로벌 경쟁력이 우수한 전기/전자 업체 보유	• 외부 환경과의 연결성 증가로 인한 취약성 증가 • 타 산업대비 복잡한 자동차 품질인증 절차 및 기간 • 차량보안관련 이해관계자의 복잡한 생태계 • 타 산업분야의 경쟁업체 출현 가능성 증대

(2) 세계시장 현황 및 전망

☐ MarketsandMarkets에 따르면, 세계 V2X 사이버보안 시장의 경우 2020년 6억 5,900만 달러로 추정되며, 2020-2025년 연평균 33.5%로 성장하여 2025년에는 27억 9,800만 달러에 달할 것으로 예상됨

☐ 세계 V2X 사이버보안 시장을 하드웨어 구성요소(Unit)로 한정할 경우 세계 시장규모는 2020년 8,200만 달러로 추정되며, 2020-2025년 연평균 44.6%로 성장하여 2025년에는 5억 1,700만 달러에 달할 것으로 예상됨

- V2X 사이버보안 유닛은 OBU(Onboard unit)와 RSU(Roadside uint)로 구분됨. 2020년 V2X 사이버보안 세계 시장(8,200만 달러)을 유닛별로 보면 OBU와 RSU가 각각 82.9%(6,800만 달러)와 17.1%(1,300만 달러)를 차지하고 있는 것으로 나타났음. 2020-2025년 연평균 성장률(CAGR)은 OBU 48.6%, RSU 11.4%를 예상됨

- 2025년까지 커넥티드 카의 60%는 사이버 보안 솔루션을 내장할 것으로 전망되어 시장 성장률이 매우 높을 것으로 예상됨

[V2X 사이버보안 세계 시장규모 및 전망(유닛으로 한정)]

(단위 : 백만 달러, %)

구분	'20	'21	'22	'23	'24	'25	CAGR('20~'25)
시장규모	82	118	164	236	340	517	44.6

출처 : MarketsandMarkets, "V2X CYBERSECURITY MARKET - GLOBAL FORECAST TO 2025", June 2020 자료를 토대로 재구성

(3) 국내시장 현황 및 전망

☐ 한국은 현대모비스, 현대엠엔소프트, 한국통신이 자율주행 테스트 차량 간의 5G-V2X 통신을 시연한 C-V2X를 지원했음. 한국은 또한 상용차용 V2X를 테스트한 몇 안 되는 국가 중 하나임. 교통부는 SK텔레콤, 현대자동차와 함께 HD 매핑과 V2X 지원이 가능한 자율주행 트럭과 버스 개발을 목표로 프로젝트에 착수했음.

☐ 국내 자동차 V2X 시장에서는 V2V 부문이 가장 큰 점유율을 차지할 것으로 예상됨. 이러한 성장은 자율 주행 프로그램과 5G-V2X를 가속화하기 위한 정부의 노력이 증가했기 때문일 수 있고, 이는 다시 V2X 사이버 보안 솔루션 제공업체에게 많은 기회를 줄 것으로 예상되며, 세계의 많은 보안통신에 영향을 줄 것으로 예상됨

☐ V2X 사이버보안 시장을 유닛으로 한정할 경우 국내 시장규모는 2020년 40.7억 원으로 추정되며, 2020-2025년 연평균 44.6%로 성장하여 2025년에는 256.8억 원에 달할 것으로 예상됨

- 2020년 V2X 사이버보안(유닛으로 한정) 국내 시장규모는 세계 시장규모에 한국의 자동차 생산 점유율 4.2%를 곱하고 2020년 원달러 환율을 적용하여 산출하였음

- 한국자동차산업협회에 따르면 2019년 한국의 자동차 생산량은 395만 614대로 전 세계 생산량의

4.2%를 차지

[V2X 사이버보안 국내 시장규모 및 전망(유닛으로 한정)]

(단위 : 억 원, %)

구분	'20	'21	'22	'23	'24	'25	CAGR('20~'25)
국내시장	40.7	58.6	81.5	117.2	168.9	256.8	44.6

출처 : 1) MarketsandMarkets, "V2X CYBERSECURITY MARKET – GLOBAL FORECAST TO 2025", June 2020, 2) 연평균 원달러 환율 : 1$=1,182.84원(2020년)을 토대로 TCI 재작성

다. 경쟁현황

(1) 국내 V2X 통신용 보안모듈 기업현황

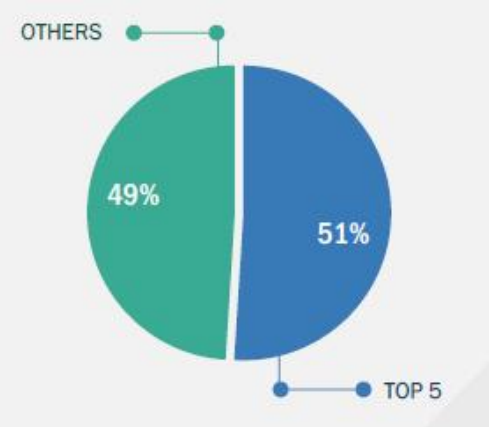
☐ 최근 국내 라닉스는 자동차 및 IoT 분야의 Total solution을 제공하기 위해 HSM기반 V2X 보안 솔루션을 시장에 선보임

- 모뎀 칩, 보안 칩, RF 칩, 소프트웨어를 통합한 V2X 통신 통합 솔루션을 개발

(2) 세계 V2X 통신용 보안모듈 기업현황

☐ 세계 V2X 사이버 보안 시장의 상위 5개 업체는 ESCRYPT(독일), OnBoard Security (미국), Autotalks(이스라엘), AutoCrypt(한국) 및 Green hHills Software(미국)임. 이들 상위 5개 기업은 2019년 세계 V2X 사이버 보안 시장의 51%를 점유하였음

[Market Share, 2019]



*출처 : MarketsandMarkets, "V2X CYBERSECURITY MARKET – GLOBAL FORECAST TO 2025", June 2020

☐ 포드는 2022년부터 출시되는 모든 신차에 LTE-V2X를 장착하겠다고 발표하였으며, 아우디는 2021년내에 아틀란타주에서 스쿨버스와 스쿨존에 대한 안전서비스를 LTE-V2X를 이용해 제공할 것이라고 발표

차량용 시스템 반도체 기술개발

- 산업통상자원부의 '차세대지능형반도체기술개발 (2020~2024)' CPU Sub-system 개발, Memory Sub-system 개발 등을 진행

가. 기술 개발 이슈

□ 유럽의 선진 자동차 관련 기업들은 자동차 보안 관련 프로젝트를 진행해오고 있으며, 그 중 대표적인 EVITA 프로젝트는 요구사항, 관련 기술 및 시큐리티 프레임워크의 하드웨어 기술인 HSM 설계에 대하여 기준 만족이 요구되고 있음

- 차량 내에서 동작하는 전장부품은 다양한 통신방식을 제공하고 있으며, 멀티미디어 데이터 통신을 위해 보다 빠르고 차량 외부 시스템과 통신할 수 있는 기술이 연구되고 있지만, 아직까지도 저사양 혹은 단순 기능을 제공하는 센서를 위해 LIN, CAN과 같은 통신 방식 역시 여전히 사용되고는 있으나 이러한 통신방식은 보안을 위한 기술 적용이 돼 있지 않으므로 추가적인 적용 개발이 필요함

- 기존 차량 네트워크 프로토콜인 CAN이나 LIN의 경우, 기본적인 구조로 인해 보안 성능을 높이기 위한 기존 기법들은 네트워크에 상당한 과부화를 유발함으로 추가적인 경량형 보안 적용 기술 개발이 필요함

- ECU의 펌웨어 추가, 업데이트 혹은 전장부품의 새로운 설정은 무결성과 신뢰성이 기반이 된 상태에서 이루어지므로 특히 무결성과 신뢰성을 가지는 보안 모듈의 중요성이 부각되고 있음

- 특정 중요 정보를 다루는 동작들은 무결성과 신뢰성이 기반이 된 상태에서 이루어져야 하며, 보안이 신뢰할 수 있는 연산 영역이 존재하여 외부침입에 의한 연산 오류로부터 보호돼야 함으로 이에 대한 기술 개발이 필요함

- 차량의 보안 기능은 자동차 동작 기능 및 정보들에 접근이 통제돼야 하며, 혹시라도 침입에 의해 설정이 조작되더라도 소프트웨어가 오동작을 일으키지 않을 수 있도록 보안 기술 개발이 필요함

□ EVITA에서 설계한 시큐리티 프레임워크는 구성을 위한 기술을 네트워크 보안 기술과 호스트 기반의 보안 기술을 포함하므로 이에 대한 기술확보가 모두 필요함

- 네트워크 보안 기술로는 보안을 위한 통신 프로토콜 기술과 네트워크상에서 연결을 위한 자원에서 구현되는 보안 기술이 있으며, 이러한 기술들은 네트워크의 구성에 따라 보안 영역이 결정되고 각 호스트의 보안을 공유함으로 관련 기술 확보가 필요함

- 호스트 기반의 보안 기술로서, 네트워크를 구성하는 두 호스트 간에 데이터를 송수신 할 때, 보내는 쪽에서는 암호화하고 중간의 전송 과정에서는 아무 조건이 없이 전송하나, 최종적으로 이를 수신하는 측에서만 복호화 하는 방식인 데이터 암호화 기술은 각 호스트에서 사용하게 되는 보안기술 중 핵심 기술로서 기술 확보가 필요함

□ 차량 보안 시큐리티 프레임워크를 설계할 때 기밀 유지나 연산의 신뢰성, 성능에 대한 요구사항을 만족시키기 위해 다양한 보안 기술이 필요

- Trusted Computing, Cryptographic Hardware, Smartcards, Tamper Protection, Physically Unclonable Functions 등의 하드웨어로 구현되는 기술들이 필요

- EVITA에서 정의하는 HSM(Hardware Secure Module)에서는 Trusted Computing과 Cryptographic Hardware 기능을 제공

- Trusted Platform Module은 기능 동작을 위해 필요한 연산을 보안이 유지되는 곳에서 수행하는 것을 의미하며 하드웨어 기반의 난수 발생, 암호화 엔진, 해시 함수 엔진, 보안저장매체(ROM, RAM, EEPROM)에 대한 각각의 세부 기술 개발이 필요함

나. 핵심 플레이어 동향

(1) 해외 플레이어 동향

☐ ESCRYPT

- 에스크립트(ESCRYPT)는 기술 및 서비스 분야의 글로벌 선도 기업인 보쉬(BOSCH)의 전액 출자 자회사인 이타스의 자회사이며 임베디드 보안 분야의 선도 기업
- 자동차 사이버보안 부문에서의 전문성과 신뢰를 쌓으며 전 세계 자동차 사이버보안 시장을 선도함
- 현재 자동차 보안 및 자동차 제조 응용 분야에서 수백만 개의 제어기에 에스크립트 솔루션이 사용됨
- 에스크립트는 HSM 펌웨어 아키텍처와 모듈을 통해 HSM을 사용하기 위한 환경을 제공하며, 이는 간단한 암호화 작업, SHE/SHE+ 기능의 에뮬레이션, 보안 ECU 부팅에서부터 백그라운드에서 실행되는 복잡한 인증서 관리 또는 소프트웨어 조작 및 변조 탐지가 가능함
- 에스크립트의 HSM(하드웨어 모듈 기술) 및 CycurHSM 소프트웨어는 온보드 통신, 실시간 조작 감지, 시큐어 부팅 등 차량 사이버보안을 보장하는 솔루션을 제공함
- 컴퓨팅(Trusted Computing), 가상화(Virtualization), 보안 운영 체제(Secure Operating Systems), 무선 인터넷 네트워크(Wireless Sensor Networks), 차량 간 통신(Car-to-Car Communication), 임베디드 보안(Embedded Security) 등에 대한 핵심 기술 보유
- HSM은 자체 프로세서 코어를 사용하여 차량 유스케이스에 필요한 보안 기능을 제공하며, 128 비트 AES 하드웨어 가속기, 암호화 키 요소 생성을 위한 진난수생성기(TRNG, True Random Number Generator), 암호화 키의 하드웨어 보호 저장장치, 플래시 및 디버깅 기능, 시스템 메모리와 분리된 HSM 자체 RAM 등이 포함됨
- 미래의 커텍티드 카와 자율주행 기술에 대한 보안은 핵심 기술 중에 하나로서침입 탐지 시스템, 차량 방화벽, OTA(over-the-air) 소프트웨어 업데이트 보안 및 V2X 보안 등 첨단기술을 결합하여 커넥티드 환경의 모든 핵심 요소를 보호할 수 있도록 기술개발 중

☐ Elektrobit Automotive

- 일렉트로비트(Elektrobit)는 세계적인 임베디드 및 커넥티드 소프트웨어 및 보안 솔루션 서비스 공급자
- 운전자 지원 시스템, 무선 소프트웨어 업데이트(SOTA), 자율 주행 기능 등 자동차의 새로운 기능을 위해서는 ECU(electronic control unit)가 필요하며, 이들 ECU는 서로 연결되고 클라우드와 연결되므로 일렉트로비트 오토모티브(Elektrobit Automotive)는 자동차 사이버 보안 문제를 해결하기 위해서 인피니언과 같은 반도체 회사들과 긴밀하게 협력
- 인피니언과 협력한 HSM은 하드웨어 기반 대칭 및 비대칭 암호화 알고리즘과 해쉬 기능(AES-128, ECC 256, SHA2)을 사용하여, 무단조작에 대한 보호 및 속도를 크게 향상시킬수 있어 하드웨어 지원으로 순수 소프트웨어 솔루션 대비 해쉬 계산(SHA256) 속도가 상대적으로 향상됨
- HSM에 최적화된 일렉트로비트의 소프트웨어 스택을 사용함으로써 1MB의 데이터를 16.2ms에 검사가 가능함

(2) 국내 플레이어 동향

☐ FESCARO

- 페스카로는 차량 제어기 레벨, 차량 내부 네트워크 레벨, 차량 외부 네트워크 레벨의 End-To-End 통합 보안 솔루션을 제공함
- 사이버 해킹 공격으로부터 자율주행차, 커넥티드 카를 보호하는 솔루션을 보유하고 있으며, 글로벌 OEM의 양산차에 그들의 솔루션을 적용하기 위한 협업 프로젝트를 진행
- 페스카로는 자동차, 안전, 보안을 종합적으로 고려해 안전성, 가용성, 심층적 방어 전략을 기반으로 자동차에 전문화된 보안 솔루션을 개발
- 제어기 자체를 보호하는 HSM 기반의 솔루션, 제어기 간 통신을 실시간 침입탐지 및 차단하는 IDPS 솔루션, 커넥티드 환경에서 무선 펌웨어 업데이트(Firmware Over The Air, FOTA) 관리, 신규 룰셋 업데이트, 다양한 엔드포인트들로부터의 정보 수집을 통한 통합 보안 인텔리전스 솔루션을 제공
- SAE J3061 자동차 사이버 보안 공학을 준수하며 설계 단계에서 보안 위협 식별 및 위험 평가를 통해 도출된 요구사항을 바탕으로 체계적인 보안
- HSM 기반 ECU 보안 플랫폼 관련하여 페스카로는 FAST Platform을 통해 E/E 아키텍처 전체 솔루션 설계가 가능하며, 또한 AUTOSAR를 준수하여 타사 제품과 호환이 가능

☐ 아우토크립트(쾐타시큐리티)

- 쾐타시큐리티로부터 분사한 AUTOCRYPT(아우토크립트)는 IEEE 1609.2 및 미국의 CAMP VSC3(Crash Avoidance Metrics Partnership - Vehicle Safety Communications 3) 규격 등의 국제 표준 기술에 따라 개발
- 아우토크립트 보안 솔루션은 차량용 인증시스템뿐만 아니라, 외부에서 차량으로 유입되는 해킹 공격을 어플리케이션 레벨에서 탐지하는 차량용 방화벽, 차량 내/외부에서 암호 키를 생성, 관리하기 위한 차량용 키관리시스템(KMS; Key Management System) 등을 포함함
- 아우토크립트(주)는 자율주행보안, 전기차/ 충전인프라 보안, 디지털키 솔루션, 차량 내부 보안, FMS(Fleet Management System, 차량 데이터 관제 서비스)를 제공하고 있으며, 자동차 사이버 보안 법규제도인 WP.29에 부합하는 컨설팅 서비스도 제공함

☐ 한컴MDS

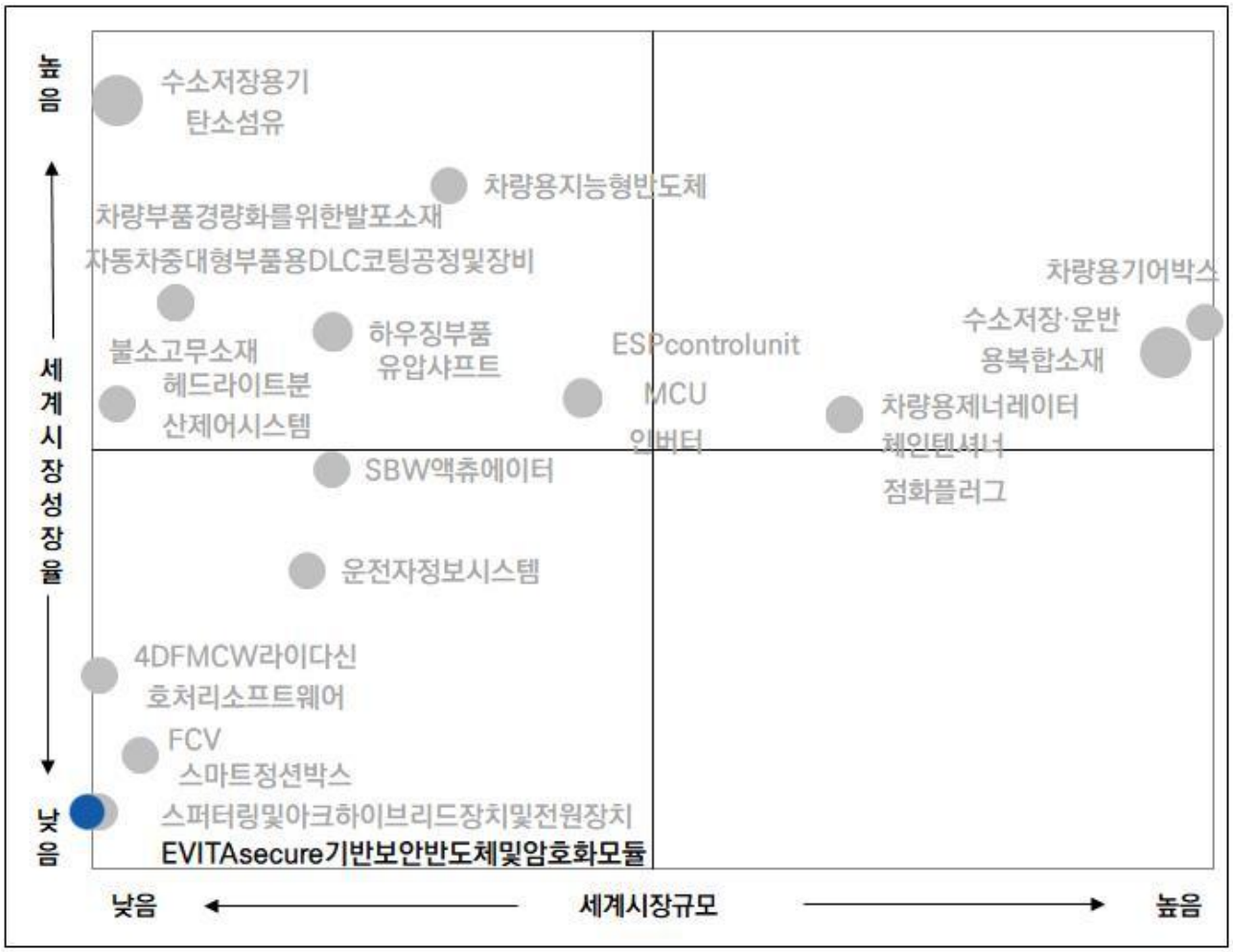
- 한컴MDS사의 HSM S/W는 HSM H/W 상에서 동작하는 보안 소프트웨어로서, HSM H/W의 자원을 이용하여 AUTOSAR 플랫폼에 다양한 암호화 관련 기능을 제공
- HSM S/W는 framework의 형태로 구현되며, AUTOSAR 플랫폼은 framework에서 제공하는 API를 호출하여 HSM S/W의 기능을 사용
- HSM에서는 최초 공장에서 제어기에 이식된 직후 제어기에 탑재된 mobilgene 플랫폼에 대해서 일정의 스냅샷을 만들어 HSM 내부의 보안 적용된 저장소에 저장, 이후 제어기에 전원이 들어와 부팅이 시작되면, HSM은 저장된 스냅샷과 현재 제어기의 mobilgene 플랫폼을 비교하여 mobilgene 플랫폼의 위/변조 여부를 판단할 수 있는 기능 내장

4. 공급망 분석

가. 시장 매력도

☐ EVITA secure 기반 보안 반도체 및 암호화 모듈은 세계시장규모도 작고 세계시장성장율이 낮아 시장 매력도가 매우 낮은 품목으로 나타남

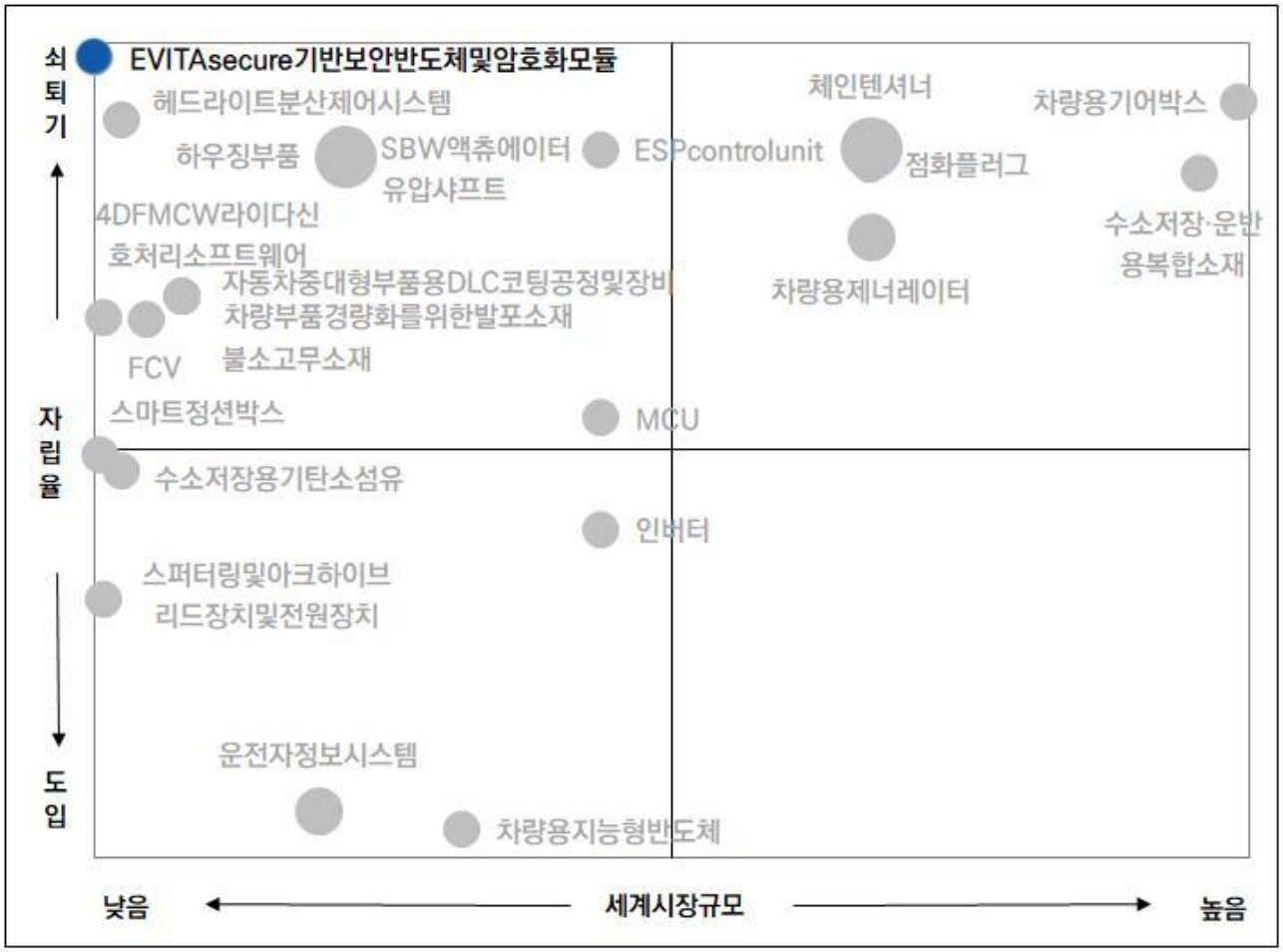
(원크기 : 수익률)



나. 생산 공백 정도

☐ EVITA secure 기반 보안 반도체 및 암호화 모듈은 세계시장규모가 매우 작은 반면 자립율이 높게 나타나 생산 공백이 없는 것으로 나타남

(원크기 : 종사자수)

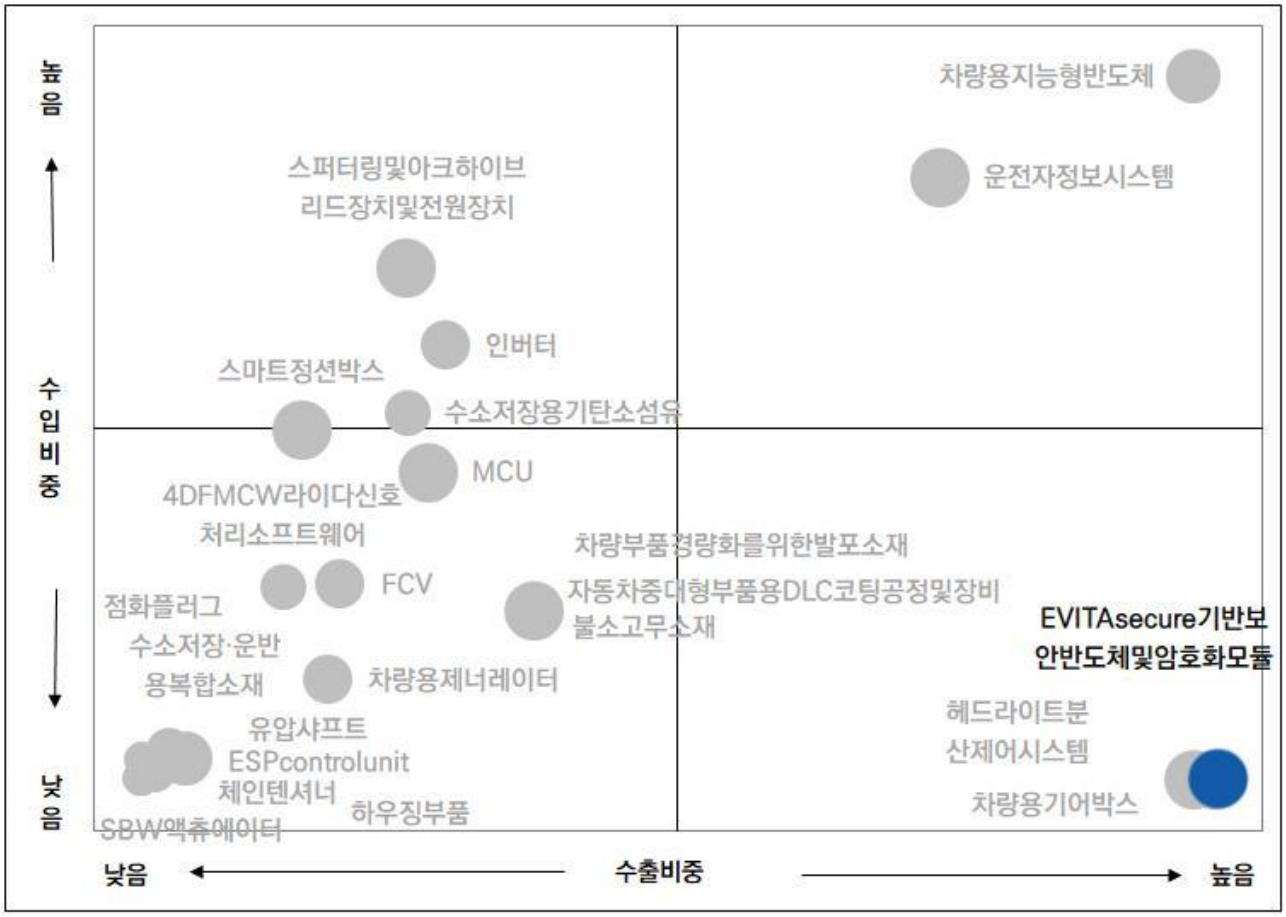


주 : 자립율 : 1-수입비중

다. 해외 지향성

☐ EVITA secure 기반 보안 반도체 및 암호화 모듈은 수출비중이 높고 수입비중이 낮아 수입보다는 수출 위주의 품목으로 나타남

(원크기 : 수출액)

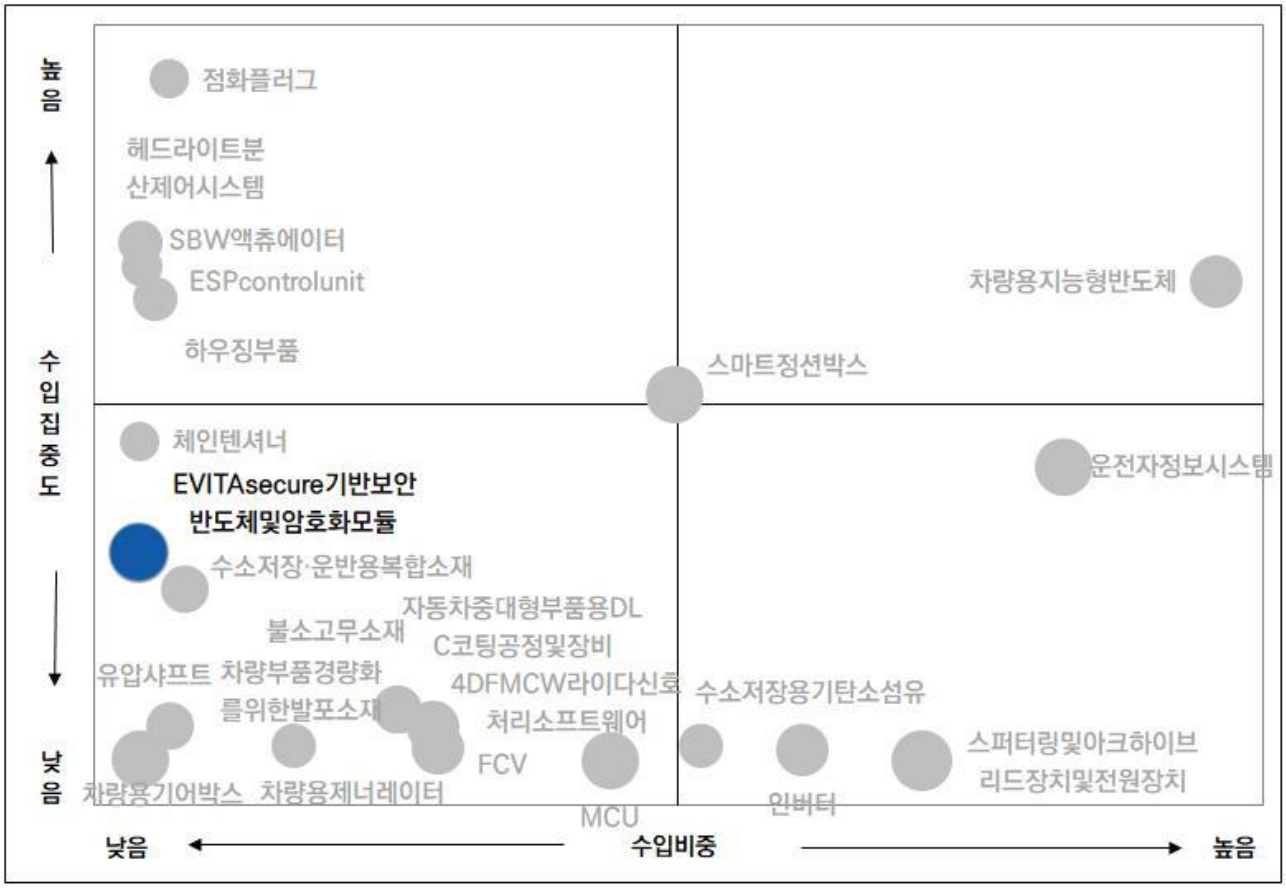


주 : (1) 수출비중 = 수출액/생산액주 (2) 수입비중 = 수입액/내수액

라. 수입 리스크

☐ EVITA secure 기반 보안 반도체 및 암호화 모듈은 수입비중이 낮고 수입 집중도도 낮게 나타나 수입 리스크가 크지 않은 품목으로 나타남

(원크기 : 수입액)

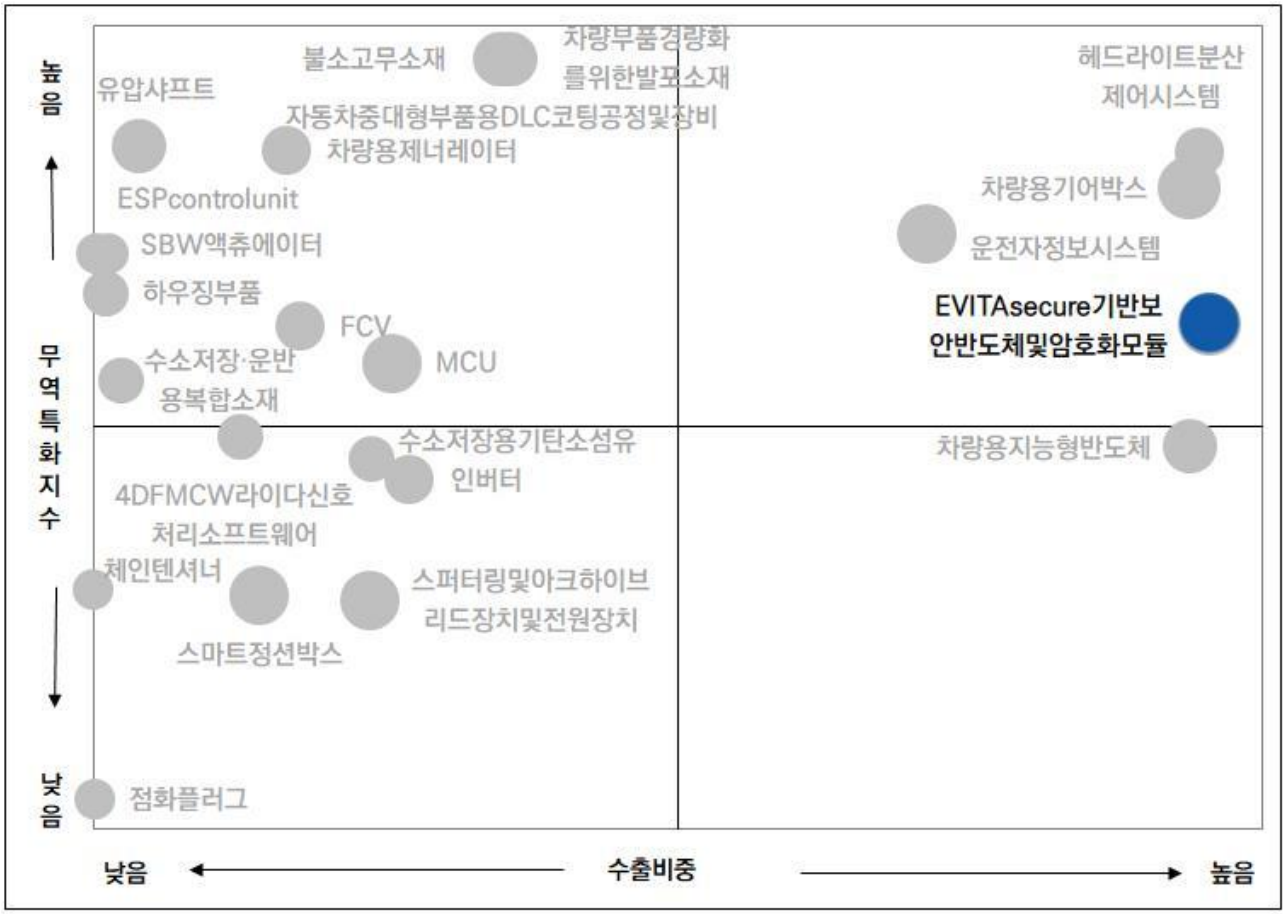


주 : 수입집중도(HHI지수) = (제1수입국 수입비중)² + (제2수입국 수입비중)² + (제3수입국 수입비중)²

마. 수출산업화

☐ EVITA secure 기반 보안 반도체 및 암호화 모듈은 수출비중이 높고 무역특화지수가 높아 수출산업화 잠재력이 큰 품목으로 나타남

(원크기 : 수출액)



주 : 무역특화지수 = (수출액-수입액) / (수출액 + 수입액)

5. 주요 플레이어 특허동향[1)]

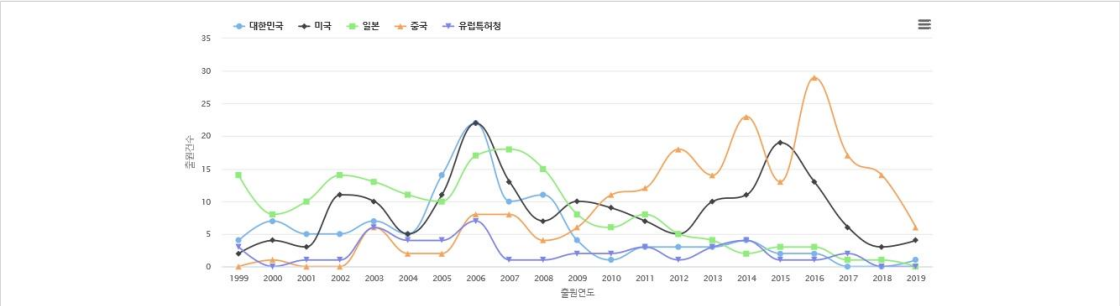
가. 동향 분석

(1) 출원 동향

☐ 연도별 국가별 출원 동향

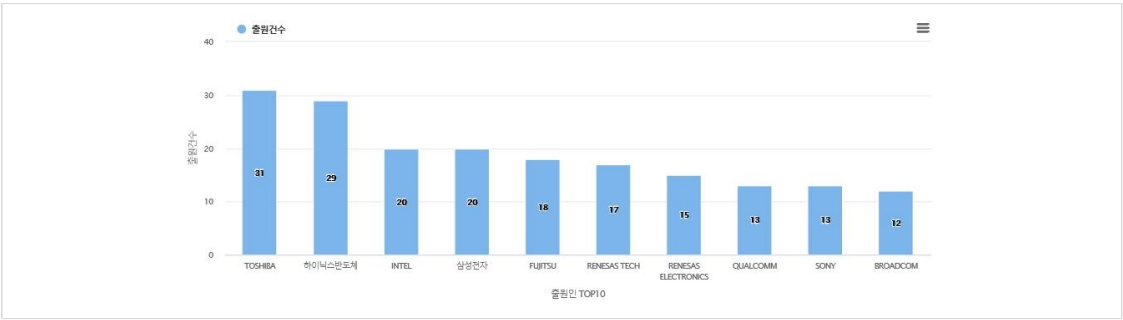
■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에 대해 1999~2019년 동안 주요 5개 국가(대한민국, 미국, 일본, 중국, 유럽)에서 출원된 특허 710건의 연도별 출원 건수를 통해 해당 품목의 특허 출원 동향을 파악한 결과, 연도별로 상기 5개 국가들의 출원 건수를 통해 국가별 최근 출원 동향을 파악함으로써 향후 기술개발 경향 및 시장 전망을 예측함

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에 있어서, 한국, 일본 및 유럽의 특허 출원은 최근 5년 사이에 감소하는 현상을 보이고 있는 것으로 파악되며, 특히 중국은 2010년, 미국은 2013년을 기점으로 특허 출원건수가 타국가 대비 증가하고 있는 양상을 나타내고 있음



☐ 주요 출원인 동향

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에서의 선도 기업(기관)을 파악하고 이들 기업(기관)의 특허 출원 현황을 비교, 분석하여 EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야의 상위 10개 출원인을 살펴본 결과, 일본의 TOSHIBA가 31건을 출원하여 동 기술 분야에서 최다출원인으로 파악됨. 한국의 하이닉스반도체, 미국의 INTEL, 한국의 삼성전자, 일본의 FUJITSU 등이 TOP 5를 형성하고 있는 것으로 확인됨

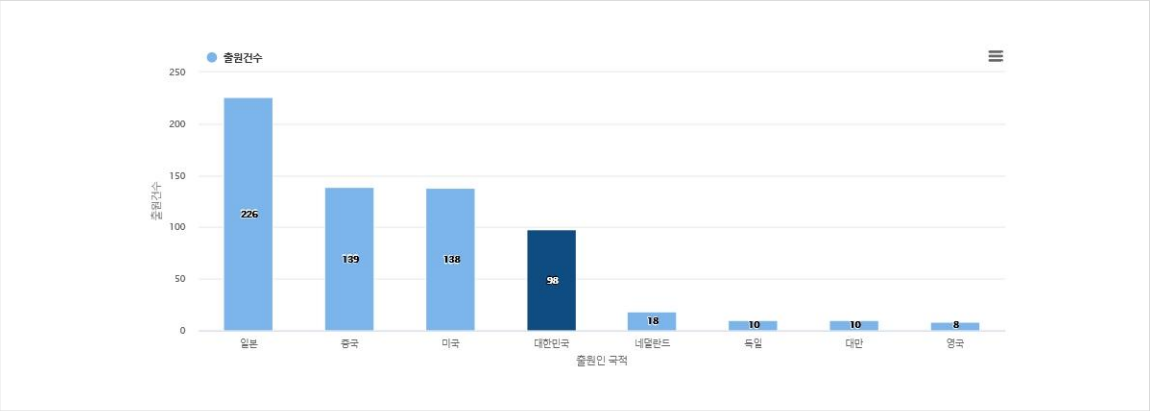


1) 자료 출처 : 특허빅데이터센터(KPBCenter), https://pbcenter.re.kr/home/p/analysis-field

(2) 국가별 세부 동향

☐ 국가별 특허 점유율 동향

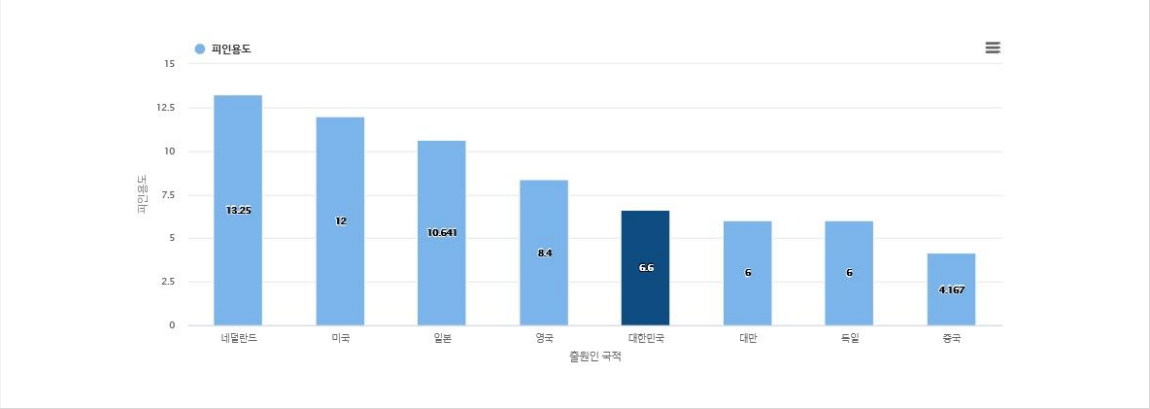
■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야 특허 출원인의 국가별 양적 점유율을 분석하여, 특허 출원 선도국을 확인하고, 선도국 대비 한국 국적 출원인의 특허 점유율을 분석하여 양적인 경쟁력을 파악한 결과, EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야는 일본이 총 226건(33.2%)의 특허를 출원하여, 가장 높은 점유율을 차지하고 있고, 그 뒤를 이어 중국이 139건(20.4%), 미국이 138건(20.3%), 한국 98건(14.4%)의 특허를 출원한 것으로 나타나, 동 기술 분야는 일본이 선도하고 있는 것으로 파악되었고, 중국, 미국 및 한국 역시 다수의 특허를 출원하고 있는 것으로 확인됨



☐ 국가별 피인용지수

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야 특허 출원인의 국가별 피인용도 분석을 통해, 영향력이 높은 특허를 출원한 선도국을 확인하고, 선도국 대비 한국 국적 출원인의 특허 피인용도 분석을 통해 질적인 경쟁력을 해석함

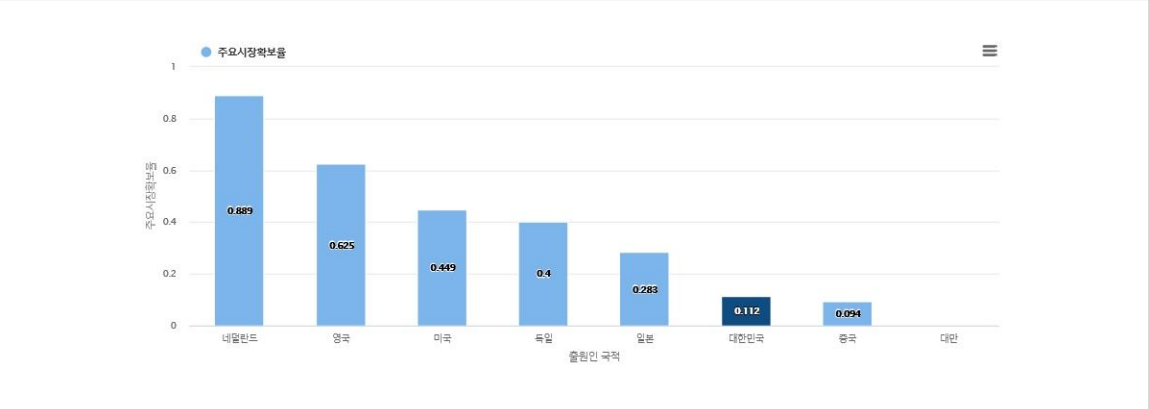
■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야의 국가별 피인용 지수를 살펴보면, 네덜란드 13.25로 특허 파급력 및 영향력이 가장 높은 것으로 파악되었고, 그 뒤를 이어 미국(12), 일본(10.641) 등으로 파악됨. 한국은 피인용지수가 6.6인 것으로 나타나 타 국가 대비 특허의 질적 경쟁력이 중간 정도 수준인 것으로 판단됨



▢ 국가별 주요시장 확보율

- EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에 있어서, 특허 출원인의 국가별로 주요 특허청(한국, 일본, 미국, 유럽, 중국) 중 3개 이상의 특허청에 동시 출원한 특허 비율을 분석하여, 주요시장 확보율이 가장 높은 선도국을 확인하고, 선도국 대비 한국 국적 출원인의 주요시장 확보율 분석을 통해 해당 품목의 국가별 시장영향력(또는 주요 시장 선점 의지)을 파악함

- EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에 있어서, 네덜란드가 해외 시장 진출을 위한 권리 확보를 위해 가장 활발하게 여러 국가에 동시 출원하고 있고, 그 다음으로 영국, 미국, 독일, 일본의 순으로 나타남. 반면, 한국은 주요시장 확보율이 0.112로 나타남에 따라, 해외 시장 진출 보다는 자국 내 특허 출원에 집중하고 있는 것으로 파악됨

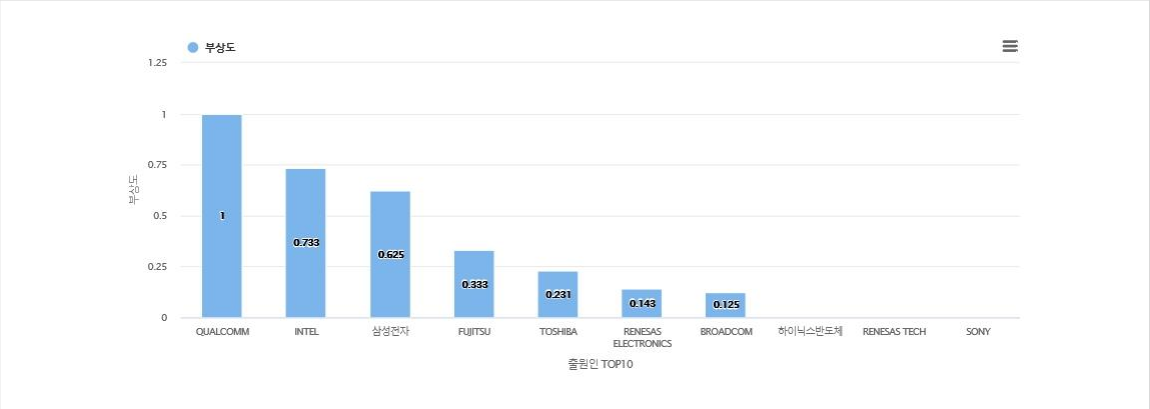


나. 심층 분석 – 주요 출원인 IP 경쟁력 관점 분석

(1) 주요 출원인 기술부상도

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야 상위 10개 주요 출원인들의 최근 5년간 특허 출원 건수를 기준으로 출원 증가율 변화를 통해 기술부상도를 산출하여 양적인 경쟁력 수준을 파악함

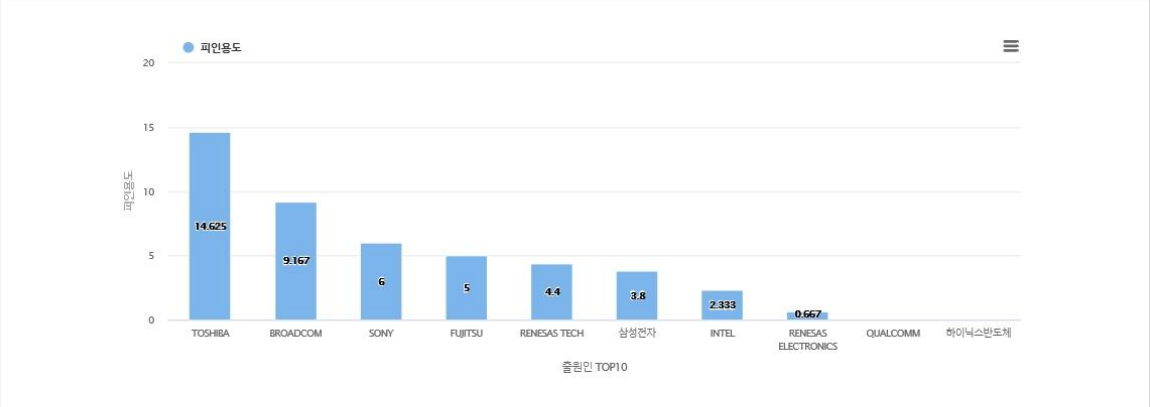
■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야의 최근 기술부상도를 살펴보면, 미국의 QUALCOMM이 1, INTEL 0.733, 한국의 삼성전자 0.625의 순으로 기술부상도가 높은 것으로 파악됨. 반면, 한국 국적의 하이닉스반도체는 0의 기술부상도를 가지고 있는 것으로 파악됨



(2) 주요 출원인 피인용지수

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야 상위 10개 주요 출원인들이 보유한 특허의 피인용 건수를 기반으로 피인용지수를 산출하여 주요 출원인들의 보유 특허에 대한 질적 경쟁력 수준을 파악함

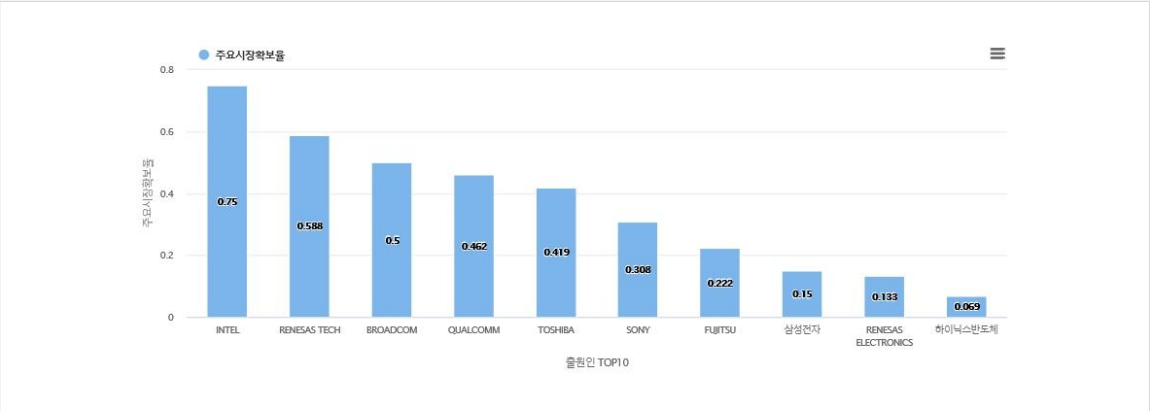
■ 일본의 TOSHIBA가 14.625로 가장 높은 피인용지수를 나타내어 특허의 질적 수준이 가장 높은 것으로 파악되었고, 그 뒤를 미국의 BROADCOM 9.167, 일본의 SONY 6, FUJITSU 5로 나타나 특허의 질적 수준이 타 기업에 비하여 상대적으로 높은 것으로 파악됨, 반면, 한국의 출원인들은 삼성전자가 3.8로 중하위권 수준, 하이닉스반도체는 0의 피인용 지수를 가지고 있어서 최하위권인 것으로 파악됨



(3) 주요 출원인별 주요시장 확보율

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야 상위 10개 주요 출원인별로 주요 특허청 중 3개 이상의 특허청에 동시 출원한 특허 비율)을 분석하여 주요 출원인들의 주요시장 진출 수준을 파악함으로써 기업(기관)의 영향력 및 해외 시장 진입을 위한 특허 활동량을 파악함

■ EVITA/UNECE secure 기반 보안 반도체 및 암호화 모듈 기술 분야에 있어서, 미국의 INTEL 0.75, 일본의 RENESAS TECH 0.588, 미국의 BROADCOM 0.5, QUALCOMM 0.462, 일본의 TOSHIBA 0.419의 주요시장 확보율을 나타내어 해외 시장 진입을 위하여 가장 활발하게 특허 활동을 펼치고 있는 것으로 파악됨. 한편, 한국이 삼성전자 0.15, 하이닉스반도체 0.069의 주요 시장 확보율을 가진 것으로 나타나 타 출원인에 비하여 상대적으로 국내 특허 출원 비중이 더 높은 것으로 파악됨



6. 전략제품 기술 개발 전략

가. 중소기업 기술 개발 전략

☐ 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈은 자동차 보안 레벨을 만족하는 기술을 개발하여 각각의 전장 모듈에 내재화 되어 보안 대응이 가능하도록 기술 개발

☐ 커넥티드카에 적용될 수 있도록 커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈의 높은 보안 수준을 확보할 수 있도록 기술 개발

☐ 커넥티드카에서의 다양한 외부 애플리케이션에 보안 기능을 사용할 수 있고 새로운 암호 알고리즘이나 동작에 대한 업데이트(OTA)가 용이하며, EVITA의 요구사항을 만족하는 HSM 기술 개발

나. 핵심기술 리스트

[커넥티드카용 EVITA secure 기반 보안 반도체 및 암호화 모듈 분야 핵심기술]

핵심기술	개요
Integration HSM (HSM 칩과 주 CPU의 통합)	• HSM이 상태 기계(state machine)에 따라 동작할 수 있는 기술 • 암호 알고리즘이나 업데이트 등이 가능한 HSM 기술 • HSM에 programmable CPU가 적용돼 있어서 암호화 기능에 대해 다양한 구현이 가능
Secure Island Module (HSM 칩과 주 CPU의 독립적 구성 기술)	• HSM과 주 CPU가 다른 칩으로 구성돼 있어서 추가적인 핀이 필요 • 낮은 안전성 및 두 연결 핀에서의 취약한 해킹에 대한 대응 기술 • 사용기간이 짧은 전장부품이나 보안 요구도가 낮은 애플리케이션을 구동에 적합한 기술