



산업통상자원부

---

– 산업혁신인재성장지원사업(R&D) –  
**「미래차보안시스템 전문인력양성」**  
**2023년도 시행계획(안)**

---

**2023. 1.**

**제 조 산 업 정 책 관**  
**미 래 자 동 차 산 업 과**

# 목 차

I. 추진 배경 .....	1
II. 사업 개요 .....	2
1. 사업목적 .....	2
2. 사업개요 .....	5
3. 사업 추진체계 .....	6
4. 추진목표 및 내용 .....	7
III. 세부 추진계획 .....	8
1. 석·박사 교육과정 개발·운영 .....	8
2. 산업계 수요를 반영한 산학 프로젝트 및 전문 교육과정 운영 ....	8
3. 산학협력 체계 구축 및 성과 확산 .....	9
IV. 근거법령 및 규정 .....	10
V. 추진일정 .....	11

# I . 추진 배경

□ (미래차 보안시스템) 미래차 취약점을 파악하여 적절한 보안기술을 개발·적용하여 자동차와 운전자, 보행자 등의 안전을 지키는 시스템

- 미래차 보안시스템의 핵심기술 분야는 ① AI 보안, ② SW 보안, ③ 네트워크 보안, ④ 클라우드 보안으로 구분

< 미래차 보안시스템 핵심기술 분야 >

핵심기술 분야	세부 기술
① AI 보안	AI 시스템 보안, 자율주행차 보안 기술, AI 모델 보안 기술 등
② SW 보안	ADAS, 텔레매틱스 소프트웨어를 위한 취약점 분석기술, 보안 이행기술, 점검 기술 등
③ 네트워크 보안	ECU 간 통신 보안 기술, WAVE 기반 V2X 보안 기술, V2P 보안 기술 등
④ 클라우드 보안	차량용 보안 프로토콜, 엣지 컴퓨팅 보안, 원격 보안 업데이트(OTA 등), 데이터 보안 등

□ (산업/시장동향) 차량 커넥트화로 인해 사이버보안 위험성이 증대 되는 추세이나, 시장은 초기단계로 관련 수요가 급증할 것으로 전망

< 미래차 보안 시장 국내·외 시장 규모 >

연도	2020	2021	2022	2023	2024
국내 (억원)	115	137	162	191	226
해외 (백만달러)	1,850	2,155	2,510	2,925	3,407

\* (산출근거) 융합보안산업 시장전망 및 경쟁력 방안 연구(한국정보산업협회, 2016 발췌), Markets and Makets(2020, 추정 계상)

- (국내) 자동차 보안의 중요성이 부각되면서 보안의 일부 영역에서 탈피하여 독립적인 분야로 인정되면서 시장규모가 급속히 팽창
  - (AI 보안) 보안관계 정보 수집·분석·공유 기술 및 AI 기반 보안 관계 플랫폼 기술개발 등의 핵심기술 개발 중
  - (SW 보안) 소프트웨어 취약점 자동 패치(Hardening) 기술을 구현 하는 바이너리 코드(Binary Code) 분석기술을 중심으로 연구 중
  - (네트워크 보안) 방화벽, IDS 등 기술이 개발되어 일부 적용 중 이며 규칙(Rule) 및 화이트리스트 기반의 탐지 기술이 주류로 운영
    - \* (사례) 펜타시큐리티, 페스카로 등에서 차량용 방화벽 기술 개발
  - (클라우드 분야) 운행정보 및 주행거리, 차량 상태 등 각종 자료를 수집 중이며 향후 다양한 형태의 보안 공격 증가 예상

- (해외) 세계 자동차 사이버보안 시장 중 소프트웨어 분야는 '20년 14.6억만 달러에서 연평균 성장률 16.9%로 증가할 것으로 전망
  - (AI 보안) 자율주행에 필요한 AI 시스템을 해킹하여 데이터를 파괴·조작시켜 안전에 큰 영향을 끼칠 수 있어 방어기법 마련 중
  - (SW 보안) 자동차 성능 향상을 위한 ECU SW·FW 업데이트를 위해 암호화, 서명 등의 다양한 보안 기법이 적용된 제품 출시 중
    - \* 자동차 ECU의 원격 업데이트를 위한 보안 표준규격(x.1373) 제정 (ITU-T, 2017)
  - (네트워크 보안) 글로벌 기업이 다양한 보안 기법을 적용하기 위해 보안취약점 분석에 적극적으로 예산 및 인력 투입 중
  - (클라우드 분야) 클라우드 장애로 자율주행 서비스들에 오류가 발생할 수 있어 클라우드 보안, 데이터 백업 등 상용 서비스 추진
    - \* 세계 최초의 커넥티드카의 사이버보안 서비스플랫폼인 'Secure IoT' 발표(Trillium, 2018)

□ (인력현황) 미래차 보안 관련 정부의 집중적인 투자 및 글로벌 기준 대응을 위해 석·박사급 전문인력 양성 및 공급이 필요

- (정부정책) 5G-V2X 기반 커넥티드형 미래차 관련한 자율주행 기술에 대해 집중적인 투자 계획 발표 및 관련 전문인력 요구
  - 핵심산업 집중 육성을 통한 성장동력을 확충하기 위해 미래차 등 차세대 핵심기술 확보 및 전문인력 양성 지원 강화
    - \* 2030 미래차 산업 발전전략('19.10), 미래차 산업 경쟁력 강화를 위한 디지털 전환 고도화 추진전략('22.1) 등
- (인력수급) 미래차 보안기술 관련 핵심기술 확보 및 글로벌 차량 규제 시스템 대응 등을 위해 석·박사 전문인력 필요
  - 미래차 보안기술을 공유하는 IoT, 스마트·친환경선박, 항공·드론 분야를 합치면 10년간 약 13.8만명 부족할 것으로 예상

구분 (명)	미래형 자동차	IoT 가전	디지털 헬스케어	스마트·친환경선박	항공·드론	합계
2020년	72,326	68,831	49,253	44,737	7,340	242,487
2030년	107,551	108,965	78,279	74,162	11,128	380,085

\* (근거) 유망신산업 산업기술인력 전망 (산업통상자원부)

미래차 보안 시스템 산업을 선도하기 위한  
현장기술 중심의 석·박사 전문인력 양성 필요

## II. 사업 개요

### 1 사업목적

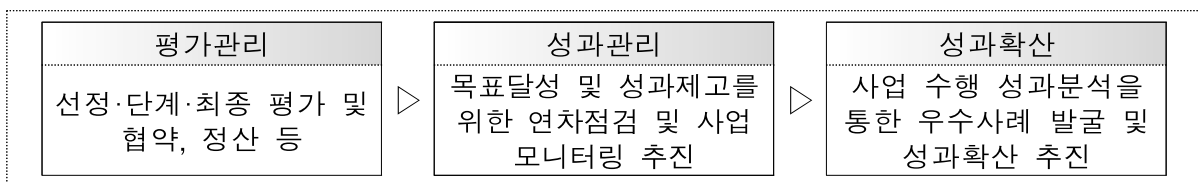
- 미래차 보안 시스템 산업을 선도할 현장기술 중심의 석·박사 전문인력 양성
  - ①AI 보안, ②SW 보안, ③네트워크 보안, ④클라우드 보안으로 구분하여 기술그룹별로 특화 또는 연계 운영하여 시너지 창출

### 2 지원개요

- (사업기간) '23. 3. 1. ~ '28. 2. 28. (최대 60개월, 2+2+1년)
  - \* 1, 2단계 평가 결과에 따라 지원규모 조정 또는 지원 중단 가능
- (사업예산) '23년 정부출연금 10억원
  - \* 정부지원연구개발비 대비 20%이상 기관부담연구개발비 매칭 (정부지원연구개발비의 10%이상은 기관현금 매칭)
- (지원내용) 인건비(학생인건비 포함), 산학 프로젝트 운영비, 교육과정 개발·운영비, 전문가 활용비 등
  - \* 연구개발비 편성의 적정성은 평가위원회를 통해 조정 가능

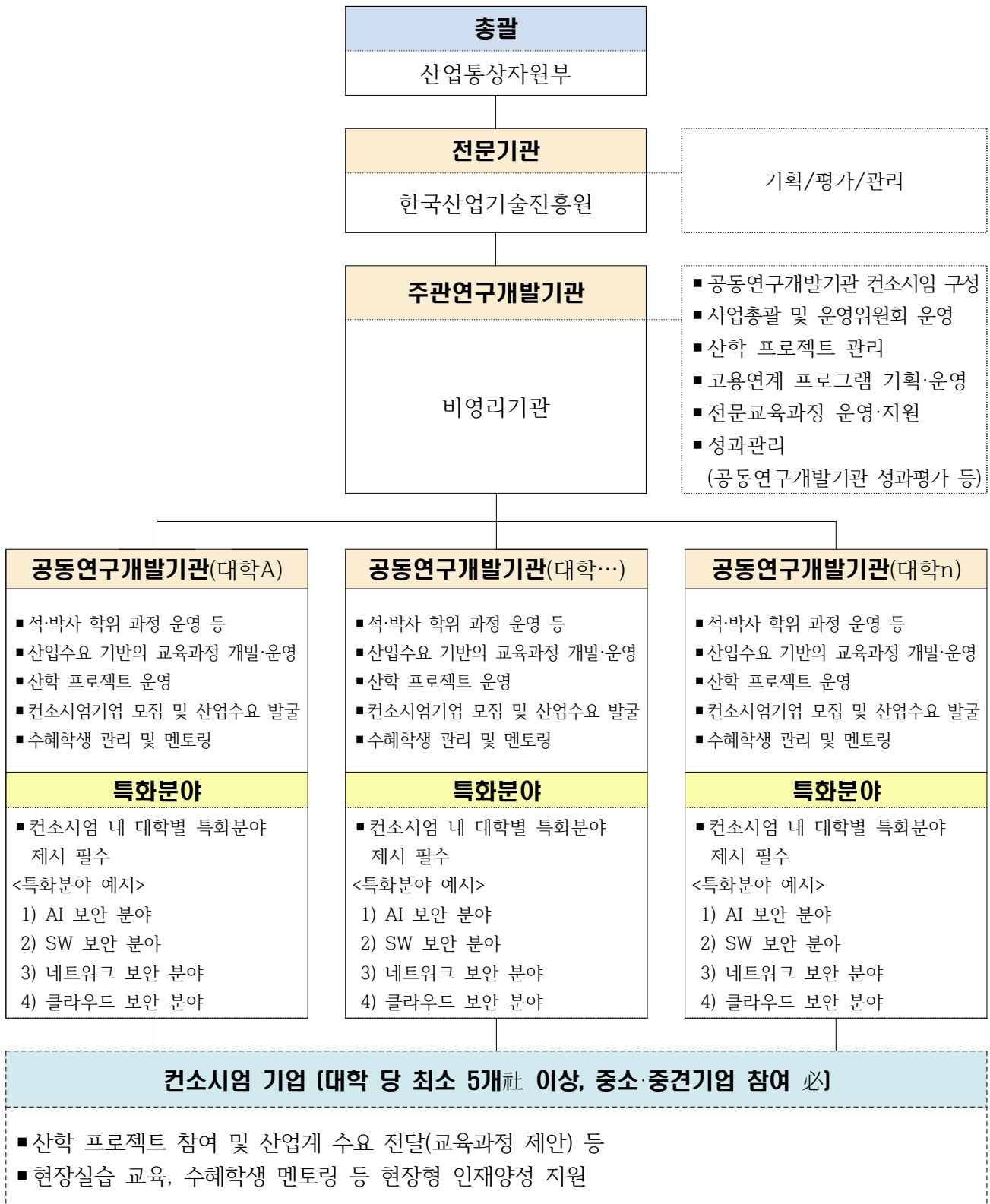
### 3 사업 추진체계

- (전문기관) 한국산업기술진흥원
  - \* (역할) 주관연구개발기관 선정·평가관리, 사업총괄관리 등



- (지원대상) 1개 비영리기관 컨소시엄(주관 및 공동 연구개발기관 구성)
  - (주관연구개발기관) 비영리기관(대학, 연구소, 협회·단체 등)
  - (공동연구개발기관) 미래차 보안 시스템 분야 관련 대학원을 운영 (또는 계획) 중인 4년제 대학 등(2개 이상 참여)
- (기업참여) 산업계 수요를 반영하기 위한 미래차 보안 시스템 분야 컨소시엄 기업\* 참여 必 (대학 당 최소 5개社 이상)
  - \* 전문기관과 별도 협약 없이(연구개발비 미지원), 참여의사 확인서를 통해 사업에 참여

**< 미래차 보안 시스템 전문인력양성 추진체계(안) >**



\* 주관연구개발기관은 공동연구개발기관 및 외부전문가 등으로 총괄운영위원회를 구성하여 사업추진 전반에 활용(10인 내외, 컨소시엄 기업 소속전문가 참여 등)

\*\* 컨소시엄은 "1개 주관연구개발기관 + N개 공동연구개발기관" 형태로 자율 구성 하되, 인재양성을 위한 대학 최소 N개 이상 참여 必

#### 4 추진목표 및 내용

<p style="text-align: center;"><b>&lt; 사업목표 &gt;</b></p> <p style="text-align: center;"><b>미래차 보안 시스템 산업을 선도할 현장기술 중심의 석·박사 전문인력 양성</b></p>	
---	--

<b>추진 내용</b>	<p><b>① 석·박사 교육과정 개발·운영</b></p> <ul style="list-style-type: none"> <li>○ 미래차 보안 시스템 분야 석·박사(전일제) 연간 신규 15명 양성 (대학당 최소 5명 이상)</li> <li>○ 산업계 수요를 반영한 특화분야 교육과정 개발·운영</li> <li>* ①AI 보안, ②SW 보안, ③네트워크 보안, ④클라우드 보안</li> </ul>
	<p><b>② 산업계 수요를 반영한 산학 프로젝트 및 전문 교육과정 운영</b></p> <ul style="list-style-type: none"> <li>○ 산학 프로젝트 운영을 통한 학생의 현장 적응력 및 문제해결 역량 함양</li> <li>○ 기업에서 필요로 하는 실무 기술역량 확보를 위한 수혜학생 중심 단기 전문 교육과정 개발·운영</li> </ul>
	<p><b>③ 산학협력 체계 구축 및 성과 확산</b></p> <ul style="list-style-type: none"> <li>○ 총괄운영위원회 구성 및 운영을 통한 산학협력 체계 구축</li> <li>○ 성과교류회, 만족도 조사, 자체평가 등을 실시하여 성과제고 및 확산</li> <li>○ 취업지원 프로그램을 통한 교육과 고용의 연계 유도</li> </ul>

#### ※ 주요 성과지표

구분	지표명		구분	지표명	
필수 지표	· 수혜인원		자율 지표	· 컨소시엄 참여기업 수	
	· 배출인원			· 취업지원 프로그램 운영 건수	
	· 취업인원(취업률)			· 기술교류회 운영 건수	
	· 산학 프로젝트	건수		· 만족도(학생 및 컨소시엄 기업)	
		참여인원 수			
	· 교과목	개발 건수			
개선 건수					

\* 필수지표는 변동불가, 자율지표는 연구개발기관에서 제시가 가능한 지표로 자율 서술 가능

### Ⅲ. 세부 추진계획

#### ① 석·박사 교육과정 개발·운영

- (교육대상 및 규모) 미래차 보안 시스템 분야 석·박사(전일제)  
연간 신규(당해연도 입학생) 15명 이상 양성(대학당 최소 5명 이상)

< 연차별 최소 교육 규모 >

구분	'23	'24	'25	'26	'27	계
신규	15	15	15	15	15	75
계속	-	15	15	15	15	60
계	15	30	30	30	30	135

- (교육과정) 산업계 수요를 반영한 특화 전공(트랙) 도입 및 교육과정(커리큘럼) 개발·운영

\* 특화분야: ①AI 보안, ②SW 보안, ③네트워크 보안, ④클라우드 보안

\* 특화 전공(트랙) 도입 필수, 필요시 특성화 학과 신설(개편) 가능

\* 산학 프로젝트 정규 교과 반영 필수

< 특화분야별 교과 체계도(석사과정 예시) >

구분	AI 보안	SW 보안	네트워크 보안	클라우드 보안
기초	미래차 보안 시스템 개론, 미래차 해킹의 이해, 사이버 관리시스템, 위협분석			
	기초 인공지능	바이너리 코드분석, SW보안	자동차 네트워크 보안	센서기반 빅데이터 기본
전공	보안 딥러닝, V2X 통신 보안, 임베디드 OS 보안			공간빅데이터 보안특론
	인공지능 보안 특론	차량용 임베디드 SW 보안	고급 네트워크 보안기술의 이해	차량용 5G, 자율주행차 보안
실무	산학 프로젝트, 현장실습 등			

- (교과목 및 교재) 사업추진 전과 후의 특화 분야별 교육과정 체계도 및 교재 개선방향 제시

#### ② 산업계 수요를 반영한 산학 프로젝트 및 전문 교육과정 운영

- (산학 프로젝트) 기업과 대학이 공동으로 기업의 기술문제를 해결하는 과정에서 학생의 연구경험 축적 및 문제해결 역량 함양



< 산학 프로젝트 운영 프로세스(예시) >

1) 프로젝트 발굴	· 컨소시엄 기업을 포함한 해당분야 기업들을 대상으로 수요 발굴 및 현장수요(애로) 기반 실제문제 도출
2) 프로젝트팀 구성	· 수요조사를 통해 발굴된 프로젝트별 수혜(참여) 학생 매칭 (대학원생과 기업 실무자로 구성된 프로젝트 팀 구성)
3) 프로젝트 선정	· 대학별 구성된 프로젝트팀을 심사하여 우선 지원 프로젝트 선정 및 지원
4) 프로젝트 수행·평가	· 팀별 프로젝트 수행 및 성과평가 실시(성과지표 개발·활용)
5) 성과 확산	· 성과교류회 등을 통한 프로젝트 성과 발표 · 성과결과를 석·박사 논문에 연계 유도 · 기업과의 스킨십을 통한 고용연계 유도

- (전문 교육과정) 기업에서 요구하는 수준의 실무 기술역량 확보를 위한 수혜학생 중심의 단기 집중교육과정 개발·운영
- (우수 강사진 확보) 대내·외 전문 강사진 Pool 구축 및 활용
- (인프라 활용) 연구개발기관(주관·공동) 및 공공기관 등의 미래차 보안 시스템 분야 既보유 인프라(실습장비, S/W 등) 활용

### ③ 산학협력 체계 구축 및 성과 확산

- (총괄운영위원회) 연구개발기관(주관·공동) 및 외부전문가 등으로 위원회를 구성\*하여 교육과정 개발·개선, 성과제고 및 확산 등 사업 추진 전 과정에 대한 자문 및 모니터링 등 성과점검 활동 추진
- \* 10인 내외, 컨소시엄 기업 소속 전문가 포함
- (성과제고 및 확산) 주관연구개발기관은 컨소시엄 차원의 성과 교류회, 만족도 조사, 자체성과평가 등을 실시
- (성과교류회, 연 2회) 연구개발기관 우수사례 발굴 및 공유
- (만족도조사, 연 1회) 컨소시엄 기업 및 학생 대상 만족도 조사를 실시하여 교육과정 개선에 반영

- (수요조사, 연 1회) 대학원 교육과정 개편 및 프로젝트 수요 발굴을 위해 관련 기업을 대상으로 수요조사 실시 및 사업계획 반영
  - \* 수요조사는 계획안(수요조사 기간, 대상, 문항 등 포함) 및 결과보고서(회수율, 주요내용 등 포함)를 문서 형태로 관리
- (자체성과평가, 연 1회) 외부전문가로 구성된 평가위원회를 통해 연구개발기관 자체 성과평가를 실시하여 사업비 차등 지원
- (고용연계 유도) 채용기업 발굴, 기업-학생 취업매칭 지원, 수혜학생 대상 취업컨설팅 등 취업지원 프로그램 운영

## IV. 근거법령 및 규정

### □ 근거법령 및 규정

- 전문기관, 주관·공동연구개발기관은 사업 수행 시 관련 법령 및 규정을 준수
  - \* 관련법령 및 규정 : 「국가연구개발혁신법.시행령.시행규칙」, 「산업기술혁신촉진법.시행령.시행규칙」, 「산업기술혁신사업 공통 운영요령」, 동 요령의 부속요령 및 하위지침 등

### □ 기술료 징수 및 성과활용

- 동 사업은 인력양성 목적의 사업으로 기술개발에 따른 수익사업이 아님에 따라, 기술료 징수 및 성과활용 보고 면제
  - \* 관련근거 : 국가연구개발혁신법 제18조(기술료의 징수 및 사용), 국가연구개발혁신법 시행령 제40조(기술료 등의 감면), 산업기술혁신사업 공통운영요령 제39조(기술료의 징수, 사용 및 관리), 제40조(사업 종료 후 활용 보고 및 평가)

### □ 동시수행 연구개발 과제 수

- 동 사업은 인력 양성 사업으로 연구책임자 및 연구자의 동시수행 연구개발과제 수 제한(3책 5공)을 적용하지 않으나 참여율은 적용함
  - \* 관련근거 : 국가연구개발혁신법 시행령 제64조(연구개발과제 수의 제한) 제2항 제4호

## V. 추진일정

---

- ☐ '23. 1월 중 : 시행계획 공고
- ☐ '23. 2월 중 : 연구개발계획서 접수 (신청기관 → KIAT)
- ☐ '23. 3월 중 : 선정평가 추진 및 평가결과 확정  
(산업부, KIAT)
- ☐ '23. 3월 중 : 연구개발계획서 수정보완 (KIAT ↔ 연구개발기관)
- ☐ '23. 3월 ~ : 협약체결 및 연구개발비 지급 등

\* 상기 일정은 상황에 따라 변동 가능