2025년도 전기 졸업과제

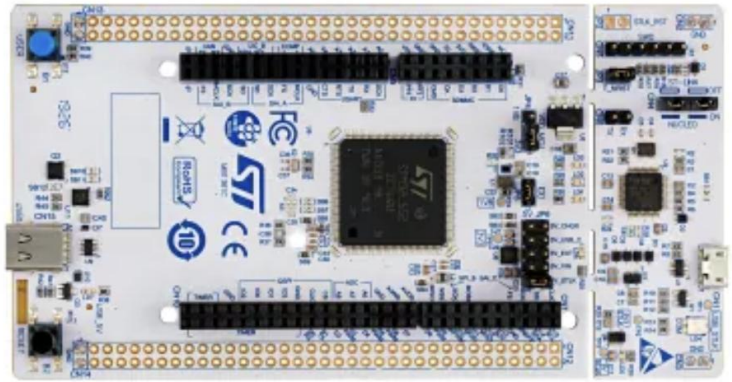
마이크로 컨트롤러에서의 안전한 로봇 어플리케이션 수행을 위한 원격 증명 기술 개발

응답하라 지휘본부

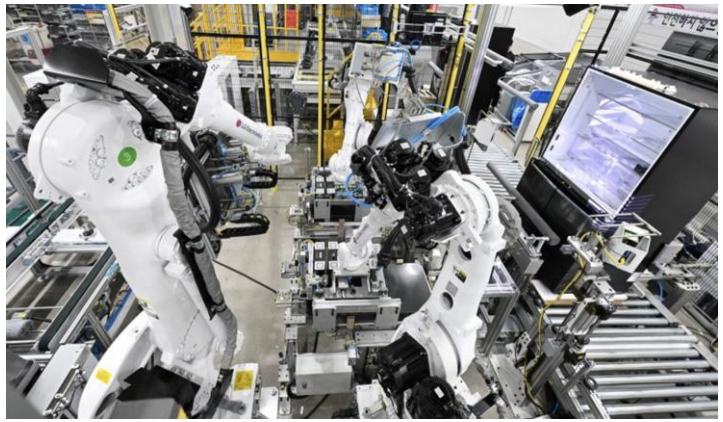
목차

1. 연구 배경

MCU 기반 로봇의 확산



MCU

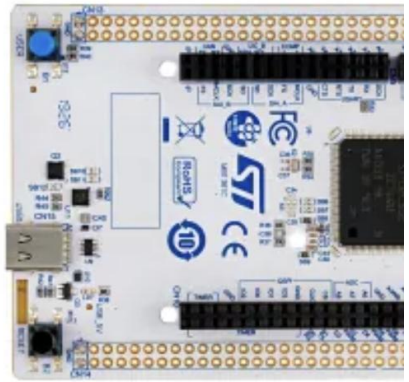


스마트 팩토리

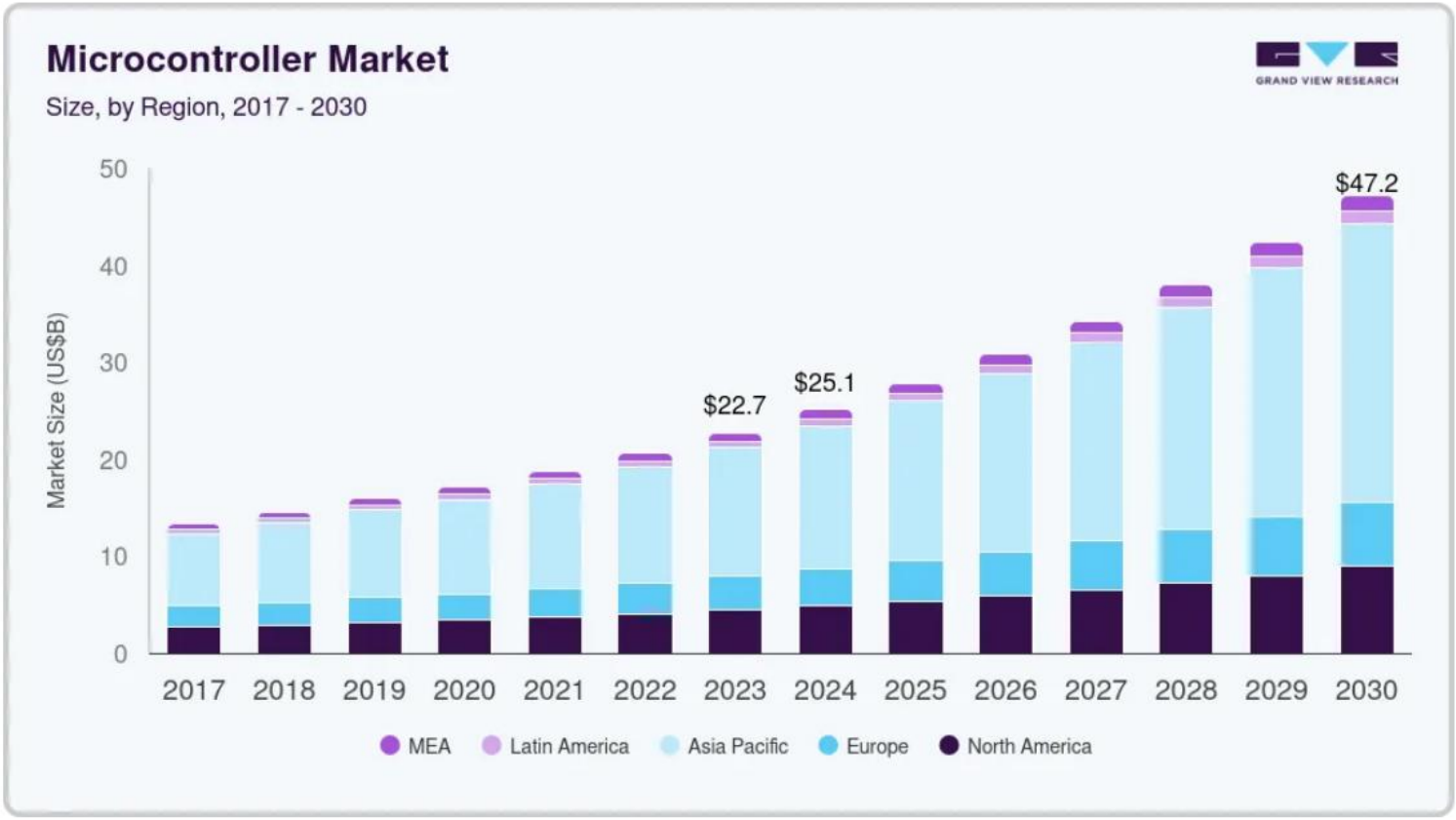
자율 로봇

1. 연구 배경

MCU 기반 로봇의 확산



MC



로봇

1. 연구 배경

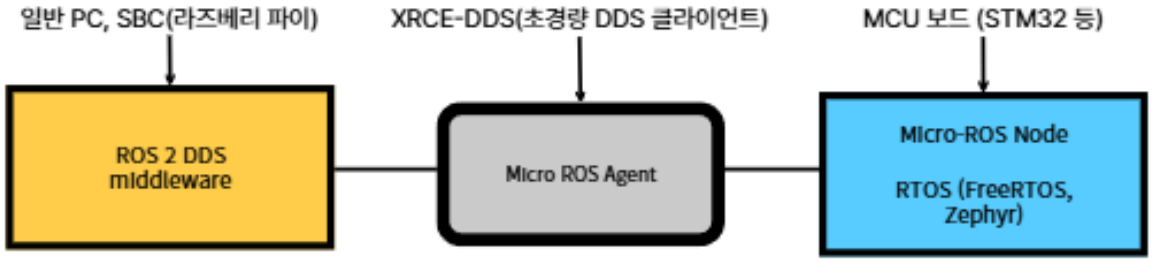
ROS

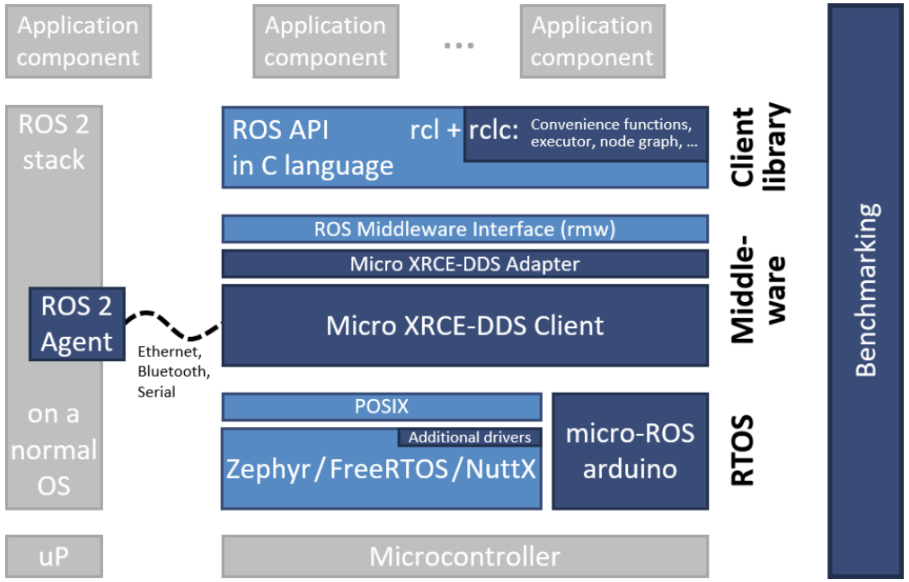
- 로봇 소프트웨어 개발을 위한 오픈소스 프레임워크
- 노드 간 메시지 기반 통신 구조
- 다양한 센서 · 하드웨어 연동 용이
- Linux, Windows, macOS 에서 모두 사용 가능

1. 연구 배경

Micro-ROS

- 고성능의 ROS2를 MCU에서 사용할 수 있도록 경량화한 버전
- 다양한 RTOS와 통합 가능





1. 연구 배경

Micro-ROS 보안의 한계

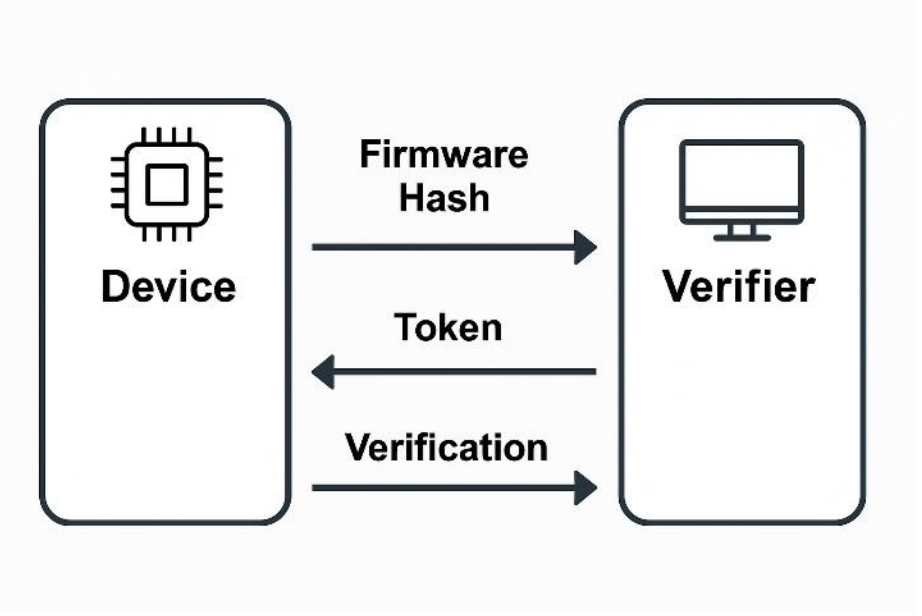
- 경량화에 집중하여 보안 기능 제한
- 제한된 메모리와 연산 자원으로 보안 기능 구현이 어려운 저사양 MCU
- 분산 구조 → 노드 하나 공격 시 전체 네트워크 위협

1. 연구 배경

원격 증명 (Remote Attestation)

- 원격으로 장치가 변조되지 않았음을 증명하는 기술

- 펌웨어 해시 · Nonce를 이용해 무결성 보장



1. 연구 배경

기존 원격 증명의 한계

- 다양한 MCU 하드웨어에서의 낮은 범용성
- 자원 제약 환경에서 활용하기 어려운 고사양의 기술
- 통신 프로토콜 보안의 부재

2. 연구 내용

구현 아키텍처

DICE

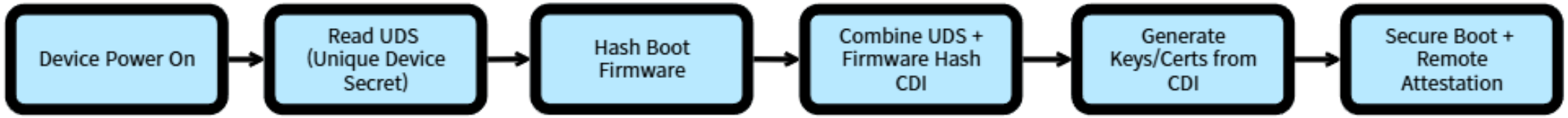
DICE + MPU

TF-M + TZ-M

2. 연구 내용

DICE

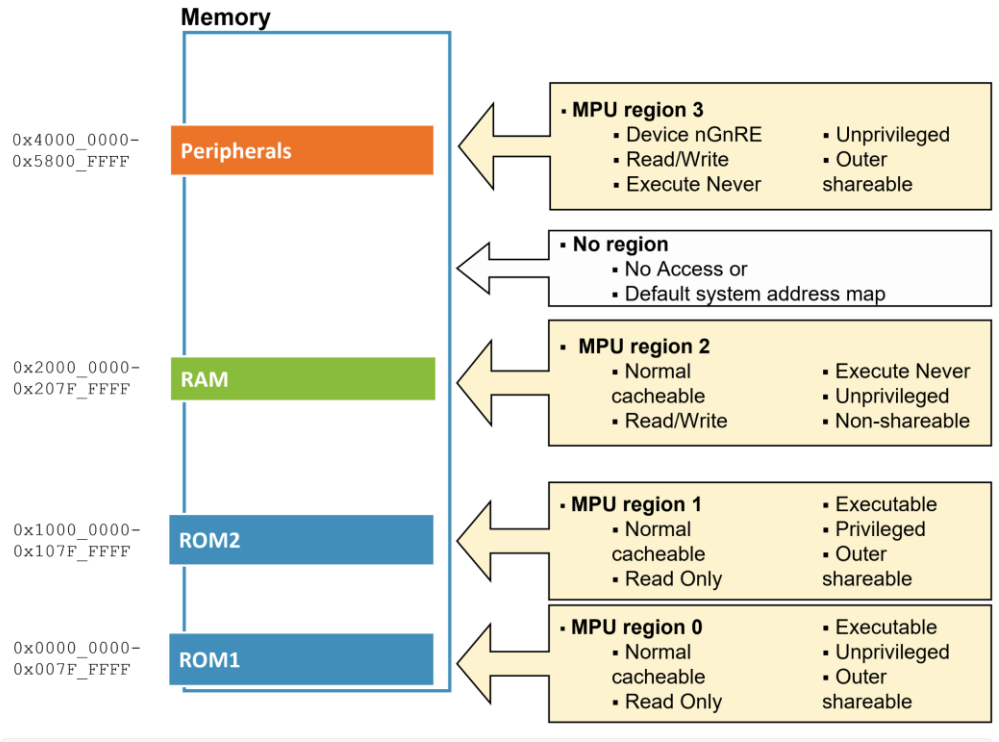
- 경량 Root of Trust 프레임워크
- 하드웨어 보안 칩 없이 MCU에서도 보안 부팅과 신뢰 연속성 제공
- 부팅 시 UDS + 펌웨어 해시로 키 생성
  → 원격 증명 기반 확보



2. 연구 내용

MPU (Memory Protection Unit)

- MCU의 메모리 접근 권한을 제어하는 하드웨어 유닛
- 코드 · 데이터 영역 보호 가능
- Privileged/Unprivileged 모드 분리로 보안 강화



2. 연구 내용

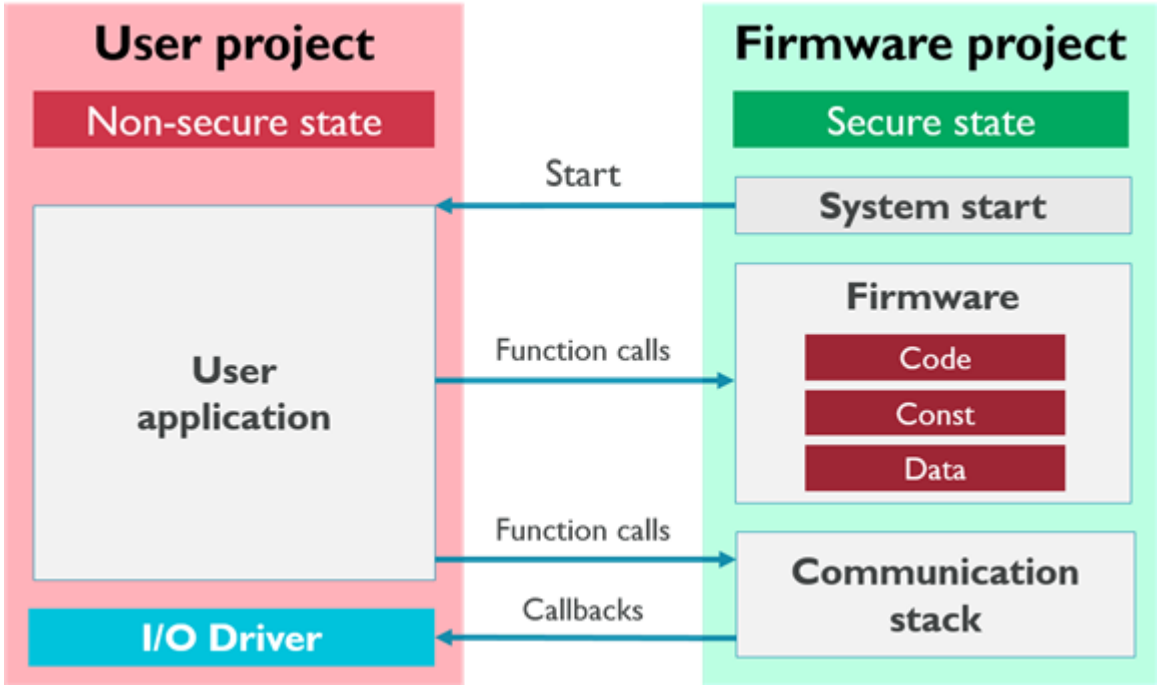
TF-M (TrustedFirmware-M)

- Arm에서 제공하는 오픈소스 펌웨어
- 암호화, 키 관리, 보안 부팅, 원격 증명 등의 보안 서비스 제공
- 경량 MCU 환경에서도 표준 기반 보안 체계 구축 가능

2. 연구 내용

TrustZone-M

- Arm Cortex-M MCU에서 제공되는 하드웨어 수준의 기능
- 메모리 · 주변장치 · 실행 모드를 Secure world/Non-Secure World로 구분
- TF-M과 결합하여 높은 신뢰성의 보안 아키텍처 구현 가능



3. 연구 결과

성능 평가

- Uart를 이용한 보드와 서버의 1대1 통신 환경
- 보드(dient)와 서버(agent) 양측에서 오버헤드 측정
- 서버(agent) 측에서는 3가지 단계로 나누어 측정
- 보드에 flash되는 firmware size도 측정

3. 연구 결과

성능 평가

- 총 소요 시간 (ms)

	Baseline	DICE	DICE + MPU	TF-M + TZ-M
Nonce 생성	0.10	0.12	0.12	0.14
Token 수신	9.20	373.03	441.79	551.96
검증 및 세션 생성	5.59	9.50	10.30	242.93
Total	14.69	382.65	451.21	795.03

- Board Cycle

	Baseline	DICE	DICE + MPU	TF-M + TZ-M
Cycles	2538704	41791713	45679547	61123655
Overhead	100%	1646%	1799%	2407%

3. 연구 결과

성능 평가

- Flash Size

	Baseline	DICE	DICE + MPU	TF-M + TZ-M
Byte	126596	220296	277924	298372
Overhead	100%	174%	219%	235%

- 보안 성능 평가

	DICE	DICE + MPU	TF-M + TZ-M
연결 시점 무결성 검증	O	O	O
토큰 생성 메모리 변조 방지	X	O	O
토큰 생성 프로세스 격리	X	X	O

3. 연구 결과

결론

- 각 아키텍처 설계 및 구현 성공
- DDS Security+라는 논문과 비교하여도 합리적인 Overhead 성능 – 약 0.79초
- 각 아키텍처 별 구분되는 보안 수준
- MCU 환경에서도 원격 증명 기술 적용 가능성 입증

3. 연구 결과

향후 연구 방향

포괄적 런타임 보안 강화	이식성 검증	지속적 무결성 검증	실시간 성능 최적화
MPU 보호 범위 확장 + CFI 적용 = 정교한 공격 방어 (ROP/DOP)	다양한 환경에 적용 하드웨어 : ARMv7-M RTOS : FreeRTOS 등 → 범용성 확보	동적 원격 증명 도입 + 무결성 훼손 탐지 시 자동 회복 매커니즘	검증 로직 재구현 (Python → C++) Or 암호화 연산에 하드웨어 가속기 활용

자료 출처

- ppt 템플릿 : https://bit.ly/3lX9BXD
- LG 전자 뉴스룸 : https://live.lge.co.kr/2506-lg-smartfactory/
- ROS logo : https://www.ros.org/blog/media/
- MPU : https://developer.arm.com/documentation/107565/0101/Memory-protection/Memory-Protection-Unit