

# ProMik

## Cyber Security

전자 제품 제조용

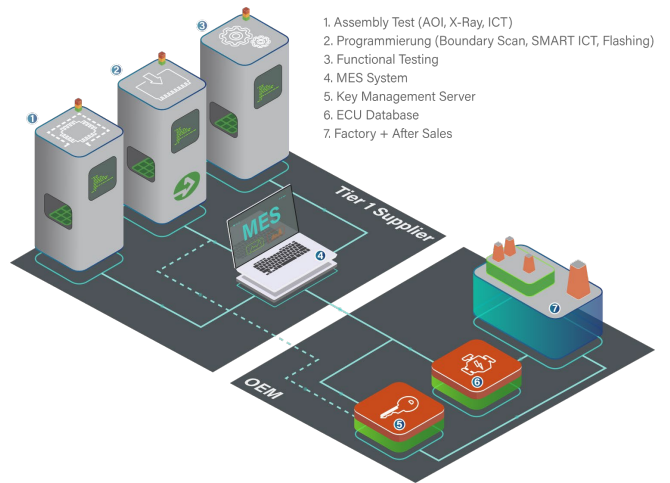


# Cyber Security

## 개요

생산 및 보안 데이터를 OEM에서 Tier 1의 생산 시설로 전송하는 인터페이스는 많은 경우 제조 실행 시스템(MES) (4)에 의해 제공됩니다. 이 통신 경로를 통해 ECU 관련 데이터는 OEM의 해당 데이터베이스(6)로 전송될 수 있으며, 보안 관련 데이터, 예를 들어 키 관리 시스템(5)에서 나온 데이터도 전송될 수 있습니다.

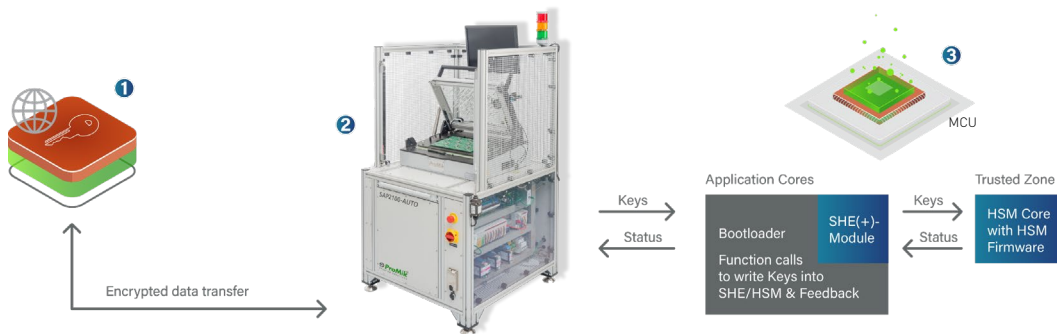
키 프로비저닝, 즉 키 생성이 Tier 1에서 이루어지는 경우, 이 키들은 OEM의 백엔드로 전송될 수 있습니다. 대안으로, 보안 정보는 중간 MES 없이 OEM 특정 통신 인터페이스를 통해 직접 전송될 수도 있습니다.



## 주요 기능

- 고객 맞춤형 사이버 보안 요구 사항에 대한 컨설팅 및 구현
- 암호화된 통신을 통한 OEM 백엔드 연결 보안
- MES, 프로그래머 및 부트로더를 통한 애플리케이션 소프트웨어의 암호화 및 복호화
- PGP, AES, RSA 및 "타원 곡선 알고리즘"과 같은 암호화 방법 마스터링
- 사이버 보안 관련 애플리케이션을 위한 소프트웨어 및 프로그래밍 하드웨어
- 펠드버스 인터페이스를 통한 보안 기능 활성화된 장치 재프로그래밍, 예: 소프트웨어 업데이트

## 안전한 ECU 생산 프로세스



### 1. 키 관리 서버

- OEM ECU 데이터베이스
- 키 프로비저닝 서버
- 제조 실행 시스템 (MES)

### 2. 보안 관련 데이터 프로그래밍

- 안전한 파일 처리
- 암호화/복호화
- 플래시 스테이션에서의 키 프로비저닝
- 시드 및 키
- 암호화 지원: PGP, AES 등

### 3. 온칩 보안 기능

- HSM/SHE(+)
- HSM 펌웨어 프로그래밍
- 키 프로그래밍
- 펌웨어 업데이트
- 디버그 인터페이스 잠금
- 플래시 보호
- 보안 부팅 활성화
- 맞춤형 HSM 펌웨어 지원 (예: Elektrobit, Vector 등)