제 3 회

스마트 의료 안전 컨퍼런스 2026

규제를 넘어 혁신으로: AI, 사이버 보안, 그리고 eQMS

의료기기 소프트웨어 환경 변화 대응 위한 전략 가이드

FDA · CRA 대응을 위한 의료기기 임베디드 보안 전략



IAR Korea 이영후 매니저

fae.kr@iar.com

Public

스마트 의료 안전
컨퍼런스 2026

CONTENTS

01 의료기기 소프트웨어 트렌드

02 규제 (FDA, CRA, IEC 62304)

03 Secure Software Development

04 IAR 솔루션 소개

05 Summary

- 세부내용
- 세부내용

Public

01

의료기기 소프트웨어 트렌드



Public

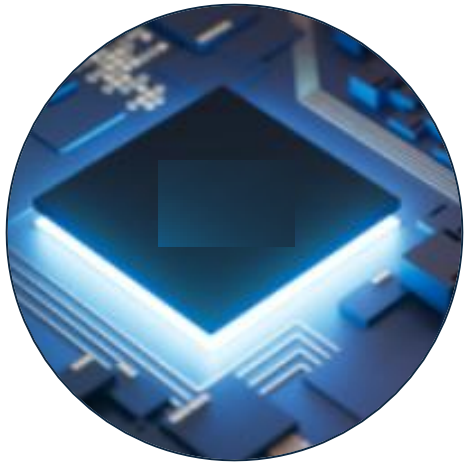
트렌드

- **연결성의 급격한 확대**
  - IoT·클라우드 연동으로 보안 관련 외부 공격이 증가
- **사이버 위협의 현실화**
  - 랜섬웨어 · 공급망 공격이 환자 안전에 직접적 위협을 가하는 사례 증가
- **규제 강화 가속화**
  - FDA·EU CRA 등 글로벌 규제 보안 강화됨

Quality

Faster and more efficient operation.

Improved performance and quality



Safety

Ensuring higher reliability and safety with product certification.



Time to market

Fast time to market for customers with various product line.



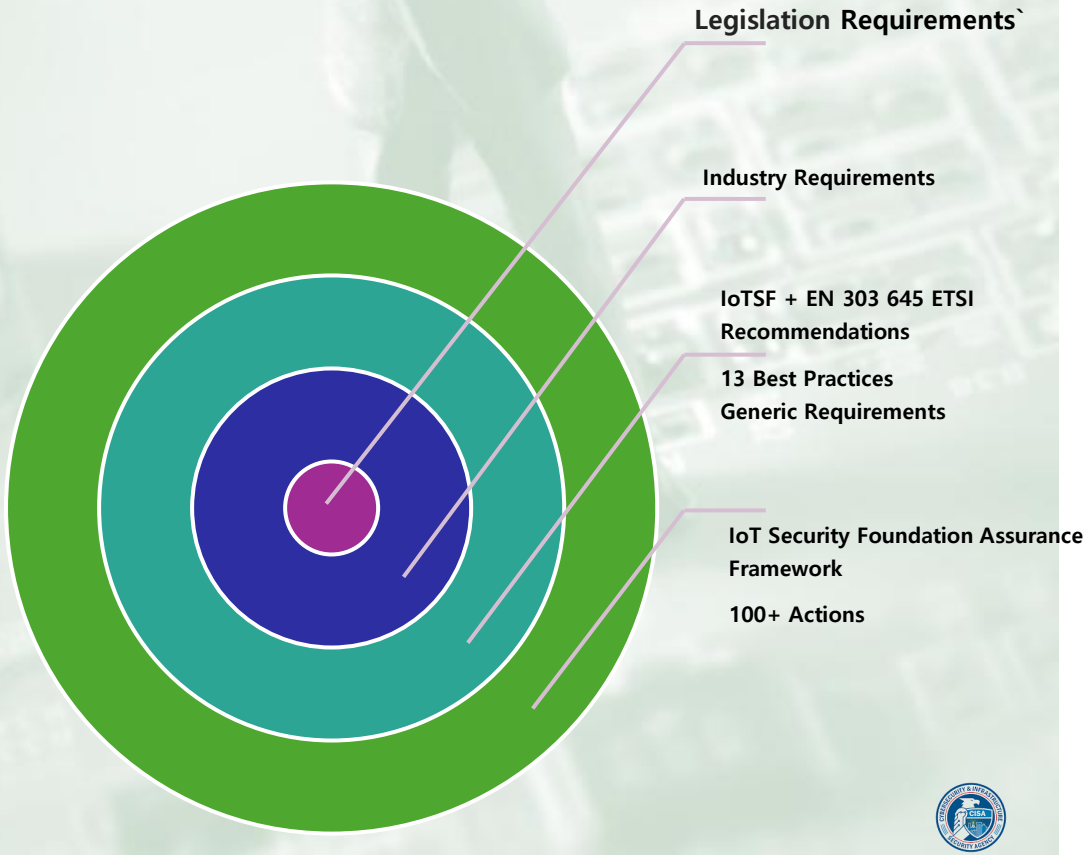
02

규제 (FDA, CRA, IEC 62304)



Public

01 Legislation Angles and the Facts Are Coming



All legislation is based on the 13 best practices defined by the UK Government

Legislation already in force

- US, Executive Order 14028: Improving the Nation's Cybersecurity *[12th May 2021]*
- US, The Cybersecurity Improvement Act of 2020 *[4th December 2022]*

Legislation coming in force

- UK, PSTI Act 2022 *[29th April 2024]*
- **EU**, Cyber Resilience Act *[Q3 2024]*
- US, Cyber Trust Mark in *[Q4 2024]*
- EU, RED – Radio Equipment Directive *[1st August 2025]*

Best Practices and Security Framework

- EN 303 645 The European Standard on connected device security
- IoT Security Foundation Assurance Framework

National Cyber Security Centre

Regulations

- **미국 FDA 사이버보안 지침**
  - 시판 전 제출, SBOM, 위협 모델링, 취약성 공개
- **EU 사이버 복원력 법안 (CRA)**
  - 필수 CE마크, 보안 내재화 설계, 5년 수명주기 의무
- **IEC62304**
  - 소프트웨어 개발 수명주기 표준, 안전 등급 분류, 문서화 및 추적성
- **핵심 규제 요구사항**
  - FDA: 판매 전 사이버보안 문서 및 SBOM 의무화
  - CRA: 연결 기기의 설계 단계부터 보안 내재화, 5년 수명주기 지원
  - IEC 62304: 소프트웨어 안전 등급(A/B/C)에 따른 개발 프로세스 추적성 요구
- 보안을 사후 검토가 아닌 개발 초기부터 내재화 요구

Requirement for Medical Device Security (1/3)

No	Requirement	Target
1	AUTOMATIC LOGOFF (ALOF)	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.
2	AUDIT CONTROLS (AUDT)	The ability to reliably audit activity on the device.
3	AUTHORIZATION (AUTH)	The ability of the device to determine the authorization of users.
4	CONFIGURATION OF SECURITY FEATURES (CNFS)	The ability to configure/re-configure device security capabilities to meet users' needs.
5	HEALTH DATA DE-INENTIFICATION (DIDT)	The ability of the device to directly remove information that allows identification of a person.
6	EMERGENCY ACCESS (EMRG)	The ability of device users to access private data in case of an emergency situation that requires immediate access to stored private data.
7	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)	How the device ensures that data processed by the device has not been altered or destroyed in an unauthorized manner and is from the originator.

Requirement for Medical Device Security

No	Requirement	Target
8	MALWARE DETECTION/PROTECTION (MLDP)	The ability of the device to effectively prevent, detect and remove malicious software (malware).
9	NODE AUTHENTICATION (NAUT)	The ability of the device to authenticate communication partners/nodes.
10	PERSON AUTHENTICATION (PAUT)	Ability of the device to authenticate users
11	PHYSICAL LOCKS (PLOK)	Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of private data stored on the device or on removable media.
12	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)	Manufacturer's plans for security support of 3rd party components within device life cycle.
13	SYSTEM AND APPLICATION HARDENING (SAHD)	The device's resistance to cyber attacks and malware.
14	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of private data stored on device or removable media.

Requirement for Medical Device Security

No	Requirement	Target
15	TRANSMISSION CONFIDENTIALITY (TXCF)	The ability of the device to ensure the confidentiality of transmitted private data.
16	TRANSMISSION INTEGRITY (TXIG)	The ability of the device to ensure the integrity of transmitted private data.
17	DATA STORAGE CONFIDENTIALITY	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.
18	TRANSMISSION CONFIDENTIALITY	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.
19	TRANSMISSION INTEGRITY	The ability of the device to ensure the integrity of transmitted data
20	REMOTE SERVICE	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection

03

Secure Software Development



Public

What journey?

"Why should I care about security?

Nobody else in our industry has any security features, why should I?

My MCU doesn't have any security features.

Security's not my job, it's the engineering team's job".

Sitting on the fence

"I know security regulations are coming for me, but nobody's telling me I must do anything right now.
Our products have never suffered an attack.
Security is too confusing to figure out how to implement on our class of product".

At the beginning

"We know this is a problem, and we want to get in front of it.
Our competitors got hacked and our board told us to make sure it doesn't happen to us.
Our vendor wouldn't sell our products in the EU because we didn't address security".

On our way, but dazed and confused

"We're using a silicon vendor solution, but are concerned if we can't get parts and must switch vendors?
We're rolling our own, but not sure if we're doing it right.
We're paying for to a security consultant.
We think we're on our way, but this is taking a lot more time, money, and effort than we budgeted.".

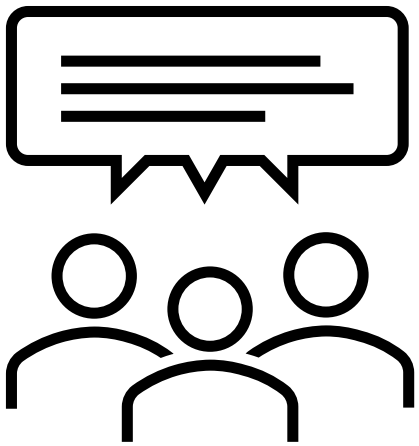
At the cutting edge of security

"Security is every team's job to minimize the attack surface.
We have a team of engineers that maintain our security products and actively monitor CVEs to issue fixes
Devices are securely provisioned for full authentication, attestation, and non-repudiation".

Do you know about the new Legislation?

Encryption/Decryption of application code	Secure boot mechanism ensures trust
✓ **COMMUNICATION & MODIFICATION:** → Only by authorized devices and entities ✓ **HIDING OF DATA :** → By high end cryptography solutions → Asymmetric and symmetric key pairs	✓ **PART OF THE CHIP:** → A secure boot manager and private data/keys ✓ **BOOT (RESET) OF THE CHIP:** → The first code to run at chip ✓ **IMMUTABLE PATH** : → To check installed code → To install new versions when needed

요구사항 분석



인증서 관리

보안
알고리즘

생산 설비

보안관련 지식

기능구현

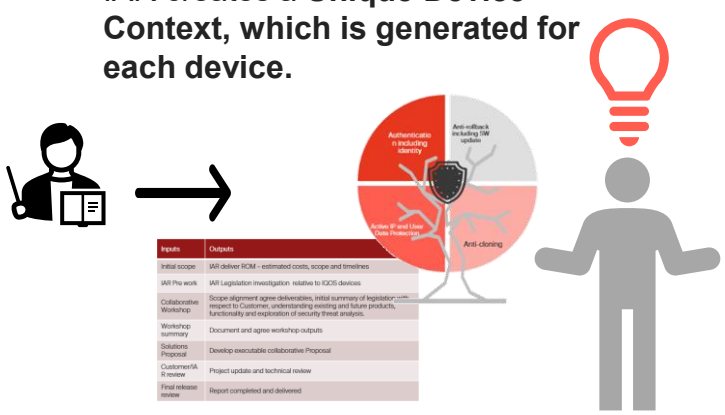
Yesterday

- Experts – All talked about their area of expertise: x509, PKI, Key cycling, 13 best practices?.
- Creating uncertainty over what Embedded Security is?
- Real Problems To Solve



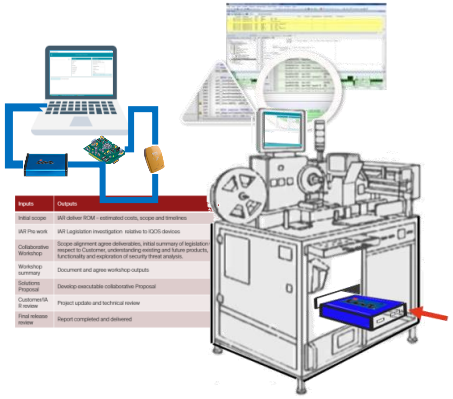
Today

- Collateral - The Problems To Solve
- Theory Hidden By Solutions
- Empowering and supporting our customer to make their own security decisions, through collateral, training, on site support, engineering and consultancy
- IAR creates a **Unique Device Context, which is generated for each device.**



The Solution

- **Legislation Consultancy -**
  Empowering and supporting our customers
- **IAR Security Tools**
- **Limited production/POC**
- **Volume production**



04

IAR 솔루션 소개



Public

The Right Tool Makes All the Difference

Code Quality

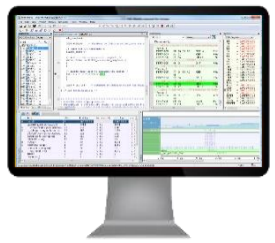
- Compiler efficiency
- code size & speed
- Analysis Tool



Dev Speed

- Advanced debugging tools reduce bug det ection time.

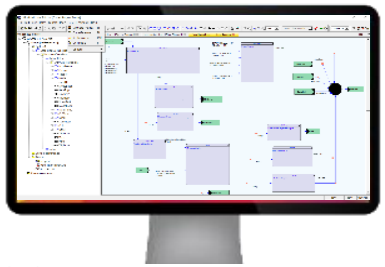


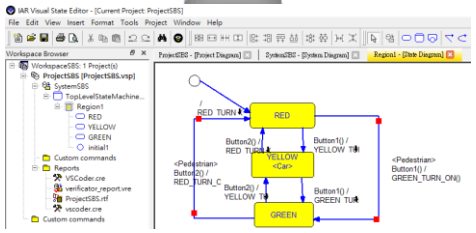


Project Life

- Tool stability
- Support Long-term maintenance

01 A development journey





Requirements

System Design

Architectural D esign

Module Design

Software Implementation

Unit Test

Integration Test

System Test

Acceptance Test

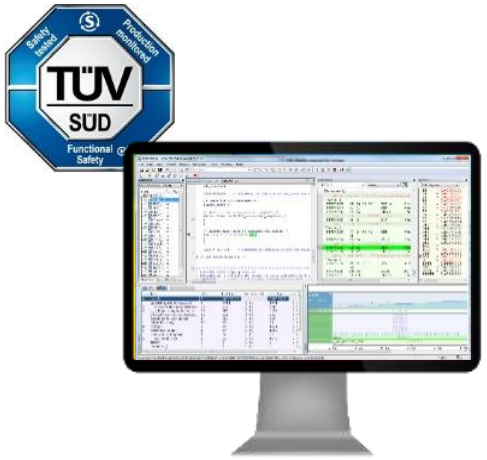








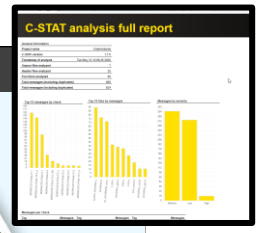


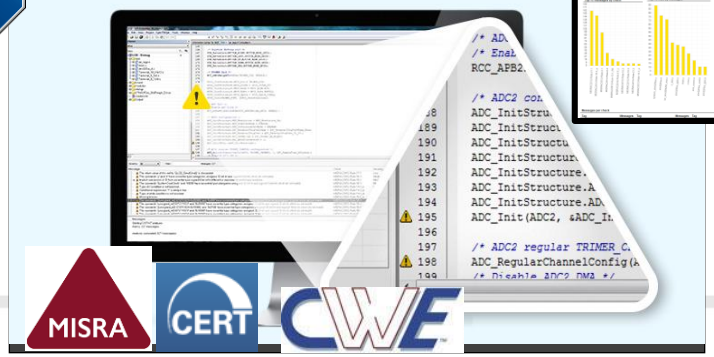




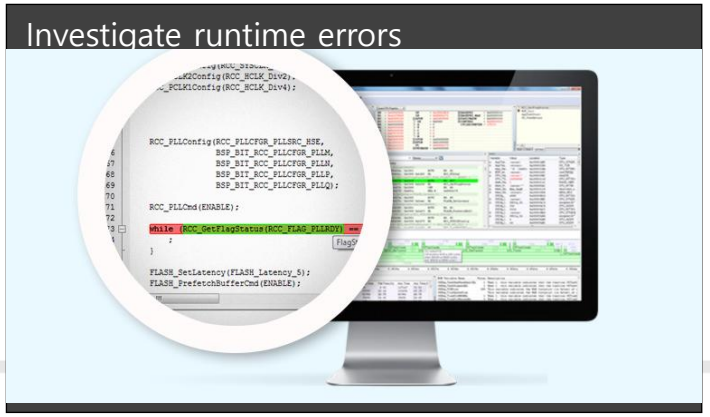


Review potential issues





Investigate runtime errors







02 Customer Success

1. Case 1
   - Application: VentFree Respiratory Muscle Stimulator
   - Their product is required to add security (SBM and software update) and SBOM (Software Bill of Materials) due to FDA requirements.

2. Case 2
   - Application: Nitric Oxide Therapy
   - Their product is required to add security (SBM and software update) due to FDA requirements.

3. Case 3
   - Negative Pressure Wound Therapy System
   - Per the new FDA cybersecurity requirements, the customer needs to secure their firmware from the point of producing the code in their lab through delivery of the code to production house for secure distribution.



HEROIC FAITH MEDICAL

Challenges

Medical device certification

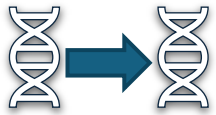
USFDA

Results

Time to Market

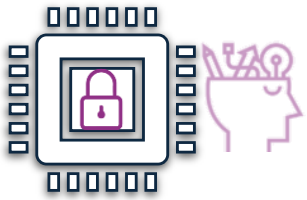
Cost Down

IAR Embedded Trust



Anti-cloning

- 프로그램 및 하드웨어에 대한 고유 식별을 지원
- 위조 방지, 생산과정 암호화 (Serial Number 활용)
- **펌웨어를 복제할 경우, 다른 디바이스에서 동작 불가**



Active IP protection

- 데이터 암호화 및 인증에 사용되는 키 관리
- **어플리케이션 이미지를 암호화 저장**



Anti-rollback

- 소프트웨어 업데이트 프로세스를 관리
- 이전 버전의 SW를 재설치하지 못하도록 방지
- **롤백 공격 및 버전 관리 위협으로부터 보호**

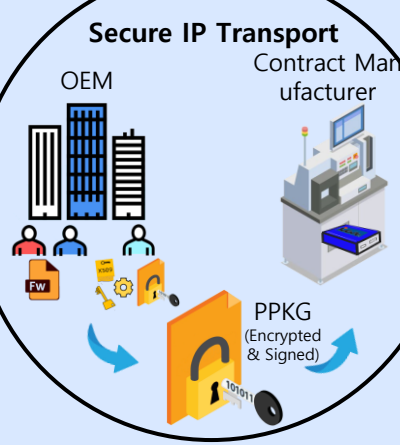


Authentication

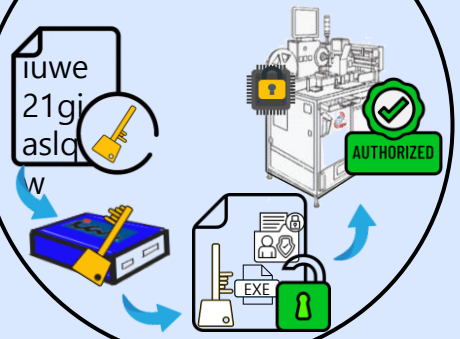
- **Root of Trust, 인증키 연동**
- **어플리케이션 인증 절차 수행**
- **개발/생산프로세스에서 인증된 사용자만 처리**

Secure Supply Chain

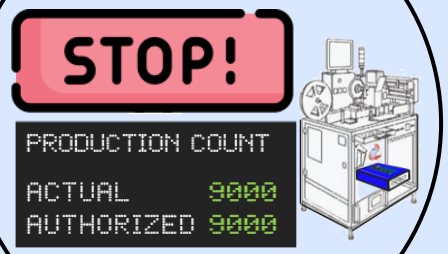
Secure IP Transport



Authorized Manufacturing



Over-production Protection

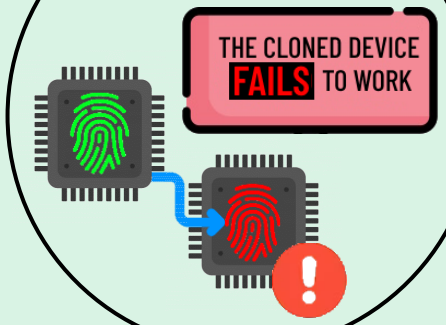


Secure Production Records

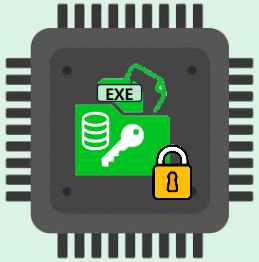


Secure Intellectual Property

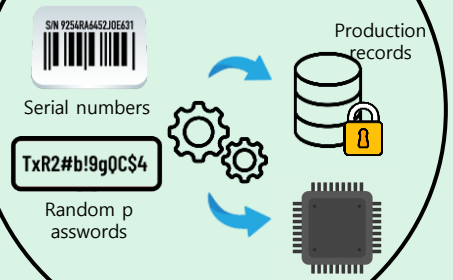
Anti-cloning



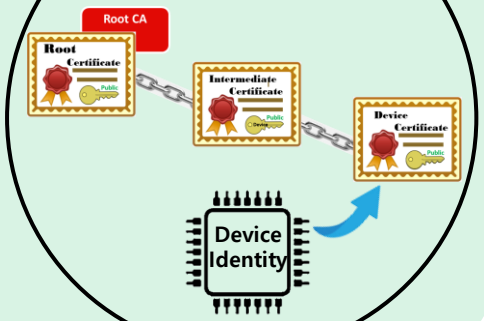
Protected Data at Rest



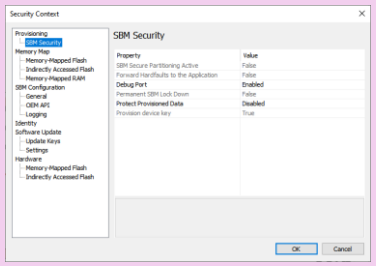
Injection/Generation of Secure Information



PKI-based Device Identity



05 Embedded Trust (ET) : User Flow







OEM

Security Context

- Security Config. Wizard (Security Management & Software Updates)
- Identities and Keys
- SBM Configuration
- Software Update Settings
- Provisioning Settings
- Memory Layout

Secure Boot Manager / Software Updates

- Immutable Boot Process
- Full ANSI C Source Code
- Secure Software Update Mechanism
- Meeting Security Legislation Requirements
- Expedite Time-to-Market
- Ports for many microcontrollers

Application

- Enable application security functions via Secure API
- Mastering: Signing and encrypting updated application

Export P PKG



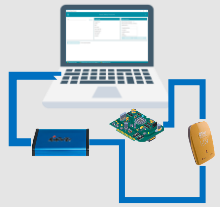
Send to

Encrypted So Only One Security Appliance Can Decode

Secure Provisioning

Prototype

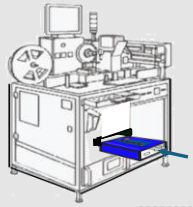
Secure Deploy (SD-P)



Security Appliance (HSM) In Every Machine

Volume

Secure Deploy (SD-M)

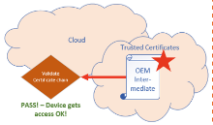




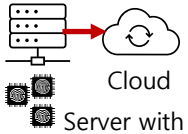


To configure device and unique device context by dialog with the device

Cloud Onboarding



OEM Intermediate Certificate



Cloud Server with provisioned devices records

Security Appliance Identity

IAR Embedded Trust (ET)

(Integrated into IAR Embedded Workbench or Standalone command line tool)

IAR Secure Deploy (SD-P)

From concept to Production

Public

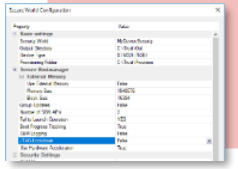
06 개발 프로세스 (Embedded Trust)

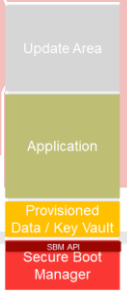


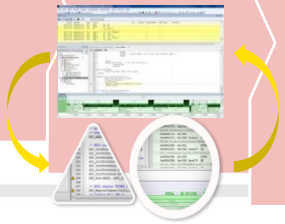




Security Requirements	Software Boot Manager	Develop Software Application	Software Testing
Deploy Security Context	Chain of Trust	Use a suitable Workbench platform	Controlled Samples
Monitor regulations	Security at the Bootloader stage	Multiple iterations creating secure Applications	Testing of Bootloader
PKI Management	Booting from Encrypted image		Secure Operational Deployment









Assign to Volume Production

Sample Production	Volume Production	Keep SW securely updated
Produce minimal quantities to verify Engineering and design assumptions	Scale across multiple geographically distributed sites	Update returned items with new releases
	Preserve security	Update on the field









- 안정성
- 확장성
- 개발 리소스

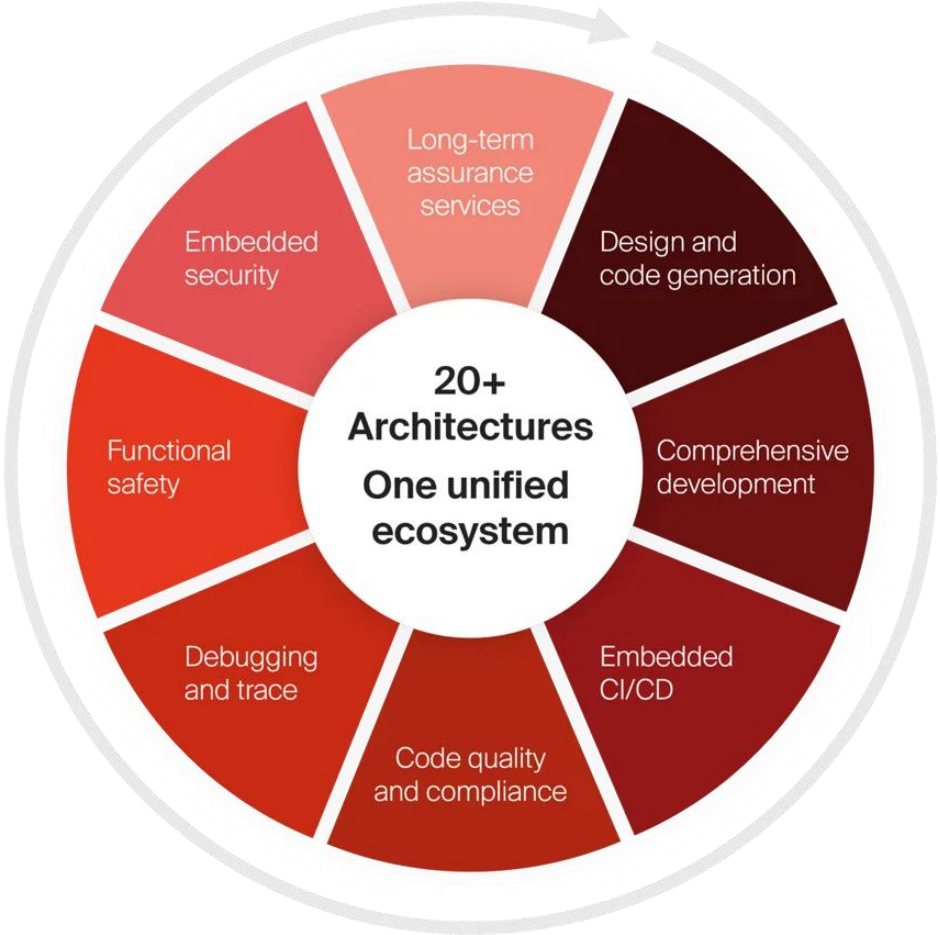
05

Summary



Public

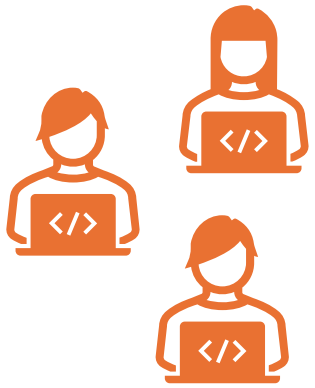
- 기능안전 인증 기반 개발환경 규격 대응
- 멀티코어 디버깅 및 고급 분석 기능
- 코드 품질 향상을 위한 정적·동적 분석
- 다양한 MCU 아키텍처를 지원
- 표준 개발환경 구성
- 보안 부트 및 암호화 기반 보안 인프라
- 자동화 빌드 및 DevOps 연계 환경 구성



표준화된 임베디드 개발환경

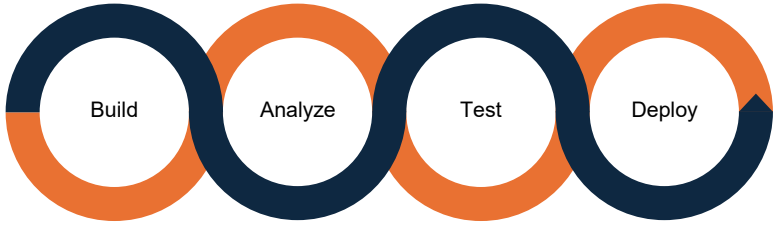
- 유연한 사용자 및 용량 관리 기반의 안정적 환경 운영
- 프로젝트 투입 인원 변동에 유기적 지원 가능
- 자동화 빌드 서버 연동으로 안정성 확보 및 규제 대응

developer users...



- Users are assigned centrally
- Log-in based

automated builds.



- Run CI/CD pipelines in the cloud, locally, or in a h ybrid model

대응 전략

❖ 규제는 현실입니다

- FDA Cybersecurity Guidance · EU CRA · IEC 62304 시행 중

❖ 보안은 설계부터

- Shift-Left 전략으로 개발 초기에 보안을 내재화 전략으로 비용·일정 리스크 절감

❖ IAR로 실무 대응

- IAR의 통합 툴체인
- 코딩 표준 준수, 취약점 탐지, SBOM 생성
- 기능안전용 툴체인 제공
- 규제 대응 과정을 지원

스마트 의료 안전
컨퍼런스 2026



Thank You

주식회사 브이웨이

Public