

ADLINK Cybersecurity Strategy



Product of Digital Element:

Any hardware or software product whose intended use involves data processing or network connectivity

In Scope

Hardware: laptops, mobile phones, routers, etc.

Software: computer applications, video games, etc.

Remote data processing solutions

Not in Scope

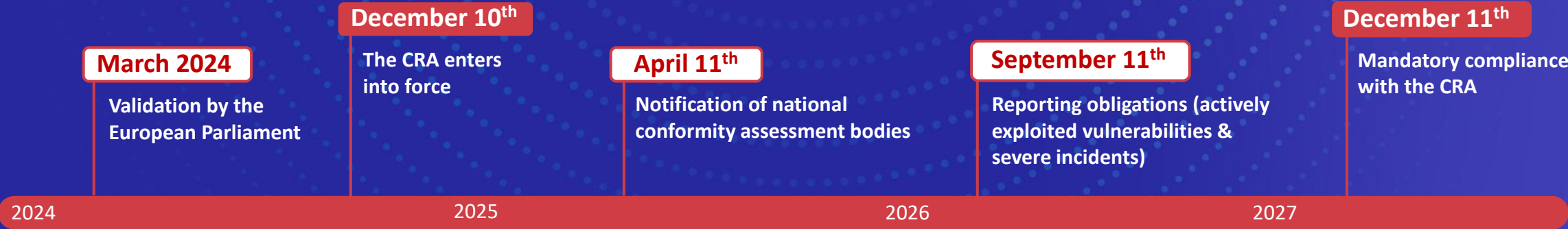
Non-commercial: non-profit open-source software

Services: websites, cloud services, or software-as-a-service (SaaS)

Specific regulated products: including medical devices, automobiles, aviation equipment, and maritime equipment

Cyber Resilience Act (CRA)

The European Parliament passed the Cyber Resilience Act in 2023, which entered into force on December 10, 2024.



During this period, collaborate with ADLINK and our strategic certification partners for self-preparation for CRA.

Risks of non-compliance

15,000,000€

fine in case of failure to meet cybersecurity requirements

5,000,000€

finances in case of inaccurate information provided to authorities

Cyber Resilience Act (CRA) Alignment with IEC 62443 Standards

IEC 62443-4 standards provide a strong framework for CRA compliance, especially for industrial and critical infrastructure products.

CRA

EU regulation mandating essential cybersecurity requirements for digital products throughout their lifecycle.

Focus

Targets hardware, software, and related services with a focus on secure design, vulnerability management, and lifecycle security..

Key Goals

- Reduce cybersecurity risks.
- Standardize security requirements across the EU.

IEC 62443

A globally recognized standard for industrial automation and control system (IACS) cybersecurity.

Focus

Industrial control system (ICS) components and their secure development practices.

Key Goals

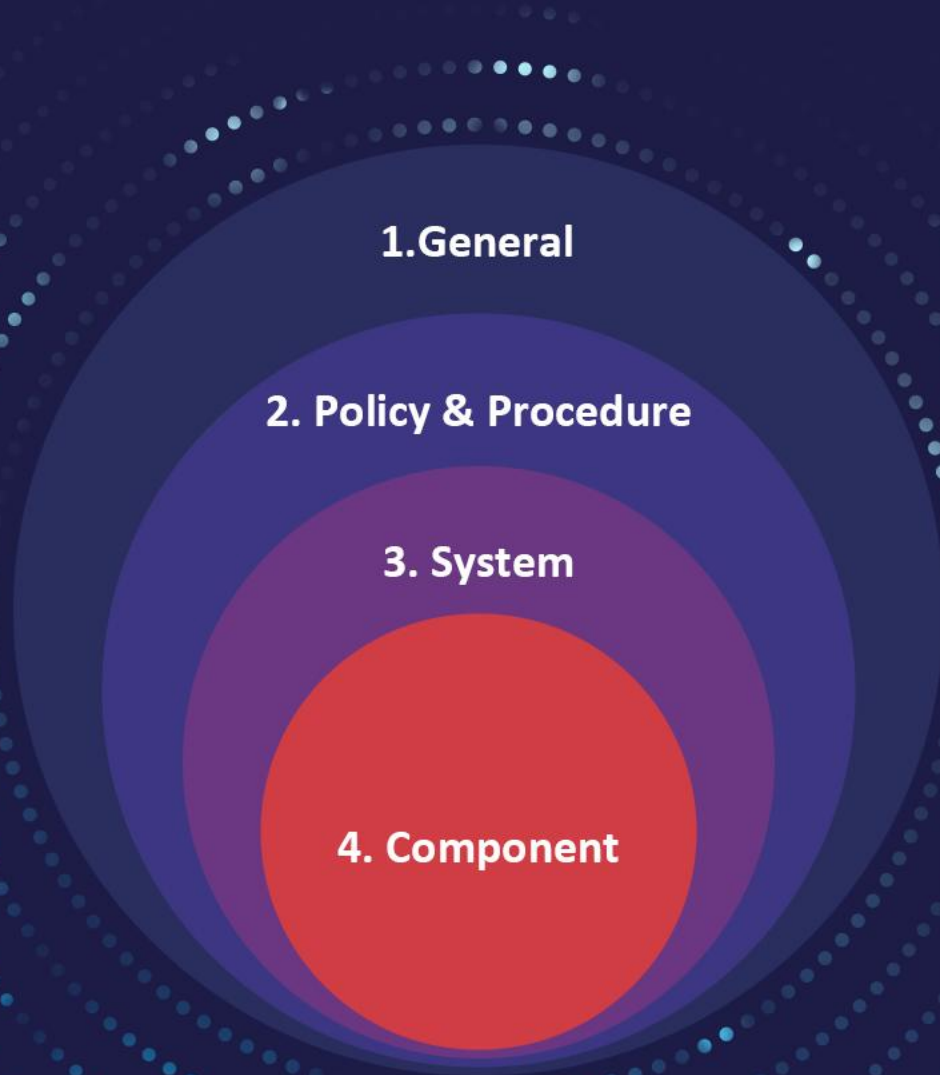
- Security by Design
- Security features
- Risk Assessment

Cyber Resilience Act Requirements Standards Mapping

Security requirements relating to the properties of products with digital elements Vulnerability handling requirements

	Security requirements relating to the properties of products with digital elements													Vulnerability handling requirements							
	1	2	3a	3b	3c	3d	3e	3f	3g	3h	3i	3j	3k	1	2	3	4	5	6	7	8
EN IEC 62443-3-2	X										X										
EN IEC 62443-4-1	X	X													X		X			X	X
EN IEC 62443-4-2				X	X	X		X		X		X	X								

Cyber Resilience Act (CRA) Alignment with IEC 62443 Standards



Industrial Automation & Control System

The Scope of IEC 62443 standard

- 1-1 : Terminology and concepts
- 1-2 : Master glossary
- 1-3 : System security compliance metrics
- 1-4 : IACS security lifecycle and use-case

- 2-1: Requirements for an IACS security management system
- 2-2: Implementation guidance
- 2-3: Patch management
- 2-4: Installation & maintenance

✓ Apply to Asset Owner

- 3-1: Security technologies for IACS
- 3-2: Security levels for zones and conduits
- 3-3: System security requirements and levels

✓ Apply to System Integrator

- 4-1: Product development requirements
- 4-2: Technical security requirement for IACS components

✓ Apply to Component Supplier



2 key standards for cybersecurity compliance:

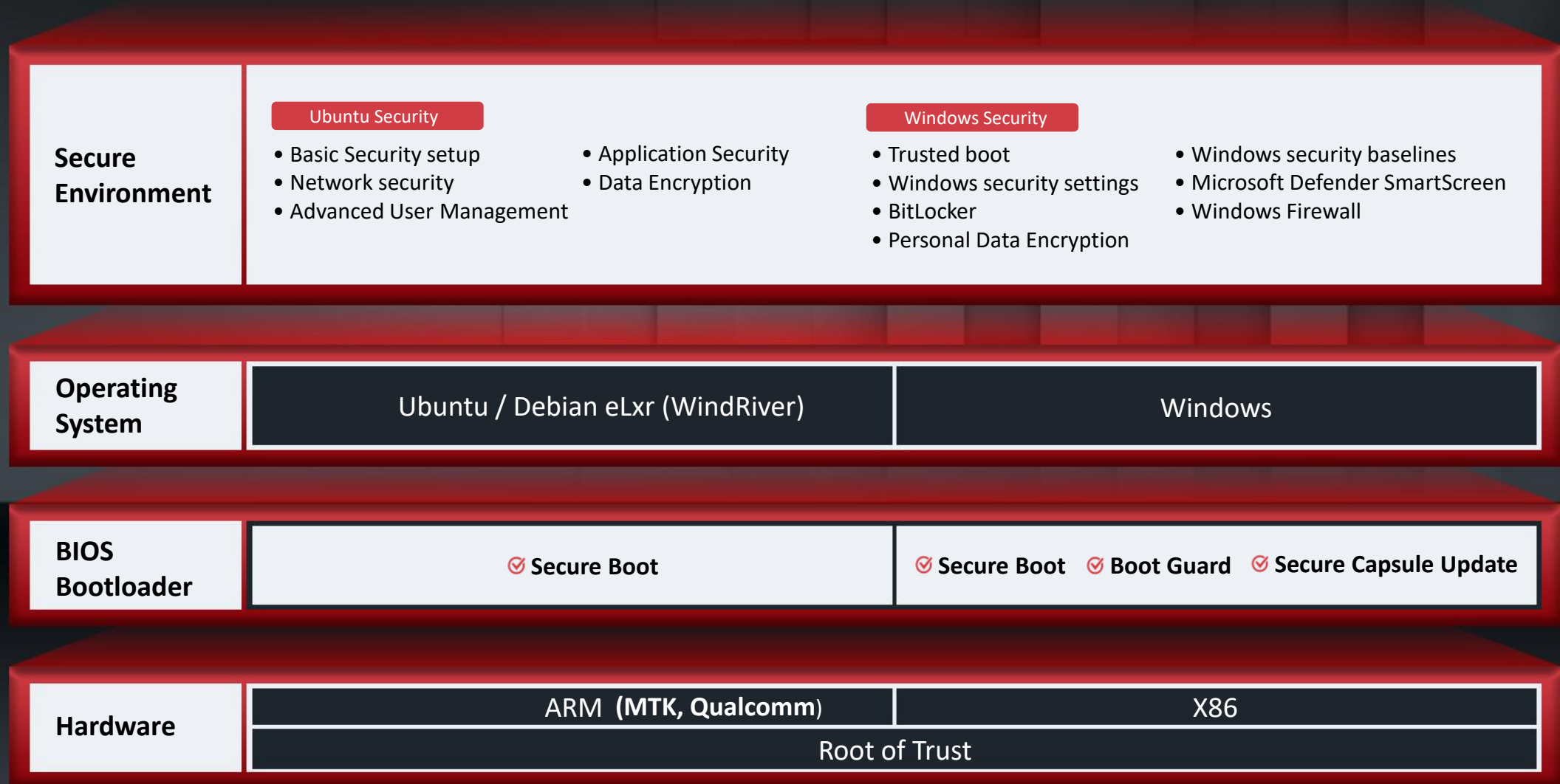
IEC 62443-4-1

Governs secure development processes within organizations, directly supporting CRA's horizontal requirements.

IEC 62443-4-2

Ensures individual product certification, addressing CRA's vertical requirements by certifying cybersecurity features.

Platform Security – IEC 62443 foundation



*Select operating system without long term support will face problem for the security maintenance (Like Yocto)

Certification and CRA Updates



Certification Updates

- IEC 62443-4-1 process security underway.
- Gap analysis completed; standard training ongoing -> refine DEV process.
- Planning for IEC 62443-4-2 (product security).

CRA Updates

- Monitoring CRA development; mandatory horizontal requirements by 2026 and vertical by 2027.
- Efforts: Ongoing gap analysis between IEC 62443 and CRA standards.

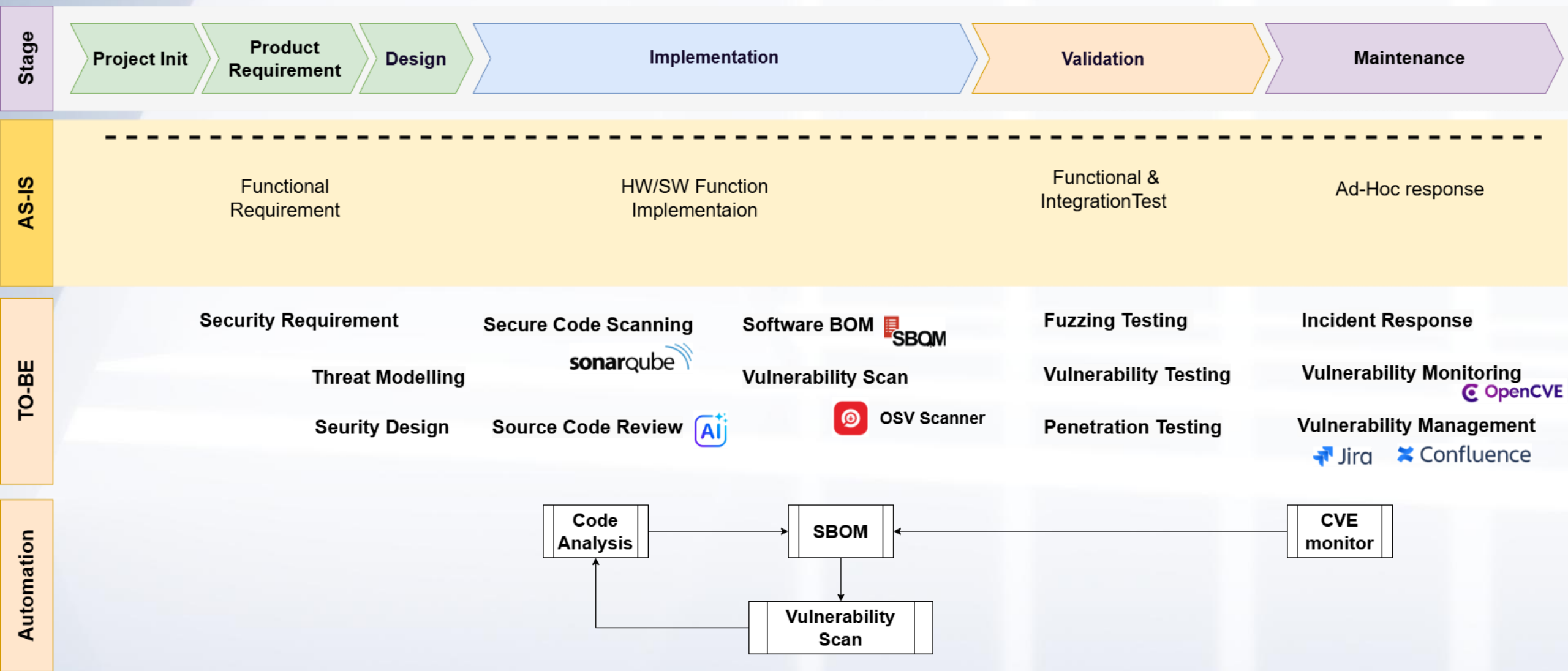
Security Starts at the Source — with IEC 62443-4-1

ADLINK has achieved IEC 62443-4-1 certification, a globally recognized cybersecurity standard for industrial control systems.

This milestone confirms that Secure-by-Design is embedded across our Secure Product Development Lifecycle (SDL)—ensuring that our edge computing solutions are built for resilience, reliability, and long-term protection.

IEC IECCE		Ref. Certif. No.
		FR_Cyber10248
IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)		
Certificate of Conformity – Industrial Cyber Security Capability		
Type	Process Capability Assessment	
Name and address of the applicant	ADLINK Technology, Inc. No. 66, Huaya 1st Rd., Guishan Dist, 333411 Taoyuan City TAIWAN	
Certificate Coverage (including Version)	ADLINK Product Security Development Lifecycle Process V 1.0	
Standard	IEC 62443-4-1:2018	
Requirements Assessed	Security management (13.0,13) Specification of security requirements (5,0,5) Secure by design (4,0,4) Secure implementation (2,0,2) Security verification and validation testing (5,0,5) Management of security-related issues (8,0,8) Security update management (5,0,5) Security guidelines (7,0,7) Maturity Level: ML2	
Additional information (if necessary may also be reported on page 2)	/ Additional Information on page 2	
As shown in the Test Report Ref. No. which forms part of this Certificate	CYT-BCCD-WTW-P24060607 001	
This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.		
 LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES - LCIE 33 avenue du Général Leclerc 92260 Fontenay-aux-Roses, FRANCE www.lcie.fr  Signature: Julien CAUTHIER Certification Officer Date: 25/11/2025		

Integrate Secure Software Development Life Cycle into ADLINK PLC

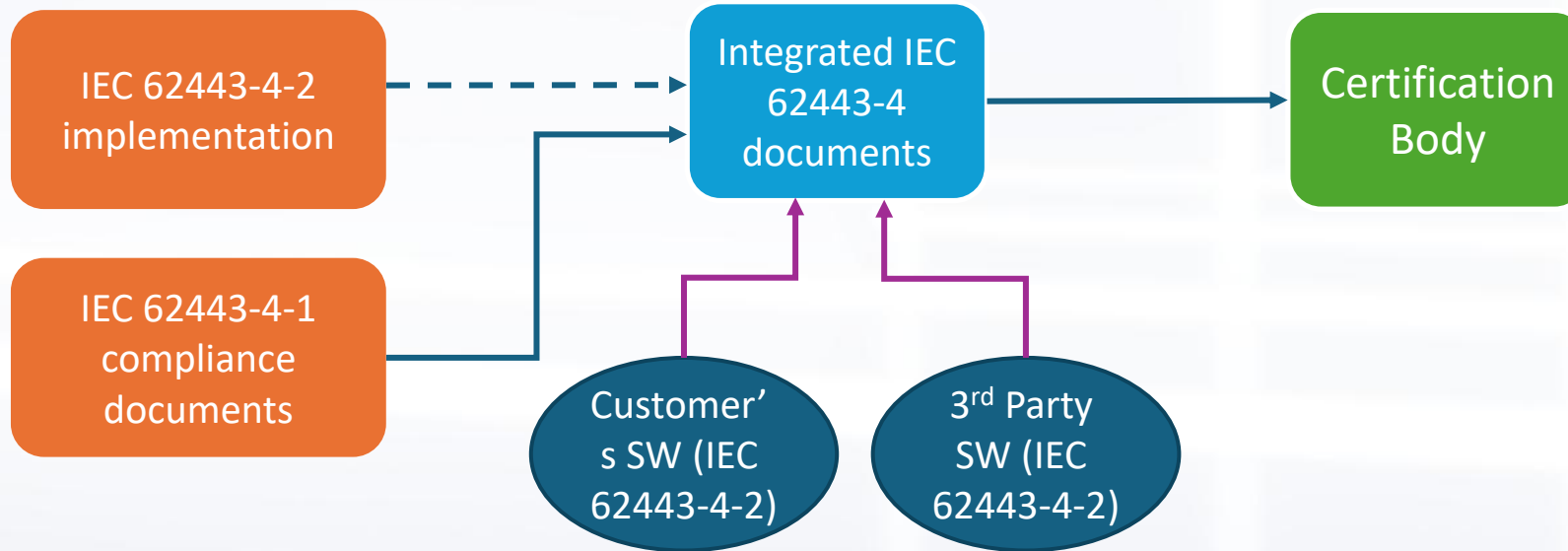


How ADLINK Support Comply with CRA

Support Customers IEC 62443-4-2 Certification

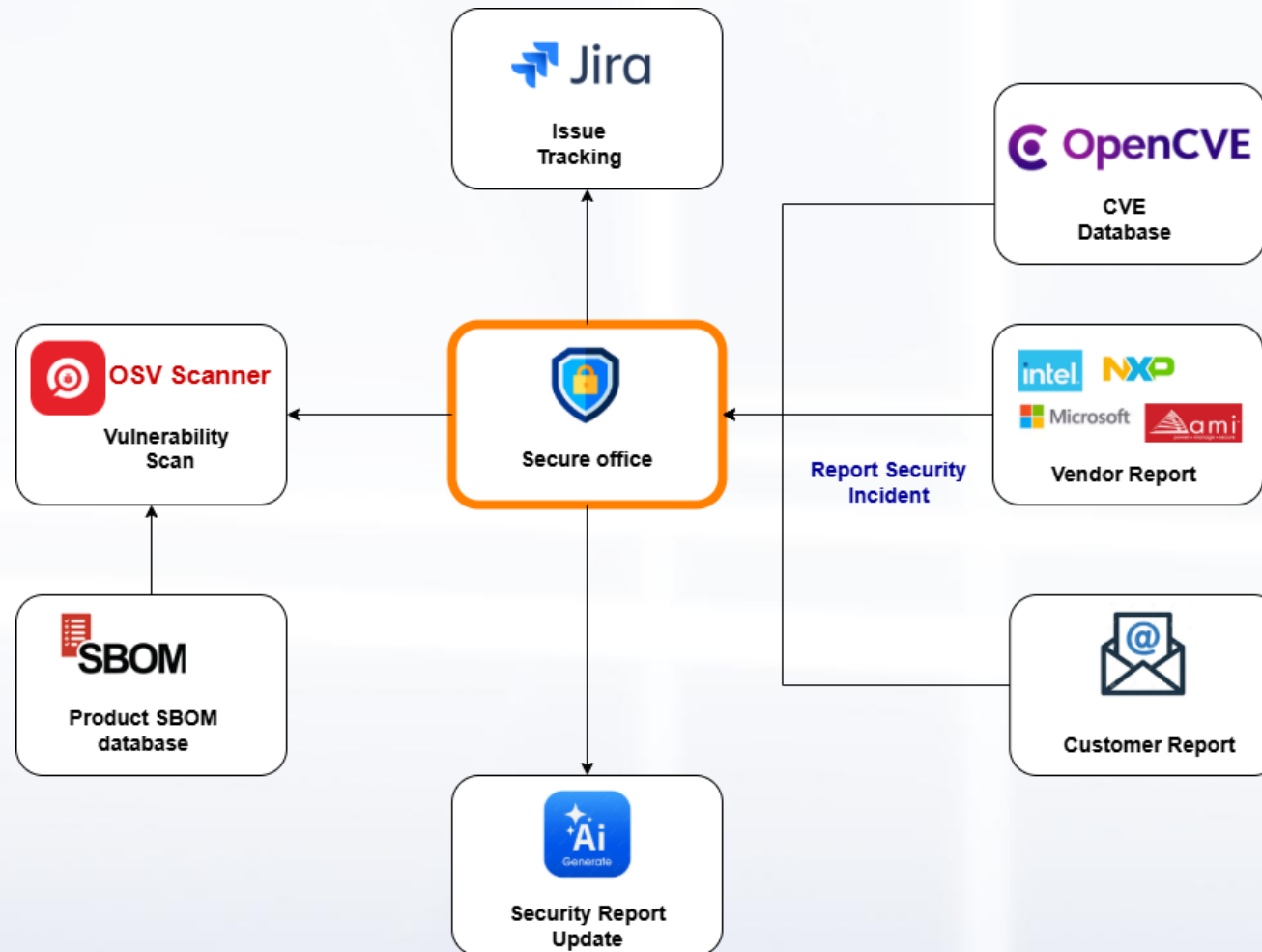


Customers



How ADLINK Support the Cybersecurity

Continuously Monitor and Report the Vulnerability



Vulnerability Management

To meet CRA obligations, a systematic process is needed:

1 Vulnerability Detection

- Continuous monitoring of CVE/NVD/OSV feeds.
- Review the Errata or platform update report from vendor
- Customer report

2 Impacted product identification

- Automated vulnerability scans integrated with CI/CD.

3 Assessment & Prioritization

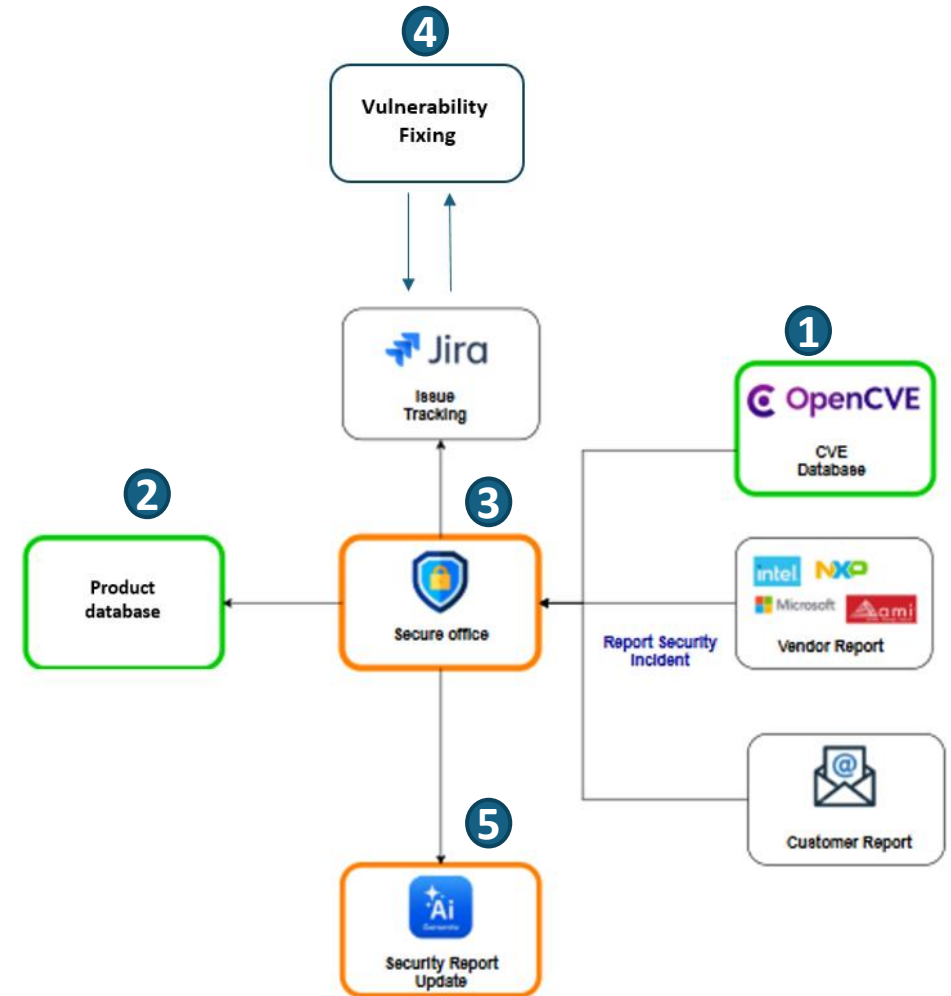
- Risk scoring (CVSS/EPSS) with mapping to product impact.
- Maintain a central Vulnerability Tracking Register (JIRA)

4 Remediation & Patching

- Define patch release
- Ensure EOL products have clear vulnerability disclosure statements.

5 Communication & Transparency

- Provide VEX (Vulnerability Exploitability eXchange) statements
- Publish security advisories and customer notification channels (Web or Email).



ADLINK Deliverables to Support EU CRA

Deliverables

Security Development Lifecycle Documentation

Prepare technical documentation for CRA conformity (risk assessments, design reviews, patch records, and vulnerability handling evidence).

SBOM & Vulnerability Reporting

Ensure every released product version includes a Software Bill of Materials (SBOM) and associated vulnerability reports.

Maintain traceability between SBOM, product versions, and security advisories.

Security Updates & VEX Statements

Provide timely security patches and issue VEX (Vulnerability Exploitability eXchange) statements to clarify exploitability status.



Compliance-Driven Design & Certification

ADLINK is on track for IEC 62443-4-1 certification, showcasing secure design practices, full security lifecycle management, and effective vulnerability response to reduce risks.

Why ADLINK?

ADLINK provides fast and reliable solutions to enhance security and accelerate market deployment.

arm



Partnership with Platform Experts for Cybersecurity

ADLINK collaborate with partners across CPU, BIOS, and OS to stay ahead of regulatory changes and implement advanced cybersecurity mechanisms.



BUREAU
VERITAS



Accelerating Certification with Partnerships

ADLINK has partnered with Bureau Veritas and Delta Cybersecurity Lab to provide customers with comprehensive cybersecurity testing and certification services, ensuring compliance with international standards and enhancing product security.

Backup



ADLINK Technology, Inc.

No. 66, Huaya 1st Rd., Guishan Dist.,
Taoyuan City 333411, Taiwan

Tel: +886-3-216-5088
Fax: +886-3-328-5706



www.adlinktech.com