Cyber Resilience Act (CRA) Compliance White Paper

Industrial Cybersecurity Readiness for Industrial IoT Devices

Publish: 2026, April, 8

1. Executive Summary

As cybersecurity regulations continue to evolve in the European Union, the **Cyber Resilience Act (CRA)** establishes mandatory requirements for products with digital elements.

ICP DAS is committed to aligning with CRA requirements by strengthening product security, secure development processes, and vulnerability management.

To support this commitment, we have initiated certification programs including:

- ISO/IEC 27001 (Information Security Management System)
- IEC 62443-4-1 (Secure Product Development Lifecycle)

Target certification timeline: **Completion by end of 2026**

This white paper outlines our approach to achieving CRA readiness and ensuring long-term cybersecurity compliance for our partners and customers.

---

2. What is the Cyber Resilience Act (CRA)?

The **Cyber Resilience Act (CRA)** is an EU regulation that:

- Applies to **products with digital elements (PDE)**
- Enforces **cybersecurity-by-design**
- Requires **lifecycle security management**
- Introduces **mandatory vulnerability handling and reporting**

Tel : +886-3-5973366 / Fax : +886-3-5973733 / Website : www.icpdas.com

Key Objectives:

- Improve product cybersecurity across the EU market
- Ensure accountability for manufacturers
- Reduce cybersecurity risks in connected devices

---

3. Scope of Our Products

ICP DAS provides industrial automation products including:

- Remote I/O Modules
- Industrial Controllers
- Gateways

These products fall under **Products with Digital Elements (PDE)** and are subject to CRA requirements.

---

4. Our CRA Compliance Strategy

To align with CRA requirements, we focus on the following key domains:

4.1 Secure Development Process

- Adoption of **IEC 62443-4-1**
- Implementation of
    - Secure coding guidelines
    - Threat Modeling
    - Security testing (SAST / DAST)

4.2 Information Security Management

- Establishment **ISO/IEC 27001 ISMS**
- Coverage:
    - Risk assessment
    - Asset management
    - Access control
    - Incident response

Tel : +886-3-5973366 / Fax : +886-3-5973733 / Website : www.icpdas.com

4.3 Vulnerability Management

- Continuous vulnerability monitoring
- PSIRT (Product Security Incident Response Team) setup
- Coordinated vulnerability disclosure process

4.4 Product Security Features

Our products are designed with:

- Authentication and authorization mechanisms
- Secure communication protocols (e.g., TLS)
- Firmware integrity verification
- Secure update mechanisms

---

5. CRA Readiness Roadmap

Phase	Timeline	Description
Phase 1	2026 Q1	Project initiation, gap analysis
Phase 2	2026 Q2–Q3	Process implementation (ISMS + SDL)
Phase 3	2026 Q4	Certification audit
Phase 4	2027 onward	Continuous compliance & monitoring

---

6. Benefits for Our Partners

By aligning with CRA, our distributors and system integrators benefit from:

- Reduced regulatory risk in EU markets
- Faster project approvals
- Increased customer trust
- Long-term product security assurance

---

7. Commitment to Continuous Compliance

Cybersecurity is an ongoing process.

ICP DAS is committed to:

- Continuous improvement of security processes
- Timely vulnerability patching

Tel : +886-3-5973366 / Fax : +886-3-5973733 / Website : www.icpdas.com

- Transparent communication with partners

8. Conclusion

With proactive investment in **ISO 27001** and **IEC 62443-4-1**,

ICP DAS is taking concrete steps toward **CRA compliance readiness**.

We aim to provide secure, reliable, and future-proof industrial solutions for the European market.

9. Legal Disclaimer and Contact Information

- **Nature of Information**:

The timelines and objectives set forth in this white paper are for reference only and do not constitute a legal commitment to "guaranteed certification" or "absolute product security."

- **Schedule Changes**:

The progress of relevant certifications may be affected by the schedules of third-party audit agencies, regulatory changes, or other force majeure events.

- **Contract Precedence**:

The specific technical specifications of the product and the terms of the information security support agreement shall be governed by the formally signed purchase contract or product specification document between the parties.

For more information regarding cybersecurity and CRA compliance:

Email：service@icpdas.com
Website：www.icpdas.com