Securing the Future of Automation

UNIVERSAL ROBOTS

Universal Robots — Cybersecurity Fact Sheet | v10.0 | August 2026

Executive Summary

New EU regulations are making cybersecurity mandatory for industrial robots. Universal Robots is already independently certified and will be fully compliant ahead of every deadline. Existing robots in operation are not affected.

This guide explains what's changing, why it matters, and how Universal Robots is leading the industry toward a secure future.

AT A GLANCE

IEC 62443-4-1 ML3	CRA Ready	Existing Robots	EU MR 2023/1230	NIS2
Certified by TÜV Rheinland 2026 | All of Teradyne Robotics	**2027** Ahead of EU deadline Free PolyScope X update	**Not affected** CRA applies only to products placed on market after Dec 11, 2027	**Target 2026** ISO 10218-1:2025 TÜV cert. EU Machinery Regulation	**Compliant** Already today

COMPLIANCE TIMELINE

2026
IEC 62443-4-1 ML3 certified
NIS2 compliant

→

2026
ISO 10218-1:2025 TÜV cert.
PolyScope 5 & PolyScope X
= EU Machinery Regulation

→

2027
IEC 62443-4-2 SL1 for PolyScope X
Free PolyScope X update
= CRA Compliance

KEY MESSAGES

- ✓ **Cybersecurity in industrial automation is no longer optional.** New EU regulations — the Cyber Resilience Act (CRA), the EU Machinery Regulation, and the NIS2 Directive — require manufacturers and operators to meet mandatory security standards.
- ✓ **Universal Robots is already independently certified** to IEC 62443-4-1 ML3 by TÜV Rheinland — one of the first cobot manufacturers globally to achieve this, and across all of Teradyne Robotics — and is on track for full CRA compliance by 2027.
- ✓ **All existing PolyScope X installations will receive CRA compliance as a free software update.** No hardware changes required. Universal Robots will be ready ahead of the EU deadline.
- ✓ **Existing robots already in operation are not affected by the CRA.** The regulation applies only to products placed on the EU market after December 11, 2027. For legacy equipment, this document provides practical Defense-in-Depth security guidelines.
- ✓ **IEC 62443-4 certification provides "presumption of conformity"** under the CRA — meaning compliance audits can be answered with an internationally recognized certificate rather than costly custom assessments.

Securing the Future of Automation

Two decades ago, the idea of a robot working safely alongside a human on a factory floor was revolutionary. Standards like ISO 10218 turned that vision into everyday reality — and Universal Robots led the way.

Today, cybersecurity is at that same inflection point. As factories become connected and intelligent, every device becomes both an asset and a potential vulnerability. New standards and regulations are emerging to ensure that the automation you rely on is as secure as it is productive.

This guide explains what's changing, why it matters, and how Universal Robots is leading the industry toward a secure future.

WHAT'S INSIDE

1. The Threat Landscape
2. IEC 62443-4 Standards Explained
3. EU Cyber Resilience Act
4. Security Posture & Roadmap
5. Product Compatibility
6. Securing Legacy Equipment
7. FAQ, Glossary & Sources

1. The Threat Landscape

Manufacturing is under siege. Understanding the scale of the threat is the first step toward building resilient operations.

#1
Most-attacked industry globally — for the **5th consecutive year**[1]

$4.6M
Average cost of a cyberattack affecting IT *and* OT systems[2]

$1M
Median ransomware payment in manufacturing[3]

40%
Of manufacturing breaches caused by exploiting known vulnerabilities[4]

THE NEW REALITY: THREE PRESSURES CONVERGING

Regulatory Mandate

The new **EU Machinery Regulation** takes effect **January 2027** with cybersecurity requirements for safety functions. The **EU Cyber Resilience Act (CRA)** follows in **December 2027**, banning non-compliant digital products. The **NIS2 Directive** imposes obligations directly on operators.

Operational Risk

Cyberattacks on production systems cause **unplanned downtime**, safety hazards, intellectual property theft, and reputational damage. Ransomware groups increasingly target OT systems directly.

Supply Chain Accountability

As supply chain scrutiny grows, enterprise customers demand **transparency into the security of every connected device**. Auditors are increasingly looking for security posture evidence — for your robots too.

THE BOTTOM LINE

Cybersecurity in industrial automation is no longer optional. Protecting **operational availability** and **operational resilience** requires equipment from a supplier that meets the highest security standards. An **IEC 62443-4 certified supplier** is a must. The good news: **Universal Robots is that supplier.**

[1] IBM X-Force Threat Intelligence Index, 2022–2026 [2] Ponemon Institute / Industrial Cyber, 2026 [3] Sophos, "State of Ransomware in Manufacturing," 2025 [4] IBM X-Force, 2026

2. The Gold Standard: IEC 62443-4

THINK OF IT AS...

IEC 62443-4 is like two complementary certifications: one for the **organization that builds the software** (is the development process secure?) and one for the **product itself** (does it have the right security features?). Together, they provide end-to-end assurance that security is built in — not bolted on.

IEC 62443-4-1 — SECURE DEVELOPMENT LIFECYCLE (The "How")

This standard certifies that the *development process* is secure — it does not certify the product itself (that is IEC 62443-4-2). Our **ML3 certification covers all of Teradyne Robotics** — one audited development process, applied consistently across every product line. The standard verifies security across **8 mandatory practices:**

1. **Security Management** — Governance, roles, and planning
2. **Security Requirements** — Threat modeling, risk assessment
3. **Secure by Design** — Defense-in-depth architecture
4. **Secure Implementation** — Secure coding, static analysis
5. **Verification & Validation** — Penetration testing, fuzzing
6. **Security Issue Management** — Vulnerability handling
7. **Security Update Management** — Secure patching
8. **Security Guidelines** — Hardening documentation

Maturity Levels (ML): How Rigorous Is the Process?

ML1	ML2	ML3	ML4
Initial	Managed	Defined	Improving
AD-HOC	DOCUMENTED	✓ UR CERTIFIED	OPTIMIZED

WHAT THIS MEANS FOR YOU

ML3 means every security practice is **planned, documented, independently audited, and demonstrably practiced the same way across the whole organization** — across all of Teradyne Robotics. It is a level of process discipline typically seen only in critical infrastructure sectors, and it places Universal Robots ahead of most industrial automation vendors.

✓ ML3 Certified — Teradyne Robotics, TÜV Rheinland (2026)

IEC 62443-4-2 — TECHNICAL SECURITY REQUIREMENTS (The "What")

This standard defines the security *features* the robot must have — its ability to identify users, protect data, resist attacks, and recover from incidents. It is organized into **7 Foundational Requirements:**

- **FR1 Identification & Authentication** — Verify who is accessing the system
- **FR2 Use Control** — Role-Based Access Control (RBAC)
- **FR3 System Integrity** — Software integrity verification, secure boot process
- **FR4 Data Confidentiality** — Encryption (TLS, SSH)
- **FR5 Restricted Data Flow** — Network segmentation and traffic control
- **FR6 Timely Response to Events** — Audit logging and alerting
- **FR7 Resource Availability** — Denial-of-Service protection

Security Levels (SL): How Strong Are the Defenses?

SL0	SL1	SL2	SL3	SL4
None	Basic	Advanced	High	Critical
MOST ROBOTS TODAY	→ UR TARGET 2027	→ UR FUTURE TARGET	SOPHISTICATED	STATE-SPONSORED

WHAT THIS MEANS FOR YOU

Most industrial robots today operate without any independently certified security features (effectively SL0). Universal Robots is engineering **PolyScope X** to meet **SL1 as a minimum** — meaning your robot can verify identities, protect its data, and resist common attack vectors. SL1 is the level that satisfies **EU CRA requirements**, ensuring your investment is regulation-ready. Beyond SL1, Universal Robots is targeting **SL2** for PolyScope X in the future, providing further protection against intentional attacks.

→ SL1 Target for PolyScope X — 2027

3. The EU Cyber Resilience Act (CRA)

The **Cyber Resilience Act (EU 2024/2847)** is the EU's landmark regulation requiring **all products with digital elements** — including industrial robots — to meet mandatory cybersecurity requirements before they can be sold in the European market. **The CRA applies to products placed on the market after December 11, 2027. Existing robots already in operation are not affected and can continue to operate.**

THINK OF IT AS...

The CE marking for cybersecurity. Just as products must meet safety standards to carry the CE mark, they will now need to meet cybersecurity standards too. Without compliance, products **cannot be placed on the EU market** after December 11, 2027 — but robots already deployed before that date can continue to operate without changes.

CRA ESSENTIAL REQUIREMENTS — MAPPED TO UNIVERSAL ROBOTS' APPROACH

CRA Requirement	What It Means	How Universal Robots Addresses It
No Known Vulnerabilities	Products must be delivered without known exploitable vulnerabilities	✓ Continuous vulnerability scanning, automated CVE monitoring
Secure by Default	Secure configuration out of the box — no default passwords	✓ PolyScope X: insecure protocols and services disabled by default, secure configuration out of the box
Vulnerability Handling	Documented processes to identify, fix, and disclose security issues	✓ IEC 62443-4-1 Practice 6 — certified vulnerability management
Secure Updates	Ability to apply security updates throughout product lifecycle	✓ PolyScope X: modular architecture enabling continuous security updates
Data Protection	Encryption of data at rest and in transit	✓ TLS/SSH encryption for critical communications, physical enclosure protection
Software Bill of Materials	Complete inventory of all software components for transparency	✓ Full SBOM maintained for PolyScope X

IEC 62443-4 AND PRESUMPTION OF CONFORMITY

The CRA allows manufacturers to demonstrate compliance through recognized standards. The European Commission has issued standardization request **M/606** to develop harmonized standards, with **IEC 62443-4** positioned as the key reference for industrial automation. Compliance grants a "**presumption of conformity**" — authorities accept the product as CRA-compliant without additional proof.

WHY THIS MATTERS FOR YOU

Presumption of conformity is your fast track through audits. Deploy IEC 62443-4-certified equipment and answer regulatory questions with an internationally recognized certificate — rather than costly custom assessments. Universal Robots' IEC 62443-4-1 certification (process) and our IEC 62443-4-2 target (product) directly support this pathway.

THE BROADER REGULATORY PICTURE

EU Machinery Regulation

The **Machinery Regulation (EU 2023/1230)** takes effect **January 20, 2027**, requiring protection of safety-relevant systems from **intentional corruption** including cyberattacks. **ISO 10218-1:2025** — the key robot safety standard — is being harmonized under this regulation.

NIS2 Directive

The **NIS2 Directive** imposes cybersecurity obligations on *operators* — including manufacturers classified as essential or important entities. **Universal Robots already complies with NIS2.** Choosing a NIS2-compliant, IEC 62443-4-certified supplier simplifies your own compliance.

Supply Chain Cascading

Under NIS2, **supply chain security** is mandatory. Large enterprises now cascade cybersecurity requirements to their equipment suppliers. Having independently certified robots means you can **satisfy audits with a certificate** rather than costly custom assessments.

WHAT THIS MEANS FOR YOU

The EU leads the world with the most comprehensive cybersecurity framework for industrial products — and the global trend is clear. The US, UK, Japan, Australia, Singapore, and South Korea have all introduced cybersecurity schemes for connected products. By building to the EU's rigorous standards, Universal Robots positions customers for compliance regardless of where they operate. **Universal Robots' compliance timeline:** Already **NIS2** compliant and **IEC 62443-4-1 ML3** certified across all of Teradyne Robotics. By 2026: **ISO 10218-1:2025** (PolyScope 5 & X) = **EU Machinery Regulation** compliant. By 2027: **IEC 62443-4-2 SL1** for PolyScope X = full **CRA** compliance. Every major regulation — covered, on schedule.

4. Universal Robots' Security Posture

Universal Robots doesn't treat cybersecurity as a checkbox — it is a core engineering discipline embedded in how we design, build, test, and maintain our products.

POLYSCOPE X: SECURITY BUILT INTO EVERY LAYER

Our next-generation software platform, **PolyScope X**, was architected from the ground up with security at its core. Here's how the 7 Foundational Requirements of IEC 62443-4-2 translate into real capabilities:

Req.	Capability	PolyScope X Target Implementation
FR1	Identity & Authentication	Password-protected access with configurable policies; individual user accounts targeted for SL2
FR2	Access Control	Role-Based Access Control (RBAC) with configurable permission levels
FR3	System Integrity	Software integrity verification, tamper detection mechanisms
FR4	Data Confidentiality	TLS-encrypted network traffic, SSH for remote access
FR5	Network Control	Configurable firewall rules, network segmentation support, minimal open ports
FR6	Event Monitoring	Audit logging of security-relevant events, exportable logs
FR7	Availability	Resource management, DoS mitigation, graceful degradation under load

> **TECHNICAL DEEP DIVE**
> PolyScope X runs on **Debian 12** (from April 2026) with a **modular architecture** that decouples application logic from the OS — enabling continuous security updates without disrupting robot operations. This is fundamentally different from legacy platforms where OS and application are tightly coupled.

COMPETITIVE POSITIONING

Universal Robots is among the first cobot manufacturers globally with **independent IEC 62443-4-1 certification** by **TÜV Rheinland**, now at **ML3** covering all of Teradyne Robotics, and is proactively engineering toward certified product security (IEC 62443-4-2). As part of **Teradyne Robotics** (parent of UR and MiR), we are also an authorized **CVE Numbering Authority (CNA)** — recognized by the global CVE Program to identify and catalog vulnerabilities.

COMPLIANCE ROADMAP

WHEN	MILESTONE	COVERS
2026	**IEC 62443-4-1 ML3** — Teradyne Robotics certified by TÜV Rheinland. One audited development process across all of Teradyne Robotics	✓ CERTIFIED
2026	**ISO 10218-1:2025** TÜV cert. for PolyScope 5 & X = EU Machinery Regulation compliant	= MACHINERY REG
2027	**IEC 62443-4-2 SL1** (CRA Compliance) for PolyScope X — Free PolyScope X update	= CRA COMPLIANT
Dec 11, 2027	**EU CRA enforcement** — Universal Robots ready **ahead of schedule**	EU DEADLINE

UNIVERSAL ROBOTS' SECURITY COMMITMENT

- ✓ IEC 62443-4-1 ML3 certified by TÜV Rheinland, covering all of Teradyne Robotics (certificate available on request)
- ✓ Authorized CVE Numbering Authority (CNA) for transparent vulnerability disclosure
- ✓ Security patches for up to **8 years** after a product's End of Life
- ✓ **Free** CRA compliance updates for all existing PolyScope X installations
- ✓ Complete Software Bill of Materials (SBOM) maintained for full transparency
- ✓ ISO 10218-1:2025 TÜV certification (PolyScope 5 & X) targeted 2026 — EU Machinery Regulation compliant
- ✓ Dedicated Product Security Incident Response capability

5. Product Compatibility

SOFTWARE PLATFORM OVERVIEW

Platform	Status	Operating System	Compatibility	CRA Compliant?
PolyScope X	**Future-Ready** Next-gen platform, secure by design. Modular architecture with continuous updates.	**Debian 12** (from April 2026) Designed for continuous OS updates with minimal impact on application.	e-Series & UR Series with **CB5.6**	**YES** Target: 2027
PolyScope 5	**Classic Main-Line** End of Sales: Dec 2027 (EU) / Summer 2028 (RoW). Maintenance support until 2036.	**Debian 8** Maintenance only. OS updates not feasible.	e-Series & UR Series (CB5.0–CB5.6)	**NO** See Section 6
PolyScope 3	**Legacy — End of Life** EOL since 2022.	**Debian 7** No updates available.	CB3 Series only	**NO** See Section 6

THINK OF IT AS...
PolyScope X is designed for easy, seamless, modular updateability — the operating system and application are decoupled, so security patches and OS upgrades can be applied without disrupting robot operations. PolyScope 3 and 5 are legacy embedded systems (firmware-like) where the OS and application are tightly coupled, making independent updates impractical. This is why PolyScope X is the path to a cyber-secure future.

HARDWARE PLATFORMS

Control Boxes

- **CB5.6** — Latest generation. Ships with PolyScope X. Required for CRA compliance path.
- **CB5.5** — Standard for PolyScope 5. Drop-in upgradeable to CB5.6.
- **CB5.0–CB5.4** — Legacy. Replaceable by CB5.5 or CB5.6.
- **CB3** — Legacy (EOL 2022). Incompatible with e-Series and UR Series robots and their PolyScope 5 and PolyScope X software.

Robots

- **UR Series** — Latest generation. Compatible with PolyScope X (with CB5.6) and PolyScope 5 (CB5.5 and CB5.6).
- **e-Series** — Compatible with PolyScope X (with CB5.6) and PolyScope 5 (CB5.0–CB5.6).
- **CB3 Series** — Legacy. Only compatible with CB3 control boxes.

6. Securing Legacy Equipment

For robots running PolyScope 3 or PolyScope 5 that cannot be upgraded — either due to compatibility or for practical reasons — we recommend a **Defense-in-Depth** strategy — multiple layers of protection so that if one layer fails, others remain in place.

> **THINK OF IT AS...**
> The medieval castle approach: a moat, a wall, a gate, and guards. If one layer is breached, the others still protect what's inside. Applied to your robot network, this means **isolation + firewall + port filtering + monitoring** working together.

> **IMPORTANT**
> The CRA applies to products placed on the market **after** December 11, 2027. Existing robots can continue to operate, but best practice is to secure all connected equipment regardless of regulation.

Step-by-Step Mitigation

1. **Trusted Devices Only:** Only connect trusted devices to the local network. Use only URCaps and scripts from trusted partners, verified for authenticity and integrity.
2. **Network Isolation:** Place the robot on a dedicated subnet, separated from office IT and internet access. No inbound connections from adjacent networks.
3. **Hardware Firewall:** Deploy a firewall between the robot subnet and other networks. Set the robot firewall to the most restrictive usable settings.
4. **Port Filtering:** Allow *only* the ports required for your specific integration (see table). Restrict outgoing connections to the smallest relevant set of ports, protocols, and addresses.
5. **Robot Setup:** Change the default password. Disable SSH when not needed. Disable "Magic Files" when not in use (PolyScope 5).
6. **Physical Security:** Restrict physical access to the teach pendant and USB ports.
7. **Monitoring:** Log network traffic to and from the robot subnet for anomaly detection.

Required Ports Reference

Service	Port(s)
Dashboard Server	29999
Primary, Secondary, RTDE, Matlab	30001–30004
Primary, Secondary, Matlab (Read-only)	30011–30013
Modbus TCP	502
EtherNet/IP	TCP/UDP 44818, UDP 2222
Profinet (incl. PROFIsafe)	UDP 8899, TCP/UDP 34962–34964
Interpreter Mode	30020
All other ports	**Block**

ROS/ROS2 and URCL use the above interfaces.
For full documentation see: docs.universal-robots.com

> **READY TO FUTURE-PROOF?**
> The most effective long-term strategy is to upgrade to **PolyScope X** with a CB5.6 control box. This gives you built-in security, continuous updates, and a clear path to CRA compliance. PolyScope 5-based robots (e-Series and UR Series) can be upgraded through a CB5.6 control box swap. Contact your Universal Robots representative to discuss upgrade options.

7. Frequently Asked Questions

Q: Do I need to replace my existing robots to comply with the CRA?
A: No. The CRA applies to products placed on the EU market *after* December 11, 2027. Existing robots can continue to operate. For improved cybersecurity, consider the suggestions in Section 6.

Q: Will PolyScope X compliance be available as a free update?
A: Yes. When PolyScope X achieves IEC 62443-4-2 SL1 certification (targeted 2027), all existing PolyScope X installations will receive a **free software update** for full CRA compliance.

Q: Why can't CB3 or PolyScope 5 robots be made CRA-compliant?
A: These platforms use tightly integrated, firmware-like software stacks on older operating systems (Debian 7 and 8). The OS and application cannot be separated or independently updated without breaking the system. This is a fundamental architectural limitation. However, **PolyScope 5-based robots (e-Series and UR Series) can be upgraded to PolyScope X through a CB5.6 control box upgrade**, enabling a path to CRA-compliant cybersecurity. CB3 robots cannot be upgraded due to hardware incompatibility.

Q: Will Universal Robots continue to support products after End of Life?
A: Yes. We provide critical safety and functionality patches for up to **8 years after a product's End of Life**. This ensures safe continued operation and spare part compatibility for your existing fleet.

Q: Is PolyScope X compatible with my existing e-Series robot?
A: Yes — e-Series robots equipped with a **CB5.6 control box** can run PolyScope X. If your e-Series currently has an older control box, a CB5.6 upgrade enables the transition.

Q: What does IEC 62443-4 certification actually prove?
A: IEC 62443-4-1 certification (process) proves that every stage of our software development — from design through testing to release — follows independently audited, repeatable security practices at ML3. IEC 62443-4-2 certification (product) proves the robot itself has specific, tested security capabilities. Both are verified by TÜV Rheinland, an independent third party.

Q: How does this compare to other cobot manufacturers?
A: Universal Robots is among the first collaborative robot manufacturers globally to hold independent IEC 62443-4-1 certification. The majority of cobot manufacturers have not yet achieved independent cybersecurity certification for their processes or products.

Glossary

IEC 62443-4-1: International standard for *secure product development lifecycle*. Certifies that the process used to build the software is secure.

IEC 62443-4-2: International standard for *technical security requirements*. Certifies that the product itself has the necessary security capabilities.

CRA (Cyber Resilience Act): EU regulation (2024/2847) requiring all digital products to meet cybersecurity standards. Applies to products placed on the market after Dec 11, 2027. Existing products can continue to operate.

NIS2 Directive: EU cybersecurity law imposing security obligations on operators of essential and important services, including manufacturers.

Defense in Depth: Layered security strategy (firewall + authentication + segmentation + monitoring) so that if one layer fails, others protect.

PolyScope X: Universal Robots' next-gen software platform. Modular, secure by design, with continuous update capability. The path to CRA compliance.

Maturity Level (ML): Measures process rigor. ML1 = ad-hoc, ML2 = managed & audited, ML3 = standardized across the organization, ML4 = continuously optimized.

Security Level (SL): Measures defense strength. SL1 = resists casual misuse, SL2 = simple attacks, SL3 = sophisticated attacks, SL4 = state-level threats.

SBOM: Software Bill of Materials — a complete inventory of all software components, enabling rapid vulnerability identification.

EU Machinery Regulation: EU 2023/1230, effective Jan 20, 2027. Replaces Machinery Directive. Includes cybersecurity requirements for safety-critical functions.

ISO 10218-1:2025: International safety standard for industrial robots, updated 2025. Being harmonized under the EU Machinery Regulation, including cybersecurity provisions.

RBAC: Role-Based Access Control — restricts system actions based on the user's role (e.g., operator vs. administrator).

Sources

[1] IBM, "X-Force Threat Intelligence Index," published annually 2022–2026. Manufacturing identified as the most-attacked sector for five consecutive years.

[2] Ponemon Institute, cited in Industrial Cyber, "Industrial CISOs Redefine Influence in 2026," February 2026. Average cost of dual IT/OT cyberattacks.

[3] Sophos, "The State of Ransomware in Manufacturing and Production," 2025. Median ransom payment of $1,000,000.

[4] IBM, "X-Force Threat Intelligence Index," 2026. Vulnerability exploitation as leading initial access vector (40% of incidents).

Ready to Secure Your Automation?

Contact your Universal Robots representative to discuss upgrading to PolyScope X, securing your existing fleet, or to request a copy of our IEC 62443-4-1 certificate.