Advisory Bulletin: Counterfeit PLCs

Issued: January 29, 2026

Overview

Programmable Logic Controllers (PLCs) are critical in water and wastewater operations. Counterfeit operational technology is increasingly surfacing due to long lead times and unauthorized online resellers. These devices pose safety and security risks. This bulletin provides guidance on identifying and mitigating risks associated with counterfeit Rockwell PLCs.

Key Risks

- ⚠️ **Increased Vulnerability:** Counterfeit devices often lack security updates and may contain backdoors, making systems more susceptible to cyberattacks and malware.
- ⚠️ **Reduced Reliability:** Authenticity issues can lead to frequent operational failures, disrupting water/wastewater processes.
- ⚠️ **Poor Quality Control:** Substandard components in counterfeit devices increase failure rates and reduce system longevity.
- ⚠️ **Lack of Support:** Counterfeit products lack warranties and manufacturer support, complicating troubleshooting and maintenance.

Recommendations

- ✅ **Validate Authenticity of Existing Technology:** Verify the authenticity of existing PLCs and critical Operational Technology (OT) through Original Equipment Manufacturer (OEM) channels.
- ✅ **Procure from Authorized Vendors:** Always purchase devices from verified suppliers or manufacturers to ensure authenticity. Implement strict procurement controls to prevent the introduction of counterfeit devices.
- ✅ **Develop Strong Procurement Controls:** Implement strict procurement controls to prevent the introduction of counterfeit devices.
- ✅ **Implement Rigorous Testing:** Conduct thorough inspections and functionality tests before deploying any new devices.
- ✅ **Register devices:** Register devices and verify warranty with OEM to ensure authenticity.

IDENTIFY A COUNTERFEIT DEVICE?

Report suspected counterfeit devices immediately to NHDES at dwcyber.erp@des.nh.gov

NHDES will reach out to NH's cyber partners to provide assistance.

Resources to Help Identify Counterfeits Already Deployed

Non-Vendor Specific Potential Indicators

Provenance and documentation gaps (or inconsistencies)

Missing or unverifiable certificates of authenticity, chain-of-custody, and traceable serial/lot codes are the first red flag. In a recent New Hampshire case, a routine firmware update failed, OEM serial-number verification flagged the unit as counterfeit, and no certificate or chain-of-custody existed—then the device was destroyed before forensics.

OEM guidance is clear: unauthorized/gray-market sources commonly relabel used/refurbished parts as "new," with packaging/label anomalies (fonts, logos, barcodes, date/lot codes). If the supplier isn't on the authorized partner list, treat the device as suspect.

Firmware integrity anomalies (update/validation problems)

Counterfeits frequently **refuse or fail legitimate OEM firmware updates**, present unsigned/altered firmware, or show identity errors in diagnostics. Some vendors now embed **counterfeit-detection in firmware**—devices may error out or even disable when tampering is detected.

Label and packaging audit

Photograph and compare **label fonts, logos, date/lot codes, barcodes** to OEM exemplars; discrepancies, missing OEM security features, and spelling errors are common.

Allen-Bradley®, FactoryTalk®, and Rockwell Automation® Specific Guidance

Do your PLCs have security features to identify counterfeits? Check Your Product Labels.

Information from Rockwell Automation on the Gray Market

Rockwell Automation Parter Locator

For "Gray Market"-related matters at Rockwell Automation: graymarket@ra.rockwell.com.

Gray market purchases refer to the buying and selling of products outside of the manufacturer's authorized channels. These products are often sold at lower prices than their authorized counterparts, but they may come with trade-offs such as warranty issues, lack of after-sales support, and potential legal risks.