Iranian-affiliated APT actors reached internet-exposed PLCs at US water, energy, and government facilities, extracted the project files, and pushed altered logic back onto the controllers. The changes overrode safety instruction sets and disabled alarms, leaving operators with normal readings on their displays.

BOTTOM LINE

- The advisory identifies no new product vulnerability. Access was opportunistic, against exposed and misconfigured devices.
- Copia covers each code-integrity and recovery mitigation in the advisory. Internet exposure, MFA, and modem hardening remain as part of network architecture.

Advisory Finding → What Closes the Gap

SOURCE: AA26-097A

	WHAT THE ADVISORY FOUND	HOW COPIA MITIGATES IT
01	**BACKGROUND INFORMATION** NEW 22 JUL 2026 At one US victim, actors downloaded a malicious project file to a PLC using configuration software. The file kept the ladder logic needed for downstream function, then *added logic that overrode specific instruction sets* responsible for maintaining safe operating parameters.	VERSION CONTROL · DRIFT DETECTION **Copia sees the addition even though the process still runs.** The code is compared to its approved baseline, so logic added alongside valid rungs alerts as a change.
02	**IMPACT · MITRE T1565 · DATA MANIPULATION** After exfiltrating project files, FBI and CISA identified modification and deletion of project file logic, including Add-On Instructions, along with manipulated HMI and SCADA displays. The changes *disabled critical shutdown and alarm logic*, letting systems reach unsafe conditions without notifying operators of the anomalies.	DRIFT DETECTION · CHANGE HISTORY **Copia names what changed, when, and who changed it.** AOIs and reusable modules are versioned, so a modified or removed interlock appears as a reviewable diff with an audit trail of what changed.
03	**MITIGATIONS · FOLLOW-UP STEPS** NEW 22 JUL 2026 Review project files running on PLCs for unauthorized changes. Use integrity checking tools and *visually compare the running program to known good logic*. Validate reusable logic and I/O configuration. When restoring, verify the backup does not itself contain malicious logic.	VERSION CONTROL · LAST KNOWN GOOD **Copia performs this review automatically, fleet-wide.** Running code is compared to baseline without an engineer opening each project, and the stored version predating the intrusion window is identified before you restore.
04	**MITIGATIONS · IMMEDIATE STEPS** NEW 22 JUL 2026 Before returning a controller to run mode, review and validate the project file. Changing modes *will lock in the current project file downloaded to the device*.	VERSION CONTROL · DRIFT DETECTION **Copia confirms the correct file at the keyswitch.** Technicians confirm the running project against the approved version in moments, not by searching a share drive while the process waits.
05	**MITIGATIONS · FOLLOW-UP STEPS** Create and test strong backups of PLC logic and configurations. Store backup files offline and secure the physical removable media *to enable fast recovery.*	BACKUPS · LAST KNOWN GOOD **Copia is the backup and recovery system for PLC code.** Automated, versioned, verifiable, restore-ready backups across all vendor PLCs. Recovery becomes a scheduled job.

THE COPIA CAPABILITIES APPLIED ABOVE

BACKUPS
Automated, versioned, verifiable, restore-ready backups of your PLC code.

VERSION CONTROL
Know when a running version no longer matches the original operating state, and which version is the baseline.

DRIFT DETECTION
Pinpoint when changes were made to the code, and how to get back to the baseline.

LAST KNOWN GOOD
Removes the hunt for the last known good version while the clock is running.