STATUS: NOMINAL PUMP_01: RUN ALARM: DISABLED SAFETY_AOI: ******

THE LOGIC LOOKED FINE

Reversing safety-system bypass in critical infrastructure PLCs

Amanda Kollmorgan · Security Architect, Veolia North America

Built entirely from public CISA / FBI / NSA reporting · Level 300

THE PREMISE

No zero-day. They logged in like a technician.

01

Exposed

Internet-facing PLCs, found by port and banner. Locating them took no exploit at all.

`Shodan-class discovery`

02

Authenticated

The vendor's own engineering software, reached with default or weak credentials.

`Studio 5000 · EcoStruxure · TIA Portal`

03

Surgical

Project files pulled off the device, safety logic rewritten, reloaded to the live PLC.

`AOIs modified · shutdowns + alarms off`

The break-in barely qualifies as one. What this talk takes apart is the tampering that came after, confirmed across water, energy, and government-services victims in several US states, some with real operational disruption and financial loss.

PRIMER, FAST

What an Add-On Instruction actually is

PLC the small industrial computer driving pumps, valves, and dosing.

Ladder logic the program. Reads like relay rungs; this is what an operator or integrator inspects.

AOI a reusable, encapsulated code module that gets written once and then trusted without anyone reopening it.

WHY IT'S THE PERFECT HIDING PLACE

An AOI gets treated like a sealed vendor component, so whoever reviews the program reads the rungs that call it rather than the logic inside. **That trust is the whole problem:** one tampered module can reach many processes at once, and the ladder logic calling it still looks completely normal.

THE CHAIN

Exposure to loss-of-view, end to end

Discover

Scan for exposed PLCs; identify by port and vendor banner.

Access

Log in via engineering software; default / weak creds.

Exfiltrate

Pull the device project file to actor infrastructure.

Tamper

Rewrite AOIs: disable safety shutdowns and alarms.

Mask

Reload; HMI shows green while conditions go unsafe.

MITRE ATT&CK for ICS mapping on the next slide. The whole chain is documented in AA26-097A.

MAP IT

Technique and detection surface

MITRE ATT&CK

T1041	Exfiltration over C2 / actor infra
T1565	Data manipulation (project file, HMI)
Impair	Disable safety / alarm response
Modify	Project file logic + AOIs

WATCH THESE PORTS

44818	EtherNet/IP
502	Modbus
102	S7comm
2222	SSH (OT)
22	Modem SSH (Dropbear persistence)

MONDAY MORNING

The defense you can actually run

Baseline & diff

Compare running logic to a known-good project file, with real attention to AOIs and safety routines.

`Vendor integrity tools · alert on AOI change`

RUN-mode discipline

Keep controllers in RUN; drop to PROGRAM only inside an authorized maintenance window.

`Log every mode change`

Kill the exposure

Take PLCs off the public internet; broker remote access through a monitored gateway.

`No 44818 / 502 / 102 inbound · MFA at gateway`

Architect for the weak

A device that can't authenticate gets protected by whatever sits in front of it.

`Segmentation · conduits · brokered access`

WHAT'S COMING

August 2026: the attackers picked up AI

NSA, FBI and partners warned that actors targeting Siemens S7 PLCs are using **AI-assisted development** to produce working exploitation scripts, **disguised as legitimate monitoring tools.**

What it changes for defenders

It shortens the timeline. Exploit code that used to take real skill now comes together faster, which narrows the gap between a device going exposed and someone weaponizing it, and tooling built to pass as ordinary monitoring is harder to catch. **What it doesn't touch is the fix.** Cut the exposure and validate integrity, and the chain still breaks regardless of who or what wrote the script.

STATUS: NOMINAL PUMP_01: RUN ALARM: ENABLED SAFETY_AOI: VERIFIED

Make the logic tell the truth.

Validate what's running against a known-good baseline, cut the exposure, and watch the ports the advisories name. Trust the module you verified, not the one you inherited.

Amanda Kollmorgan · Sources: CISA/FBI/NSA AA26-097A and the August 2026 S7 advisory, all public.

ATT&CK for ICS mapping

Advisory AA26-097A maps to the Enterprise matrix; below are the ICS-matrix equivalents for the same behavior.

ACCESS	**T0883** Internet Accessible Device **T0812** Default Credentials **T0886** Remote Services
COLLECT	**T0845** Program Upload (exfiltrate project file)
IMPAIR	**T0843** Program Download **T0889** Modify Program **T0821** Modify Controller Tasking **T0838** Modify Alarm Settings **T0878** Alarm Suppression
DECEIVE	**T0856** Spoof Reporting Message
IMPACT	**T0829** Loss of View **T0880** Loss of Safety