BLACKSWAN CYBERSECURITY

# THREAT ADVISORY
# Iranian-Affiliated Cyber Operations Targeting U.S. Water, Energy, and Critical Infrastructure Sectors

**July 27, 2026**

## Executive Summary

U.S. federal agencies (FBI, CISA, NSA, DOE, EPA, Treasury, and U.S. Cyber Command) have issued multiple warnings in 2026 regarding an ongoing campaign by Iranian-affiliated threat actors targeting Operational Technology (OT), Industrial Control Systems (ICS), and Programmable Logic Controllers (PLCs) within U.S. critical infrastructure. The campaign appears focused on creating disruptive effects rather than traditional intelligence collection. Victim organizations have reportedly experienced operational disruptions and financial losses.

The activity is particularly concerning because threat actors have moved beyond basic web application compromise and are directly interacting with PLC project files, HMI displays, SCADA environments, and controller programming logic. Federal agencies reported at least one incident where attackers altered PLC programming to disable critical shutdown and safety alarm functions, potentially allowing unsafe operating conditions without operator awareness.

The latest July 2026 advisory expands observed targeting beyond Rockwell Automation devices to Schneider Electric and Siemens PLC platforms, indicating a broader campaign against industrial automation technologies used throughout the Water/Wastewater, Energy, and Municipal sectors.

---

## Threat Actor Assessment

### Primary Attribution

The activity has been attributed by U.S. government agencies to Iranian-affiliated Advanced Persistent Threat (APT) actors. Several sources connect the activity to actors associated with:

- CyberAv3ngers
- Shahid Kaveh Group
- Iranian Revolutionary Guard Corps (IRGC) Cyber Electronic Command (CEC)
- Handala (separate but related Iranian-aligned operations)

### Strategic Objective

Federal agencies assess that these operations are intended to:

- Create disruptive effects inside the United States
- Impact on critical infrastructure operations
- Generate economic and public confidence impacts
- Demonstrate retaliatory cyber capabilities amid ongoing geopolitical tensions involving Iran, Israel, and the United States

---

# THREAT ADVISORY
# Iranian-Affiliated Cyber Operations Targeting U.S. Water, Energy, and Critical Infrastructure Sectors

**July 27, 2026**

## Affected Sectors

Confirmed and observed targeting includes:

| Sector | Status |
|---|---|
| Water & Wastewater | Confirmed |
| Energy | Confirmed |
| Government Services & Municipalities | Confirmed |
| Industrial Manufacturing | Potential |
| Utilities | Confirmed |
| Critical Infrastructure Broadly | Confirmed |

---

## Targeted Technologies

### Operational Technology

#### PLC Vendors Identified

- Rockwell Automation / Allen-Bradley
- Schneider Electric
- Siemens
- Potentially additional PLC manufacturers

#### Specific Product Families Referenced

- CompactLogix
- Micro850
- Schneider Modicon M340 (BMX P34)
- Siemens S7-1200

#### Associated Technologies

- SCADA systems
- HMI systems
- Engineering Workstations
- PLC Programming Software
- Remote Management Infrastructure

---

# THREAT ADVISORY
# Iranian-Affiliated Cyber Operations Targeting U.S. Water, Energy, and Critical Infrastructure Sectors

**July 27, 2026**

## Observed Tactics, Techniques, and Procedures (TTPs)

### MITRE ATT&CK for ICS Mapping

#### Initial Access

**T0819 – Exploit Public-Facing Application**

Attackers specifically targeted internet-connected OT assets and exposed PLC management interfaces.

**T0886 – Remote Services**

Use of remote access methods to directly access PLC environments and engineering workstations.

---

#### Execution

**T0831 – Modify Controller Tasking**

Threat actors altered PLC programming logic.

Observed behavior included:

- Modification of project files
- Logic manipulation
- Control process alteration

---

#### Impair Process Control

**T0836 – Modify Parameter**

Attackers manipulated operational settings and displayed values within HMI/SCADA systems.

---

#### Inhibit Response Function

**T0814 – Denial of Control**

One reported intrusion involved altering controller logic so that safety shutdown and alarm mechanisms would no longer trigger properly.

---

#### Discovery

Threat actors probed OT protocols associated with multiple vendors, including:

- EtherNet/IP
- PROFINET
- Modbus

---

## Indicators of Compromise (IOCs)

The public advisory contains additional IOC data that should be imported directly from the CISA bulletin. Based on the available reporting, the following indicators and artifacts have been publicly identified.

# THREAT ADVISORY
# Iranian-Affiliated Cyber Operations Targeting U.S. Water, Energy, and Critical Infrastructure Sectors

**July 27, 2026**

## Network Indicators

### PLC Communication Ports

Monitor for unauthorized external traffic involving:

| Protocol | Port |
|---|---|
| EtherNet/IP | 44818 |
| EtherNet/IP I/O | 2222 |
| Siemens S7 | 102 |
| Modbus/TCP | 502 |

---

### Remote Access Indicators

Observed infrastructure included:

- RDP running on TCP 43589
- External access from foreign hosting providers
- Engineering workstation-based attacks

---

### Host Indicator

Reported workstation certificate:

Common Name:
**DESKTOP-BOE5MUC**

---

### Protocol Exposure

Additional services observed on attacker infrastructure:

- TCP/135 (DCERPC)
- MSMQ
- NetBIOS

---

## Handala / Cal Water Incident Assessment

Another Iranian-linked operation involved Handala's claim to have compromised California Water Service (Cal Water).

## What Was Claimed

Handala claimed:

- Access to Cal Water systems

- Ability to disrupt water supply
- Theft of approximately 5 GB of information

## Investigation Findings

Mandiant's investigation reportedly found:

- No evidence of compromise within OT environments
- No evidence of compromise within internal enterprise networks
- Activity limited to:
    - Third-party service provider platforms
    - Compromised user accounts

## Strategic Assessment

This event demonstrates a recurring pattern observed with some Iranian-aligned operations:

- Public influence messaging
- Exaggerated capability claims
- Information operations combined with actual cyber intrusions

Organizations should treat claims of OT access seriously but validate operational impacts through forensic investigation rather than relying solely on adversary statements.

---

## Risk Assessment

| Threat Area | Risk |
|---|---|
| Internet-Exposed PLCs | Critical |
| Direct OT Internet Connectivity | Critical |
| Weak Remote Access Controls | High |
| Engineering Workstations | High |
| Unvalidated PLC Project Files | High |
| Legacy Water Infrastructure | High |
| Vendor Remote Support Channels | Medium-High |

---

## Recommended Defensive Actions

### Immediate (0–7 Days)

#### Remove Direct Internet Exposure

Federal agencies specifically recommend:

- Removing PLCs from direct internet access
- Eliminating inbound control-system exposure

### Review Firewall Rules

Block inbound access to:

- 44818
- 2222
- 102
- 502

from untrusted networks and foreign sources.

### Threat Hunt

Search logs for:

- Connections to exposed PLCs
- Unexpected engineering workstation activity
- Foreign-hosted IP communications
- Configuration changes to PLC project files

---

## Near-Term (30 Days)

### Validate Engineering Workstations

Monitor:

- Studio 5000 activity
- PLC download events
- Logic changes
- Firmware uploads

### OT Segmentation

Implement:

- Purdue Model segmentation
- Industrial DMZs
- One-way monitoring where feasible

### MFA for All Remote Access

Especially:

- Vendor access
- Integrator access
- Engineering systems

- Jump hosts

---

# Strategic (90+ Days)

## Deploy OT Security Monitoring

Recommended solutions include:

- Claroty
- Nozomi
- Dragos
- Microsoft Defender for IoT

## Establish PLC Integrity Monitoring

Monitor for:

- Logic modification
- Unauthorized project downloads
- Safety function changes
- Alarm suppression

## Conduct OT Incident Response Exercises

Include scenarios involving:

- Water treatment interruption
- PLC tampering
- SCADA data manipulation
- Safety alarm suppression

---

# Executive Takeaway

The most significant aspect of this campaign is not simply that Iranian actors gained access to industrial systems; it is that federal agencies have documented attempts to manipulate PLC logic, falsify operator displays, and disable safety functions. This represents a progression from nuisance activity and hacktivism toward disruptive OT operations capable of affecting public services and critical infrastructure. Organizations operating in water, wastewater, energy, municipal, and industrial environments should treat internet-exposed PLCs as a priority risk area and immediately validate segmentation, remote access controls, and PLC integrity monitoring capabilities.

Need Assistance or Want to Discuss Further?
Contact Blackswan Cybersecurity at 855-BLK-SWAN or Contact@BlackswanCybersecurity.com