The Post-Mortem.

Anatomy of a Critical Infrastructure Breach and the Prescription for Recovery.

An analysis of the Aliquippa, PA, and Muleshoe, TX, water system attacks.

The Attacks Were Not Sophisticated. The Failures Were Foundational.

Key Finding 1

- **Who:** Nation-state affiliated actors (Cyber Av3ngers - Iran, CARR - Russia)
- **Where:** Critical water systems in Aliquippa, PA, and Muleshoe, TX
- **How:** "Simple Means"—scanning public internet for vulnerable devices with default credentials

Key Finding 2

- **The Impact:** Physical consequences, including a tank overflow in Muleshoe and defaced HMIs threatening water safety.

These incidents represent a critical failure at the most foundational layer of cybersecurity: **Maturity Level 1 (Basic).**

Our Diagnostic Framework: Measuring OT Cybersecurity Maturity

We will analyze each failure through this framework. The diagnosis for the recent attacks is a systemic failure to meet even the most basic requirements of Level 1, leaving critical systems completely exposed.

The Diagnosis

Three Critical Failures of Basic Cyber Hygiene

Diagnosis 1: Acute Network Exposure

The Evidence:

- **Aliquippa:** Unitronics PLCs were directly exposed to the public internet.
- **Muleshoe:** HMI was remotely accessible, allowing attackers to overflow a tank.

Maturity Assessment (Process 2 - Segmentation):

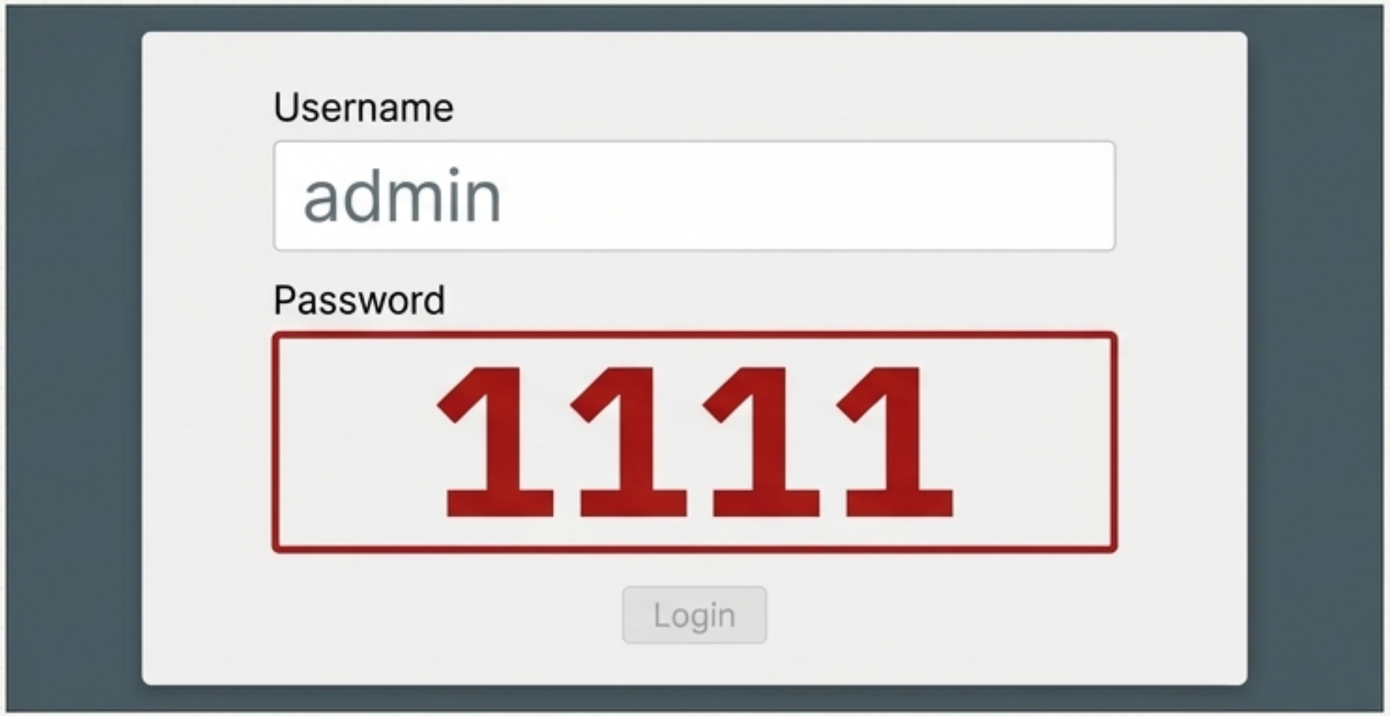
Current State: Level 1 (Basic). A "flat" network with no separation between the internet and the physical control layer.

The Lesson: PLCs and HMIs must **never** be internet-facing. A **Level 2 (Intermediate)** maturity requires an Industrial Demilitarized Zone (IDMZ) and a firewall blocking all inbound internet traffic to the OT network.

IEC 62443 Violation:
This violates the fundamental "Zones and Conduits" model. Critical assets were placed in an "Untrusted Zone" (the Internet).

Diagnosis 2: Chronic Access Control Negligence

Default Password in Use: “1111”



Maturity Assessment (Process 3 - Access Control)

Current State: Level 1 (Basic) (in crimson #B71C1C). The utility relied entirely on default vendor configurations. Security by Obscurity failed.

The Lesson: Level 2 (Intermediate) (in amber #F57F17) maturity mandates that default accounts are disabled and unique, complex passwords are enforced for all devices upon commissioning.

IEC 62443 Security Level (SL) Failure

Result: Failed to meet SL-1 (in crimson #B71C1C) (protection against casual violation).
Requirement: This attack required only SL-2 (in slate blue #455A64) (protection against against intentional violation using simple means) to defeat.

Diagnosis 3: Supply Chain & Geopolitical Blindness

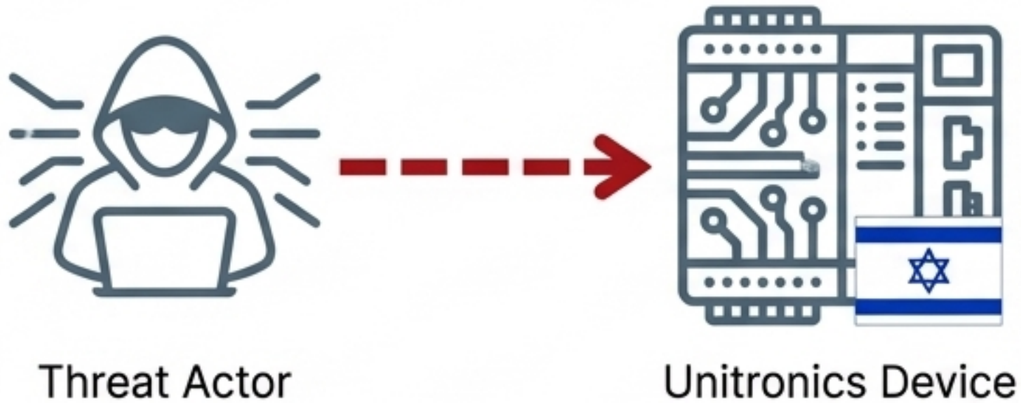
The Evidence:

- **Targeting Logic**: Attackers (Cyber Av3ngers) explicitly targeted Unitronics devices because they are **manufactured in Israel**.
- **On-Screen Message**: HMIs were defaced with political messages (‘**Down with Israel**’).

Maturity Assessment (Process 16 - Supply Chain Risk):

Current State: Level 1 (Basic) The PLC was viewed as a “dumb device,” not a potential political target.

The Lesson: In the modern threat landscape, your hardware's origin can make you a target. **Level 3 (Advanced)** maturity requires active Supply Chain Risk Management (SCRM) to understand the provenance and geopolitical risks of your technology.



The Prescription

A Phased Roadmap for Immediate Hardening and Long-Term Resilience

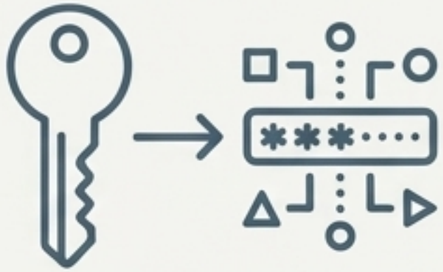
Phase 1: Emergency Hardening

Timeline: Weeks 1-2

Goal: Remove the target from the public eye.

1. Disconnect from Internet (Process 2)

- **What:** Immediately physically disconnect ethernet cables linking PLCs/HMIs to any external modem.
- **Why:** Stops the attack vector instantly. PLCs do not need to talk to the internet to pump water.



2. Password Reset Campaign (Process 3)

- **What:** Change the password on every PLC and HMI from the default to a complex string. Disable default admin accounts.
- **Why:** Prevents re-entry if the network is ever re-connected.

3. Search for 'Shadow Assets' (Process 1)

- **What:** Use a tool like Shodan.io to scan your own public IP range.
- **Why:** Discover if other devices (cameras, pumps, sensors) are visible to the public internet without your knowledge.

Phase 2: Secure Remote Access

Timeline: Months 1-3

Goal: Allow for necessary maintenance without creating exposure.

1. Implement VPN/SRA with MFA (Process 4)

What: If remote access is a requirement, install a firewall with a VPN Concentrator. Mandate Multi-Factor Authentication (MFA) for all remote logins.

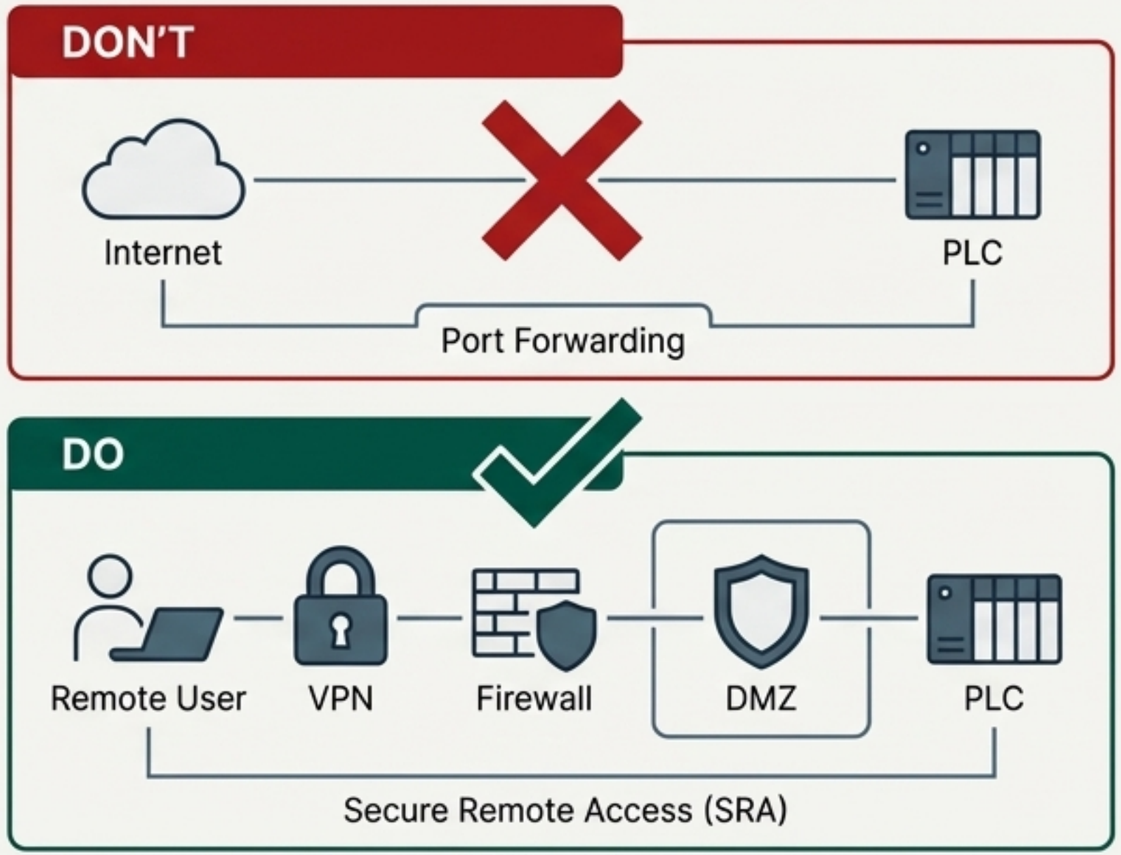
Why: Creates an encrypted, authenticated, and controlled tunnel for remote access, preventing direct exposure.

2. Cybersecurity Awareness Training (Process 15)

What: Train all operators and technicians on the specific risks of internet connectivity.

"If a vendor asks to put a device on the internet for 'easy maintenance,' the answer is NO." Teach staff that convenience often equals vulnerability.

Critical Detail Visual



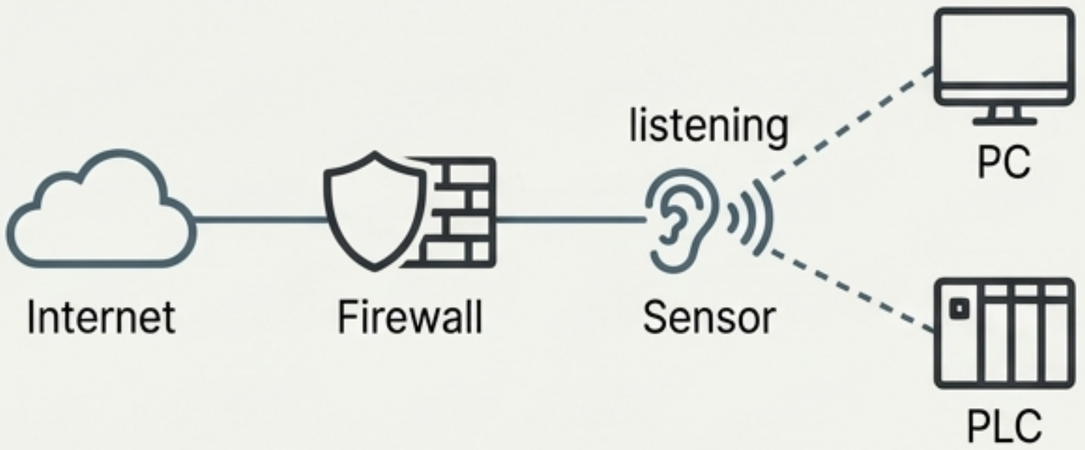
Phase 3: Resilience & Monitoring

Timeline: Months 3-6

Goal: Be able to detect the next attempt and ensure operational continuity.

1. Deploy Passive Monitoring (Process 10)

- **What:** Install a network sensor (e.g., Dragos, Nozomi) behind the new firewall to monitor internal OT traffic.
- **Why:** You need to know if an attacker has bypassed your perimeter defenses. A Level 3 maturity system would alert you if a PLC suddenly communicates with an IP address in Russia or Iran.

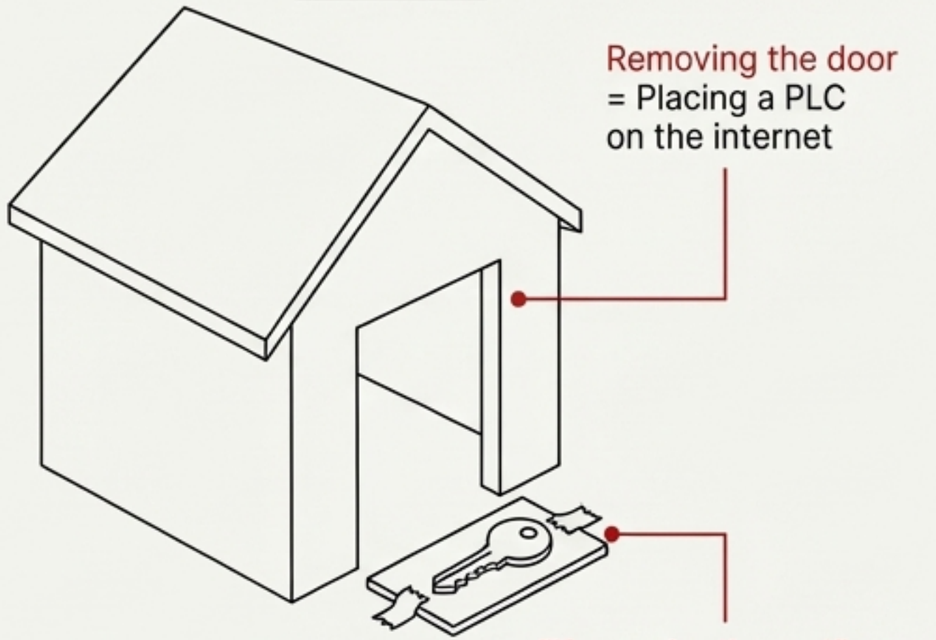


2. Manual Override Drills (Process 11)

- **What:** Regularly schedule and conduct drills to verify that the 'Manual Mode' for pumps and other critical functions actually works and that staff are proficient in using it.
- **Why:** In Aliquippa, operators had to switch to manual operations. Drills ensure that if control screens are defaced or disabled again, essential water service continues without interruption.

This Was Not a Master Locksmith Picking a Complex Lock.

THE PROBLEM



THE SOLUTION

The immediate lesson is not about buying expensive AI tools.
It is about putting the door back on its hinges and keeping the key in your pocket.