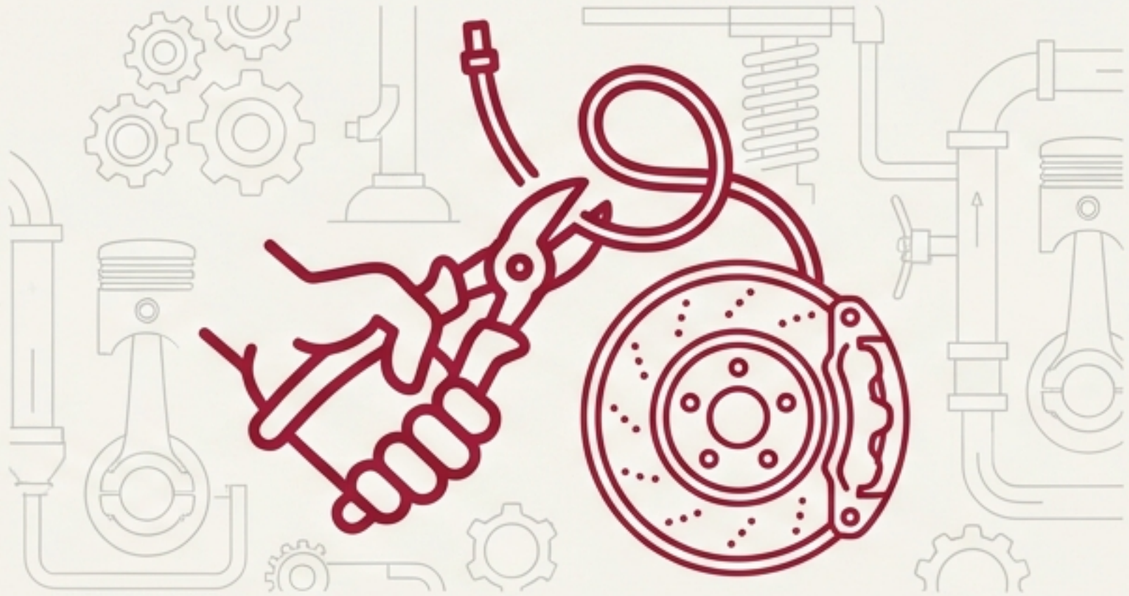
Some Threats Steal Your Valuables. Others Cut Your Brakes.

DATA THEFT



PHYSICAL SABOTAGE

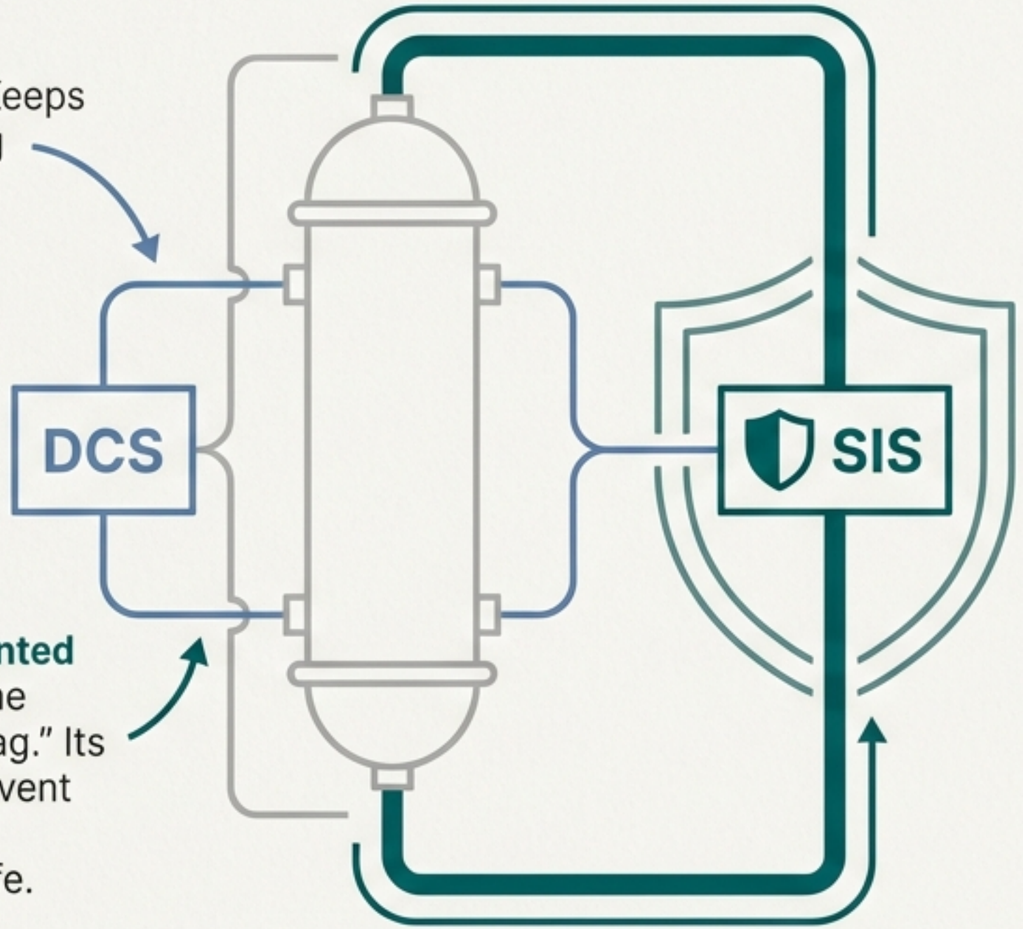
A standard ransomware attack is a burglar. They break into your house to steal the TV. The goal is financial gain through disruption and data theft. This is a known risk we manage.

The Trisis attack was different. It was a mechanic breaking into your garage, not to steal the car, but to silently cut the brake lines. The goal is catastrophic physical failure.

- **We are not defending against theft. We are defending against an attack on physical safety and integrity.**

The Target Was The Last Line of Defense

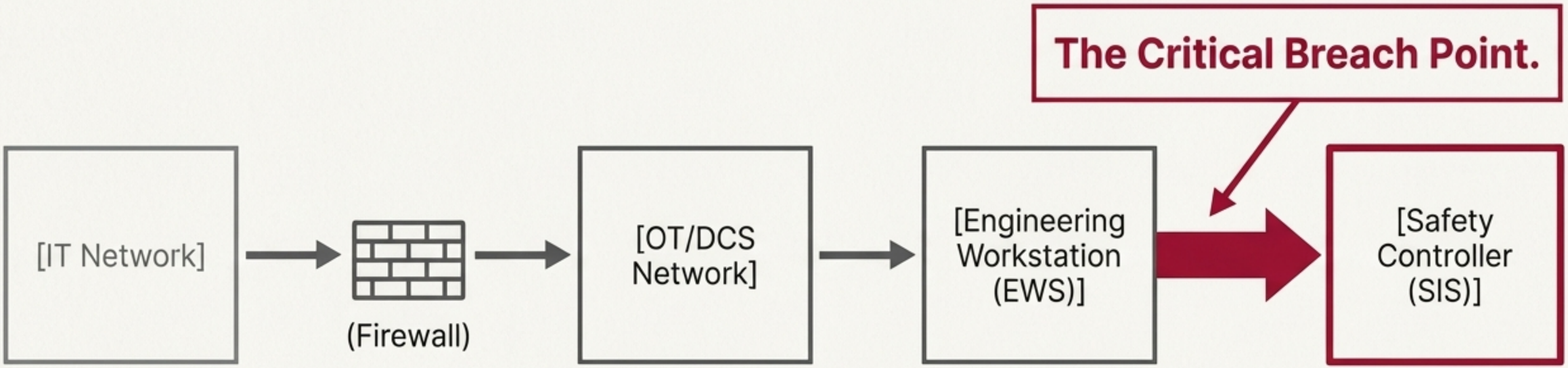
Process Control System (DCS): Keeps the plant running efficiently.



Safety Instrumented System (SIS): The automated "airbag." Its only job is to prevent explosions and protect human life.

- The **Trisis** attackers, attributed to a **Russian government research institute**, did not **target** our business systems or even our primary process control network.
- They targeted the **Safety Instrumented System (SIS)**—the independent, **failsafe** system designed to shut down a plant before a **catastrophic failure** occurs.
- This is the fundamental difference between an **IT attack** on data *availability* (like the Ascension ransomware case) and an **OT attack** on physical *integrity*.

The Path to Catastrophe Bypassed Our Standard Defenses



- The attack began with a standard entry point, likely phishing, on the corporate IT network.
- From there, the attackers moved laterally into the plant's process control network (OT/DCS).
- The critical failure was their ability to then access the Engineering Workstation (EWS) connected directly to the Schneider Electric Triconex safety controllers.
- This path demonstrates that the most sensitive system in the plant was accessible from less secure network layers.

Diagnosis #1: The Safety Zone Was Violated

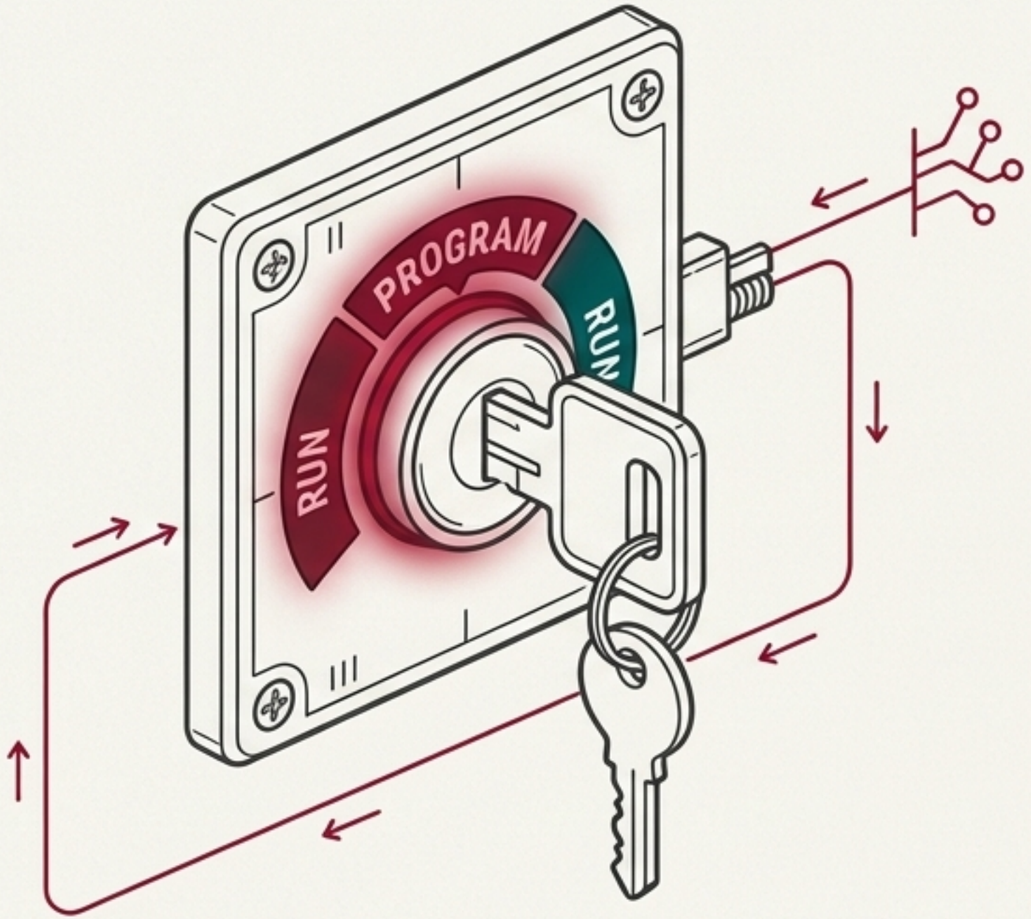
What Happened

Attackers moved freely from the process control network to the safety network.

The Diagnosis (Maturity & Standards View)

- **Current State (Maturity Level 2)**: The SIS was treated as just another part of the OT network.
- **Required State (IEC 62443-3-2)**: The SIS must exist in its own dedicated **Safety Zone**. The 'Conduit' (network path) into this zone must be the most restricted in the entire plant.
- **Security Level Mismatch**: This was a nation-state **SL-4 attack** (intent to sabotage), but our defenses were at **SL-1/SL-2**, designed to stop basic threats.

Diagnosis #2: The “Keys to the Kingdom” Were Left in the Ignition



What Happened

The attackers used the Engineering Workstation to inject malicious logic directly into the safety controller’s memory.

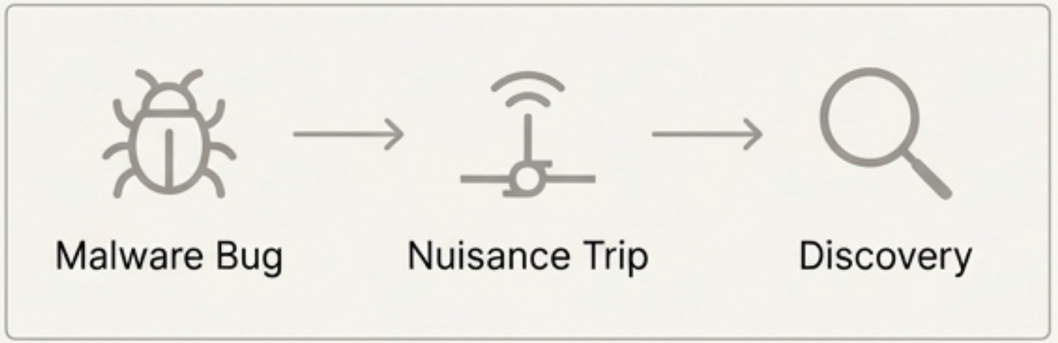
The Diagnosis (Physical & Procedural Failure)

The Triconex controller has a **physical key switch**. When this key is in the ‘RUN’ position, remote programming is **physically impossible**. The circuit is open.

The attack only succeeded because the key was left in ‘PROGRAM’ mode, likely for convenience. This is a critical failure of physical security and operational procedure (Configuration Management).

• **Maturity Lesson**: In an advanced security model, the safety EWS is disconnected from the network and the key is locked in ‘RUN’ mode except during planned, authorized maintenance windows.

Diagnosis #3: The Attack Was Discovered by Accident



What Happened

We did not detect the attackers compromising the EWS or uploading new firmware to the safety controller. The attack was only found because a bug in their own malware caused a safe shutdown of the plant (a 'nuisance trip').

The Diagnosis (Monitoring Blind Spot)

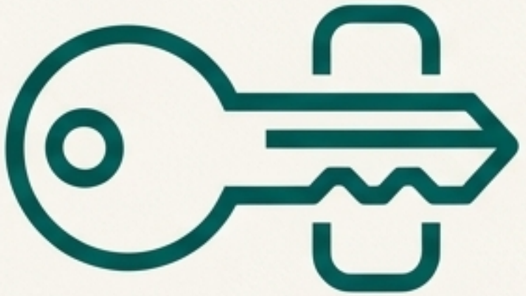
- Our monitoring tools were blind to the proprietary **'TriStation' protocol** used by the safety controllers. We could not see the 'Firmware Write' command being executed.
- **Maturity Lesson:** Relying on attacker incompetence is not a strategy. **Level 4 Maturity** requires deep packet inspection (DPI) capable of decoding proprietary safety protocols to provide high-fidelity alerts on any unauthorized configuration changes.

The Prescription: An Action Plan for SL-4 Resilience

- Based on our diagnosis, a targeted action plan is required to defend against a state-level (SL-4) threat like Trisis.
- The strategy focuses on building layers of defense, starting with physical hardening and strict isolation, followed by advanced monitoring.
- This is our roadmap to making a repeat of this attack impossible in our environment.

Phase 1: Physical Hardening (Immediate)

Goal: Make Remote Manipulation Physically Impossible



Action 1: Enforce the ‘Physical Key’ Policy.

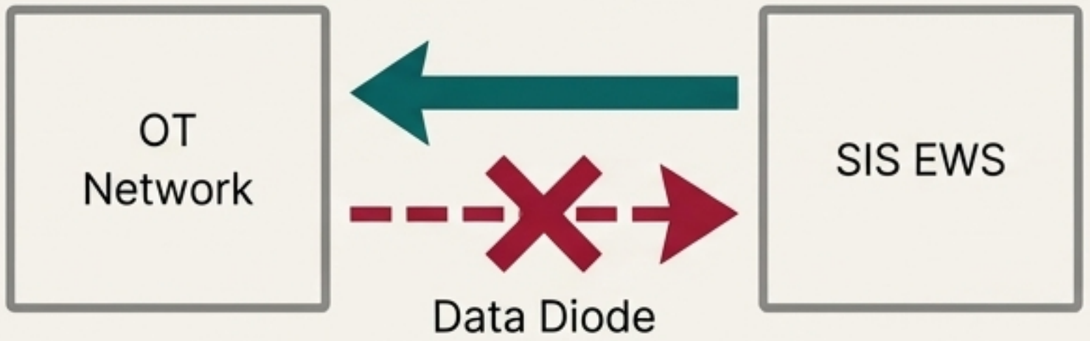
- **What:** Audit all SIS controllers. Turn physical keys to **‘RUN’** or **‘LOCKED’** mode. Implement a formal check-out procedure for the key.
- **Why:** This creates a hardware-level air gap. Even with full network access, an attacker **cannot** write to the controller if the physical circuit is open.

Action 2: Verify Failsafe Logic.

- **What:** Review and confirm the ‘Safe State’ configuration in all SIS controllers.
- **Why:** The Trisis malware bug caused a safe shutdown. We must ensure our systems are configured to do the same—to trip the plant if they detect internal corruption, failing safely rather than dangerously.

Phase 2: Segmentation & Access Control (Months 1-3)

Goal: Build an Impenetrable Safety Zone



Action 1: Harden the Engineering Workstation.

- **What:** Disconnect the SIS Engineering Workstation from the main OT network. If one-way data flow is needed (for historians), implement a **Data Diode**.
- **Why:** This enforces the 'Safety Zone' concept from **IEC 62443**, making the SIS the highest-integrity, most isolated zone in the plant.

Action 2: Implement Dedicated MFA for Engineering Access.

- **What:** Require a separate, hardware-based multi-factor authentication token for any login to the SIS EWS.
- **Why:** This prevents the use of compromised corporate credentials to access the most critical engineering terminal.

Phase 3: Advanced Detection (Months 3-6)

Goal: Achieve Full Visibility to Detect the “Silent” Attack

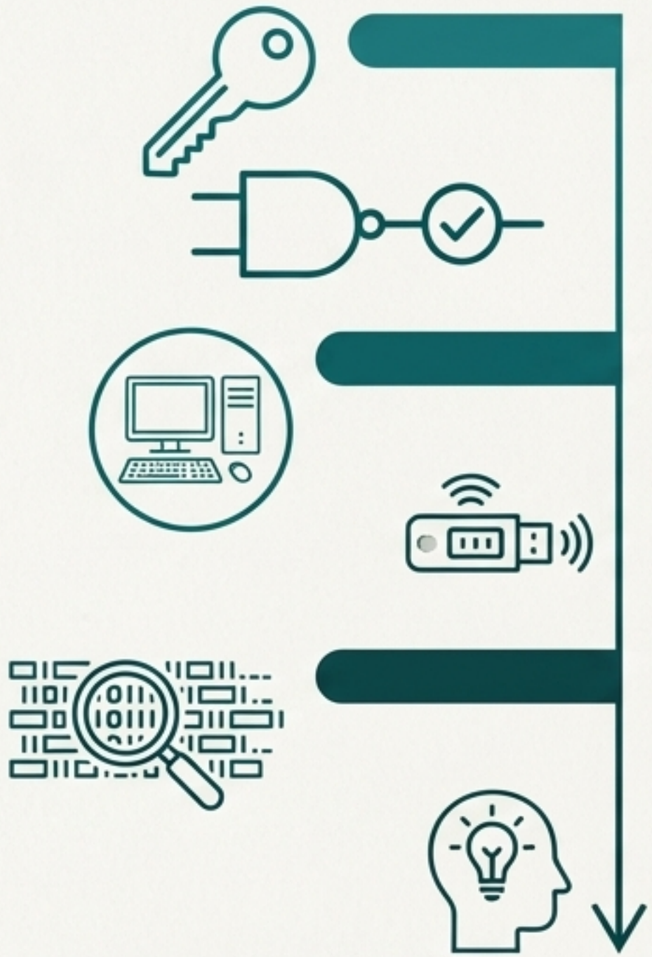
Action 1: Deploy Safety-Specific Monitoring.

- **What:** Implement an OT monitoring solution (e.g., Dragos, Nozomi) with deep packet inspection for our specific safety vendor protocols.
- **Why:** To create high-fidelity alerts for any command attempting to ‘Write,’ ‘Upload,’ or ‘Download Logic’ to the SIS outside of a scheduled and authorized maintenance window.

Action 2: Train Process Engineers on Cyber Indicators.

- **What:** Develop and deliver training based on the Trisis narrative for all Process and Control Engineers.
- **Why:** To teach them that a ‘nuisance trip’ or an unexpected controller reset might not be an equipment fault—it could be the first sign of a probe by a state actor. This turns our engineers into a human sensor network.

Our Roadmap to a Hardened, Resilient Safety Architecture



Phase 1 (Now)

Enforce Physical Key Policy

Verify Failsafe Logic

Phase 2 (1-3 Mos.)

Isolate Engineering Workstation

Implement Dedicated MFA

Phase 3 (3-6 Mos.)

Deploy Protocol-Specific Monitoring

Train Engineers

This plan systematically eliminates the vulnerabilities exploited in the Trisis attack, moving us from a reactive posture to a physically hardened and actively monitored state.

We Must Evolve from Locking the Garage to Welding the Hood Shut

Perimeter Defense (Firewalls)

A firewall is the lock on the garage door. It is necessary, but a determined attacker will eventually get through it.

Inherent Safety (Physical Controls)

The Physical Key policy is the equivalent of welding the hood of the car shut. Even if the attacker gets into the garage, they cannot tamper with the engine or the brakes.

Our strategy must shift from relying solely on perimeter security to enforcing inherent physical safety. This is how we protect our people, our plant, and our operations from the most sophisticated threats.