INDUSTRY WATCH — QUICK REFERENCE

ICS / OT Incident Response Checklist

A plant-floor-ready guide for the first hours of a suspected cyberattack on your control systems — before, during, and after.

> **How to use this:** Print it, laminate it, and keep it in the control room — not just in an IT folder. In a real incident you may not trust the network enough to pull it up on screen. This is a quick-reference companion to a full incident response plan, not a replacement for one.

1 Before It Happens — Preparation

Do this now, not during an incident

- [ ] Maintain a current asset inventory: make, model, and firmware version of every PLC, HMI, and RTU on the floor.
- [ ] Confirm no control system device is reachable directly from the public internet without a VPN or jump host in front of it.
- [ ] Document and drill manual-override procedures for every automated process — operators should be able to run the plant without the network.
- [ ] Keep an out-of-band contact list (phone numbers, not just email/chat) for your IR team, leadership, and safety officer.
- [ ] Know in advance who has the authority to order a shutdown, and under what conditions.
- [ ] Know your reporting obligations before you need them (CISA, EPA for water systems, state fusion center, sector-specific regulators).

2 First 15 Minutes — Detect & Assess

The moment something looks wrong

- [ ] Confirm whether OT/control systems are actually affected — don't assume it's "just IT" until verified.
- [ ] Ask the harder question: is the data on the HMI/SCADA screen still trustworthy, not just still present?
- [ ] Log the exact time, symptoms, and affected assets before memory fades — who saw what, and when.
- [ ] Do not reboot, power off, or "just restart it" before consulting engineering — this can destroy evidence and, more importantly, push a process into an unsafe state.
- [ ] Notify your safety officer in parallel with IT/security — this is a safety event until proven otherwise.

3 Contain — Without Causing a Second Incident

Minutes to hours

- [ ] Prioritize physical safety and process integrity over forensic data preservation, always.
- [ ] If you can't verify a system's integrity, shift to manual operation rather than continuing to trust it.
- [ ] Isolate affected segments at the network boundary — don't unplug control hardware itself unless engineering confirms it's safe to do so.
- [ ] Preserve logs before they rotate out or get overwritten.
- [ ] Use out-of-band communication (phone, not the network you suspect is compromised) to coordinate the response.

> **Real-world example:** in the 2026 multi-state water utility attacks, the difference between "no effect on services" and actual flooding or lost water pressure came down to exactly this — how fast the intrusion was noticed, and how fast staff could revert to manual control.

4 Notify

In parallel with containment, not after

- [ ] Internal chain of command and safety officer
- [ ] Legal counsel and cyber insurance carrier
- [ ] CISA (cisa.gov/report or 1-888-282-0870)
- [ ] Sector regulator (e.g., EPA for water systems)
- [ ] State fusion center / ISAC for your sector
- [ ] Customers or public — only after the above, and only with legal/comms sign-off

5 Eradicate & Recover

Hours to days

- [ ] Restore only from backups/configurations that have been verified clean.
- [ ] Change every default or weak credential on affected control system devices before reconnecting anything.
- [ ] Don't restore internet-facing access until segmentation has been independently verified — the exposure that let attackers in is often the same one that let them do damage.
- [ ] Bring systems back online in stages, verifying each before moving to the next — not all at once.

6 After Action

Within 5 business days

- [ ] Hold a debrief with operations, IT, and safety together — not IT alone.
- [ ] Update your asset inventory with anything discovered during the incident.
- [ ] Update the incident response plan itself based on what actually happened versus what the plan assumed.
- [ ] Consider a third-party OT security assessment to close the specific gap that was exploited.