# How does Cyber Crucible align with IEC 62443 for industrial control systems?

**Short answer:** Cyber Crucible supports the IEC 62443 defense-in-depth model for industrial automation and control systems by adding autonomous, kernel-level endpoint protection that does not disrupt production. It runs locally, tolerates disconnected operation, and suspends only malicious processes, which aligns with the standard's emphasis on both security and operational availability.

## How it maps to the standard's intent

- **Zone and conduit protection.** Endpoint-resident prevention hardens the devices inside a zone without depending on a network round trip.
- **Availability first.** Selective suspension of a malicious process avoids the plant downtime that blunt containment causes.
- **Works in low-connectivity settings.** Suitable for manufacturing floors, logistics fleets, and edge sites where cloud connectivity is unreliable or deliberately absent.

## The honest boundary

IEC 62443 certification applies to systems and processes, not to a single endpoint tool; Cyber Crucible is a component that supports the standard's objectives. Control mapping is available under NDA.

---

Revision #2
Created 2026-07-23 15:18:26 UTC by Dennis Underwood
Updated 2026-07-23 18:19:56 UTC by Dennis Underwood