DE-4000 / ACM-4000

Next-Generation Safety Shutdown & Control System

Non-Software Cybersecurity Recommendations

ALTRONIC
www.altronic-llc.com | sales@altronic-llc.com

1.0 Executive Summary

The DE-4000 and ACM-4000 platforms occupy what NIST SP 800-82 Rev. 3 classifies as Purdue Levels 1–2 (basic control and area supervisory control). Both products were designed around modern, Ethernet-first connectivity: integrated Wi-Fi, multiple Ethernet NICs (one Gigabit and two 10/100 on the ACM-4000), USB-A and USB-C, microSD, HDMI, RS-485, and CAN. This connectivity is a competitive differentiator, but it also expands the attack surface relative to the legacy DE-3000 generation that preceded it.

This guidance document provides non-software cybersecurity recommendations—physical, architectural, electrical, and procedural—that customers can implement without modifying firmware. The dominant theme is that a true "air gap" is no longer realistic for a connected product family that is marketed for remote monitoring; instead, the goal is a defensible, segmented, monitored, and physically controlled deployment that satisfies CISA Cross-Sector Performance Goals and the ISA/IEC 62443 Zones and Conduits standards.

Recommendations are organized into six areas:

1. Network architecture and segmentation
2. Physical hardware controls
3. Removable-media and port management
4. Wireless management
5. Power, grounding, and environmental
6. Procedural and supply-chain controls

NOTE: This document is informational; it does not constitute legal or compliance certification.

2.0 Threat Model

Threats applicable to a DE-4000 / ACM-4000 deployment fall into five practical categories. The non-software controls in this document target each of them.

Threat Category	Realistic Vector at a Compressor Station	Primary Non-Software Control
Remote network intrusion	Internet-exposed Modbus/TCP, Ethernet/IP, or HTTP(S) ports on a DE-4000 reachable from a SCADA WAN, vendor VPN, or cellular gateway	Firewalled DMZ, unidirectional gateway, segmentation
Removable media (sneakernet)	USB drive used to export data logs from the DE-4000 / ACM-4000 microSD or to load configuration files; technician laptop carrying malware	USB lockouts, sanctioned media kiosk, port blockers
Insider / contractor misuse	Field technician with panel key reconfigures setpoints or disables shutdown logic	Two-key panel access, tamper-evident seals, badge logs
Wireless attacks	Drive-by association to the DE-4000 / ACM-4000 integrated Wi-Fi from outside the fence	Antenna removal, RF shielding, directional antennas, disabled radios on production units
Supply chain & spares	Counterfeit or pre-compromised replacement modules, microSD cards, or HMI displays entering the spare-parts pool	Sealed-bag receiving, serialized parts, vetted distribution

Two industry-validated points worth noting up front: first, NIST SP 800-82 Rev. 3 explicitly states that air-gapping alone is not a sufficient protective measure, and incidents from Stuxnet (USB vector) through the 2020 ransomware attack on a U.S. natural-gas compression facility confirm this. Second, recent CISA guidance emphasizes that owner/operators must assume IT-OT convergence is permanent and design layered, defense-in-depth protection accordingly. The recommendations in this document reflect both points.

3.0 Network Architecture and Segmentation

This section addresses the single highest-leverage non-software control: where the DE-4000 and ACM-4000 sit on the plant network, and what threats can reach them.

3.1 Purdue-Model Placement

The DE/ACM systems are intended to sit in a segmented OT network (Purdue Level 1–2), isolated from corporate IT and the internet. The DE-4000 / ACM-4000 must never share a broadcast domain or VLAN with:

- Level 4/5 corporate IT (email, file shares, ERP, domain controllers)
- Engineer or technician laptops on general-purpose Wi-Fi
- Cellular routers or LTE modems with public-facing interfaces
- Building-management systems, IP cameras, or VoIP phones

All traffic between the OT zone and any higher Purdue level must traverse a dedicated industrial firewall (Belden IAF-240, Hirschmann EAGLE40, Fortinet FortiGate Rugged, or Cisco Catalyst IE3400 are recommended) configured to deny-by-default.

3.2 Use the Three NICs on the ACM-4000 as a Hardware Segmentation Tool

The ACM-4000 ships with three network interface controllers (NICs)—physical Ethernet interfaces—one Gigabit and two 10/100. Treat them as three separate trust zones rather than three ways onto the same network:

Port	Recommended Role	Justification
Gigabit NIC	Local control LAN	Connects only to the DE-4000, AFR-500, MIDAS HMI, and other Altronic devices on the skid. No uplink to plant network.
10/100 NIC #1	Plant / SCADA uplink (read-only ideally)	Single, documented path to the process-control network. Routed through a firewall and, where possible, a data diode or unidirectional gateway.
10/100 NIC #2	Service / commissioning port (disabled in production)	Physically capped with a tamper-evident locking RJ-45 blocker. Enabled only during scheduled maintenance windows under change-control.

3.2.1 DE-4000 Without ACM-4000 (Legacy Configuration)

In deployments where no ACM-4000 is installed, the DE-4000 does not provide separate NICs for hardware-level network segmentation. Full network isolation between the local control LAN and the plant/SCADA uplink is therefore not achievable without additional external hardware such as a managed switch or firewall.

In this configuration, connecting to Port 7 is recommended, as Port 7 does not have the ability to communicate directly with the ST Microcontroller (the core controller logic), limiting a connected party to the web application interface only. This provides a meaningful reduction in exposure compared to other ports, but should not be considered equivalent to full network segmentation.

For sites requiring true hardware-level network isolation, Altronic recommends upgrading to an ACM-4000, which provides three independent NICs that can be configured as separate trust zones as described above.

3.3 Unidirectional Gateways (Data Diodes) for High-Consequence Sites

For LNG, gas-storage, and large-bore compression sites where a process upset can cause catastrophic surge or loss of containment, a true hardware data diode (Waterfall Security, Owl Cyber Defense, or Siemens RUGGEDCOM RX1500 with Fox-IT) is recommended between the OT zone and any historian, cloud-telemetry, or remote-monitoring service. A diode physically prevents return traffic at the optical layer and cannot be misconfigured to permit it. This is the only architecture that meaningfully resembles an air gap while still allowing the DE-4000 / ACM-4000 to publish data outward.

3.4 No Direct Internet, No Direct Cellular

- Never connect the DE-4000 or ACM-4000 directly to a cellular modem, satellite terminal, or DSL/cable router. Always interpose at minimum a stateful industrial firewall and a dedicated jump host.
- If remote access is contractually required, terminate the VPN at a hardened gateway in a DMZ—not on the DE-4000 itself. Use multi-factor authentication on the gateway and enforce session recording.
- Disable any UPnP, mDNS broadcast, or auto-discovery features on any router that touches the OT zone.

3.5 Conduit Hardening

- Use industrial managed switches (Hirschmann, Moxa EDS, and Cisco IE-series) with port security—sticky/persistent MAC and/or 802.1X authentication—where the plant environment supports it. **NOTE:** Sticky MAC and 802.1X compatibility is vendor-, platform-, and release-specific. Verify support in the documentation for switch model and software version before combining these features.
- Disable unused switch ports physically (port blockers) and logically (admin shutdown).
- Run all OT cabling in dedicated metallic conduit, separated from IT cabling, and labeled with red “OT—DO NOT CROSS-CONNECT” tags every 10 feet.

4.0 Physical Hardware Controls

Physical access is consistently identified by CISA as one of the most under-controlled aspects of OT environments. Each recommendation below can be implemented at the panel-build stage. The following hardware-physical controls can be requested at the time of quote for new Altronic panels or retrofit kits.

4.1 Panel and Enclosure

- Specify NEMA 4X or NEMA 12 lockable enclosures with key-different cylinder locks (not universal three-panel "square keys", which are sold on Amazon). Best practice is the use of high-security cylinders with documented key control (ABLOY Protec2 or Medeco).
- For unmanned remote sites, add a secondary intrusion-detection switch (magnetic reed or plunger) wired to one of the DE-4000's spare digital inputs and configured as a non-shutdown alarm reported to SCADA. This provides a hardware-based, tamper-detection layer at no additional software cost.
- The DE-4000 and ACM-4000 digital input terminals are potential physical manipulation points — an unauthorized party with access to field wiring could force a shutdown or spoof a sensor state. Ensure all input wiring terminals are housed within the locked enclosure or in a secured, tamper-evident junction box.
- Apply numbered, tamper-evident security seals (e.g., TydenBrooks) across every enclosure door and across the seam of any USB or Ethernet port plug. Log seal serial numbers in the maintenance management system.
- Fit a transparent, polycarbonate "button guard" over the MIDAS HMI or 8"/15" touchscreen to prevent casual screen-tap reconfiguration. Hinged button guards with a hasp accept a small padlock.

4.2 Two-Person / Two-Key Access for Critical Sites

For Class I, Division 2 sites tied to TSA-regulated pipelines or PHMSA-regulated gas storage, a two-key panel design is recommended: one key held by the operations technician, one by a supervisor or remote-dispatch authority; neither key alone can open the panel. This is standard practice in nuclear and high-consequence chemical facilities and is cheap to retrofit.

4.3 Hardware Write-Protect Where Available

- The ACM-4000 uses a microSD card for data logging. Altronic recommends network-based data export rather than physical card removal. If card removal is necessary, use a full-size SD adapter with the physical write-lock slider in the locked position before connecting to any external device.
- Where the panel design allows, route the DE-4000 Controller, DE-4000 Terminal Module, and ACM-4000 outputs through a key-switched bypass so a supervisor can physically disable remote control commands during planned work without de-powering the unit.

4.4 Display and HMI Placement

- Mount displays/HMIs so screens are not visible from outside the fence line or from windows in adjacent buildings—shoulder surfing the alarm summary reveals more than people assume.
- Use privacy filters on any display/HMI located in a shared control room.

5.0 Removable-Media and Port Management

Removable media and communication ports/interfaces are all potential ingress points. The Stuxnet, Industroyer, and 2020 U.S. natural-gas-compressor incidents all involved removable media or technician hardware as part of the kill chain.

The ACM-4000 has the following ports:

- 3× Ethernet
- 2× USB-A
- 2× USB-C
- 1× USB-OTG
- 1× microSD
- 2× HDMI
- 3× RS-485
- 1× CAN bus
- 1× PCI-E (Legacy)

The DE-4000 Controller Module has the following ports:

- 7× Ethernet
- 1× USB-A
- 1× USB-C
- 1× microSD
- 1× CAN bus
- 2× RS-485

Each DE-4000 Terminal Module has the following ports:

- 1× Ethernet
- 1× RS-485
- 1× CAN bus

5.1 Securing Ports

- Install keyed USB port blockers (Lindy, Smart Keeper, or PadJack) on every USB-A and USB-C port not in active production use. Maintain a single key holder per site.
- Install RJ-45 port blockers on unused Ethernet ports.
- Cap unused HDMI with a locking cover. HDMI is a credible attack vector via maliciously crafted EDID (extended display identification data—display metadata) payloads on rogue capture devices.
- Use a sealed plug or epoxy-fill on the microSD slot once the production card is installed and write-protected, if data export is performed via network share rather than card removal.
- RS-485 and CAN bus are not routable network protocols and require physical wire access to exploit — the primary control is ensuring the enclosure is locked and access is controlled.
- Disable unused RS-485 and CAN bus ports in the device configuration menu where firmware supports it. Confirm with Altronic Engineering whether this is supported on your specific DE-4000 / ACM-4000 firmware version.
- Apply tamper-evident covers over unused RS-485 and CAN bus connectors as an additional physical deterrent.
- For active RS-485 or CAN bus ports connected to a gateway or CAN-to-Ethernet converter, ensure that device is placed on the secured OT network segment and is not internet-accessible.
- Do not rely on the bus or port itself as a security boundary — access control must be enforced at the enclosure, connected device, and network architecture levels.

5.2 Sanctioned-Media Kiosk

For any site that legitimately needs to import configuration files or export logs via USB, deploy a dedicated, offline media-sanitization kiosk (OPSWAT MetaDefender Kiosk, Votiro Secure File Gateway, or Honeywell SMX) at the control-room entry.

Recommended procedure:

- All USB media coming on-site is scanned and re-written to a clean, factory-issued, color-coded “OT-only” USB drive.
- Original media never enters the OT zone.
- OT-only drives are inventoried, serialized, and returned to a locked cabinet after each use.

5.3 Eliminate Personal Devices

- Prohibit charging of phones, tablets, vape pens, or any consumer device from DE-4000 / ACM-4000 USB ports. Provide a separate, isolated 5 V USB charging strip in the control room.
- Post visible signage at each panel: "NO PERSONAL USB DEVICES—VIOLATION IS A REPORTABLE INCIDENT."

6.0 Wireless Management

The DE-4000 ships with an integrated Wi-Fi radio and an external body-mount Wi-Fi antenna (Altronic P/N 691781); the ACM-4000 has an integrated Wi-Fi radio, but no antenna. Wi-Fi is convenient for commissioning but is the most commonly criticized cybersecurity feature in modern industrial controllers.

6.1 Radios Off in Production By Default

- Disable the integrated Wi-Fi radio in software (one-time configuration in the settings menu) **AND** physically disconnect the external antenna for all production deployments.
- The antenna should be re-installed only during commissioning or scheduled maintenance, by an authorized technician, and removed before the panel is closed.

6.2 If Wi-Fi Must Stay On

- Install a directional patch antenna (not an omnidirectional whip) aimed at the operator's documented work location, reducing RF spill outside the fence line by 15–25 dB.
- Where the panel is inside a metal enclosure, leave the antenna inside the enclosure; the Faraday effect of the cabinet provides meaningful attenuation.
- Place the entire skid inside a fenced compound with at least 50-foot setback from public access, so a drive-by attacker cannot get close enough for a reliable association.
- Conduct an annual RF survey using a handheld spectrum analyzer (e.g., RF Explorer or Wi-Spy) to confirm signal strength at the fence line is below the manufacturer's minimum association threshold.

6.3 Bluetooth and Other Radios

Verify with Altronic engineering whether any third-party PCI-E or USB peripheral added to the DE-4000 or ACM-4000 introduces a Bluetooth, Zigbee, or LoRa radio. If so, treat it under the same rules as Wi-Fi: disabled by default, antenna removed, justified per-deployment.

7.0 Power, Grounding, and Environmental Controls

Several non-obvious cybersecurity controls live in the electrical and environmental design of the panel.

7.1 Dedicated Power and Disconnect

- The DE-4000 and ACM-4000 already require a dedicated disconnect (PMM, fuse block, or breaker) marked as the over-current and disconnect for the system (refer to the installation manuals for the DE-4000 and ACM-4000). Expanding upon this practice, each DE-4000 and ACM-4000 should have its own lockable disconnect that supports lockout/tagout (LOTO).
- LOTO is not just a safety control—it is also a cybersecurity control. A panel that is physically de-energized cannot be remotely exploited during planned maintenance windows.

7.2 Power Conditioning and UPS Strategy

- Use an industrial DC Uninterruptible Power Supply (Phoenix Contact QUINT-UPS, Puls UB10, or Sola SDU) sized for graceful shutdown rather than indefinite runtime. An attacker who can cause a power glitch can sometimes force a controller into a fail-state that bypasses normal protections; a 5-minute holdup eliminates that class of attack.
- Specify a power-line filter / surge suppressor at the panel ingress. Beyond lightning protection, this attenuates conducted RF that could otherwise be used in side-channel attacks against the Raspberry Pi Compute Module 4 (CM4) in the ACM-4000 or the SoM in the DE-4000.

7.3 Grounding for Emissions Security (EMSEC)

- Single-point grounding (refer to the installation manuals for the DE-4000 and ACM-4000) is mandatory for safety; from a cybersecurity perspective, it also reduces ground-loop signaling that can leak data via emanations. For sensitive sites (federal, defense, critical infrastructure tier 1), specify a copper ground bus, < 1 Ω to earth, and bond all shielded cables at one end only.

7.4 Environmental Sensors as Tamper Detection

- The DE-4000 has 32–160 configurable inputs. Allocate one of them as a panel-door contact and a second as an alarm for interior temperature above expected ambient. Both should generate annunciator alarms that are logged in the SCADA historian, providing a free, hardware-based, tamper-detection layer.

8.0 Procedural and Supply-Chain Controls

8.1 Manufacturing and Shipping

The following controls represent Altronic's recommendations for customers who require enhanced supply-chain security. These are not standard practice by default and customers must request these measures specifically at the time of quote.

- Ship every DE-4000 and ACM-4000 in tamper-evident packaging with a serialized hologram seal. Customers verify the seal against a number printed on the packing slip.
- Pre-load a unique factory configuration baseline cryptographic hash on the unit's nameplate or in a customer-portal record. Customers can verify post-installation that no firmware has been substituted in transit.
- Maintain a complete Hardware Bill of Materials (HBOM) and Software Bill of Materials (SBOM) per CISA Secure-by-Design guidance, made available to customers under NDA.

8.2 Spare Parts Custody

- Store spare DE-4000 / ACM-4000 modules, microSD cards, and displays/HMIs in a locked cabinet with two-person access. Spares pulled from open stockrooms are a documented advanced persistent threat (APT) pre-positioning vector.
- Color-code or RFID-tag spare parts so they cannot be confused with personal-use electronics.

8.3 Personnel and Access

- Maintain a written list of personnel authorized to open OT panels. Review quarterly. Revoke on the same business day of termination or role change.
- Require escort for all third-party personnel—field service, integrators, gas-engine OEM technicians—inside the OT zone.
- Log every panel-opening event in a paper logbook stored at the panel, in addition to any electronic system, as paper cannot be remotely altered.

8.4 Decommissioning

- When a DE-4000 or ACM-4000 is removed from service, the microSD card and any onboard non-volatile storage should be physically destroyed (shredded or degaussed), not erased. This prevents a returned unit from leaking production data.
- The customer should physically destroy the microSD card and any storage media per NIST SP 800-88 (Media Sanitization) —"destroy" level for any device that handled production data before disposal or re-purposing.

9.0 Quick-Reference Hardening Checklist

A field technician should be able to verify each item below in under 30 minutes per panel.

#	Control	Verification Method
1	Enclosure locked with high-security cylinder; key inventory current	Visual + key log
2	Tamper-evident seals intact on enclosure door and unused ports	Visual; record seal serials
3	Unused USB-A, USB-C, RJ-45, and HDMI ports physically blocked	Visual
4	Wi-Fi antenna removed (or directional, justified, documented)	Visual + RF survey
5	Unused Ethernet ports capped and disabled	Visual + switch log
6	Dedicated, lockable disconnect installed and labeled	Visual + LOTO test
7	Panel door contact-wired to DE-4000 input and alarming in SCADA	Function test
8	No cellular modem, hotspot, or rogue access point within enclosure	Visual + spectrum analyzer
9	MicroSD card physically write-locked OR slot-sealed	Visual
10	Spare parts serialized, stored in locked cabinet with two-person access	Cabinet audit
11	Authorized-personnel list current within 90 days	Document review
12	Paper panel-opening logbook present and current	Visual

10.0 Additional Measures

Contact Altronic or your local Altronic Distributor to discuss additional cybersecurity measures, including:

- Pre-hardened DE-4000 / ACM-4000 panel
- Cyber-health site visit

11.0 References

- NIST SP 800-82 Rev. 3 — Guide to Operational Technology (OT) Security
- NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization
- ISA/IEC 62443-3-3 — System Security Requirements and Security Levels
- ISA/IEC 62443-4-1 / 4-2 — Secure Product Development Lifecycle and Component Requirements
- CISA CPG 2.0 — Cross-Sector Cybersecurity Performance Goals 2.0 (2024 Update)
- CISA / DOE / NCSC — Joint Guidance for Industrial Control Systems Cybersecurity
- TSA Security Directive Pipeline-2021-02C (SD02C) — Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing
- INL/RPT-24-79372-Rev000 — Cybersecurity Considerations for the Liquefied Natural Gas Sector
- Altronic DE-4000 Operation and Configuration Manual
- Altronic ACM-4000 Installation and Operation Manual

712 Trumbull Avenue I Girard, Ohio 44420
(330) 545-9768 I Fax: (330) 545-9005
www.altronic-llc.com I sales@altronic-llc.com

ALTRONIC