TECHNICAL GUIDE • OCTOBER 2026 EDITION

How to protect your refrigeration

Security and contingency for supervisory systems. How to protect access, update the equipment and restore operations safely.

FOR IT, MAINTENANCE AND OPERATIONS MANAGEMENT



Rafael Cocchiaro

Head of Tech | Digital Tech

October 15, 2026 · Version 2.0

EXECUTIVE SUMMARY • QUICK READ

What you need to ensure in every store

These are the priorities to decide on and follow up.
The next pages detail models, versions and procedures.

01 **Protect remote access**

Take administration interfaces off the public internet and use a VPN or protected network.
Coordinate the change with Estech to keep readings flowing.

02 **Update or replace**

Check model and firmware: update Danfoss 800A and XWEB PRO as the manufacturer specifies.
For unsupported equipment, such as XWEB EVO, approve the migration.

03 **Have a backup that has been restored**

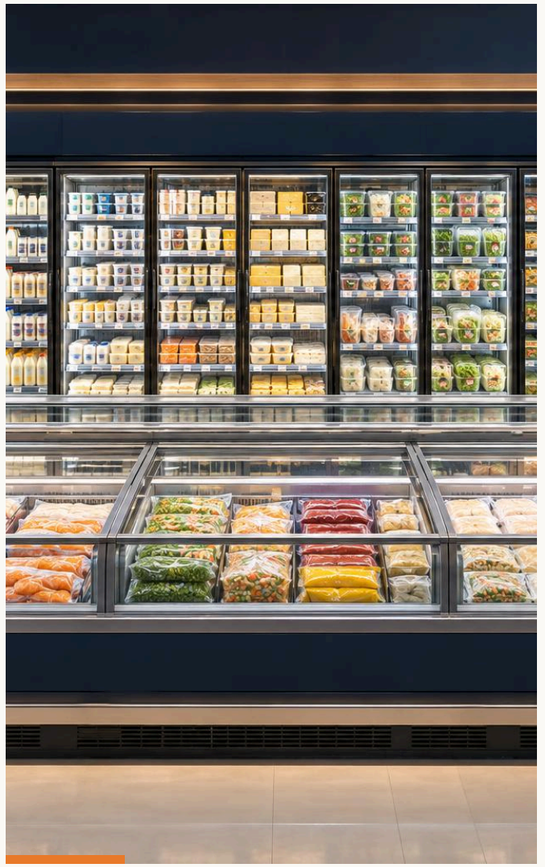
Keep copies of the configuration off the device and off-site.
Run a real restore test and record the result and the recovery time.

04 **Assign an owner and a frequency**

Adopt a review every 3, 6 or 12 months, based on criticality and capacity.
Critical alerts and significant changes require action outside the schedule.

05 **Prepare the incident response**

Protect the products, isolate remote access and call IT, the integrator and Estech.
Before reconnecting, rebuild and validate the equipment as the manufacturer specifies.

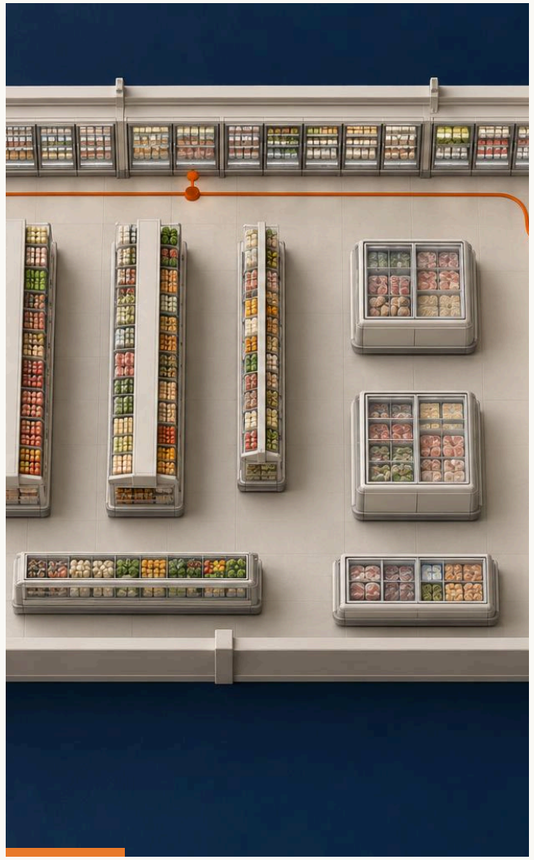


NAVIGATION

Contents

Choose a topic to go straight to its page.
The Contents button in the footer brings you back.

02 Executive summary
04 The alert and the priority
05 AK-SM 800A models
06 Vulnerable firmware ranges
07 Legacy models and replacement
08 Where to get the update
09 XWEB EVO and PRO: versions and support
10 Protected remote access
11 Changing without losing readings
12 What to include in the backup
13 Where to store the copies
14 How to test the restore
15 Reviews every 3, 6 or 12 months
16 Owners and evidence
17 First response to an incident
18 Rebuilding from scratch
19 Criteria to return to operation
20 Sources and contact



01 • UNDERSTAND THE RISK

Remove open access from the internet

CERT-FR has reported compromises of refrigeration supervisory systems. The first step is to block public access to the administration interfaces.

01

Families named in the alert

Danfoss AK-SM and AK-SC, as well as Copeland/Dixell XWEB.
The alert was published on Oct 12, 2026 and expanded on Oct 13, 2026.

02

Permanent protection

Use a VPN (a protected private connection) or another protected network.
An IP allowlist is only a temporary measure until the VPN is ready.

03

If a compromise occurs

Isolate access and plan the factory recovery with the integrator.
A reset alone does not fix a security flaw.



CERT-FR · CERTFR-2026-ALE-012 ↗

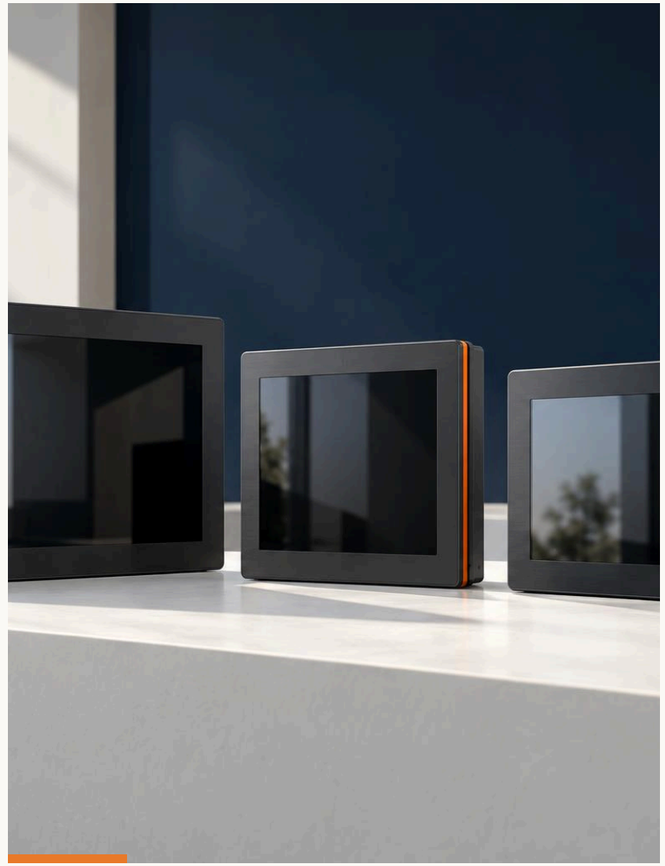
02 • IDENTIFY THE EQUIPMENT

AK-SM 800A: check every model

The 800A family includes the models below.
The letter A is part of the model name and changes the update guidance.

MODEL	RANGE WITH PUBLISHED FLAWS[1]	ACTION
AK-SM 820A	Earlier than 4.3.1	Update from the official page
AK-SM 850A	Earlier than 4.3.1	Update from the official page
AK-SM 880A	Earlier than 4.3.1	Update from the official page

[1] In the advisories reviewed, the limits are common to the 8xxA series.
The specific flaws and their limits are on the next page.
Include special versions, such as the TP78 retrofit (legacy controller network), according to the code on the label.



Danfoss catalog ↗ · Security advisories ↗

03 • CHECK THE VERSION

Which firmware versions are vulnerable?

The limits below apply to the AK-SM 820A, 850A and 880A.
“Earlier than” covers every version below the number shown.

AFFECTED FIRMWARE	PUBLISHED FLAWS (CVE)[1]	FIRST FIX
Earlier than 3.3	2023-25913, 2023-25914 and 2023-25915	3.3
Earlier than 4.2	2025-41450	4.2
Earlier than 4.3.1	2025-41451 and 2025-41452	4.3.1

The ranges overlap.
Version 4.2 is still affected by the flaws fixed in 4.3.1.
Update to the current compatible version, in the manufacturer’s sequence; the historical minimum is not a stopping point.



[1] A CVE is the public identifier of a flaw.
This matrix compiles the AK-SM 800A advisories reviewed on Oct 15, 2026; it does not identify which flaw was used in each incident.

Sources: DSA-2023-08-01 ↗ · DSA-2025-03-01 ↗ · DSA-2025-08-01 ↗

04 • HANDLE LEGACY EQUIPMENT

With no fix available, plan the replacement

Do not apply 800A firmware to a legacy model.
Danfoss reports end of service for the legacy families below.

MODEL / FAMILY	SECURITY FIRMWARE	NEXT STEP
AK-SM 820, 850 and 880 800 family, without the A	No fixed version indicated in the sources reviewed	Isolate and migrate
AK-SC 255 and AK-SC 355	No fixed version indicated in the sources reviewed	Isolate and replace
AK-SM 350 and AK-SM 720	Families with end of service	Assess migration with Danfoss

CERT-FR does not detail models or firmware for the AK-SC series.
No version of that series can be declared “secure” based on the alert.
For legacy units, confirm their status by product code with Danfoss support.
The list above is not a per-model list of CVEs.



Danfoss · end of service ↗ · CERT-FR ↗

05 • UPDATE UNDER CONTROL

Download only from the official source

For the AK-SM 820A, 850A and 880A, use the Danfoss page for the 800A series.
As of Oct 15, 2026, it lists the 5.3.x package and the Danux 4.14.017.194 system.

01 **AK-SM 800A: software and operating system**

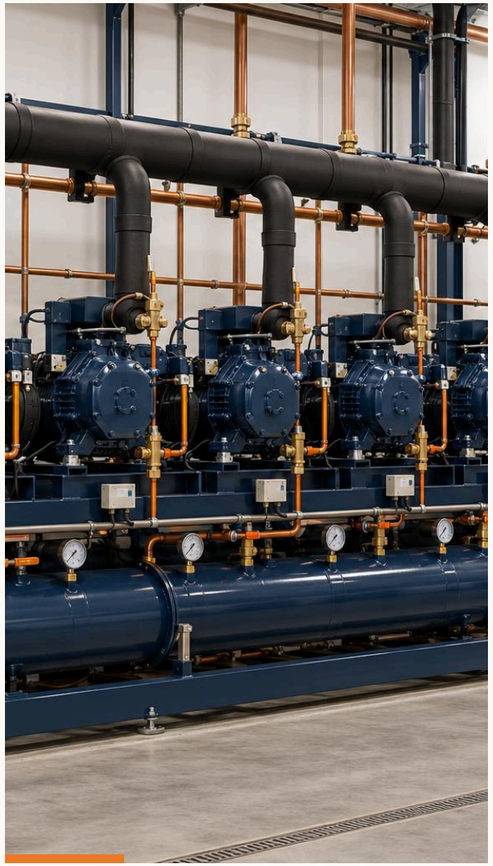
Open the official Danfoss downloads ↗.
Read the instructions, prerequisites and compatibility notes before installing.

02 **Legacy AK-SM / AK-SC: support and migration**

Contact Danfoss ↗.
Provide the model, code, version and photos of the label.
Do not use files from forums or from another model.

03 **Copeland / Dixell XWEB: separate track**

Open System Software Updates ↗.
Select the exact family and confirm the fix with the manufacturer; do not extend the AK matrix to XWEB.



Firmware is the device’s internal software.
Danux is the 800A operating system.
Record both versions and follow the installation order required in the package notes.

Danfoss · downloads and instructions ↗

06 • COPELAND / DIXELL XWEB

XWEB EVO and PRO: check versions and support

The official alert also covers Copeland/Dixell XWEB.
CERT-FR does not separate EVO and PRO or list versions; the details below come from Copeland.

FAMILY AND MODELS	FIRMWARE / SUPPORT	GUIDANCE
XWEB 300D PRO **XWEB 500D PRO** **XWEB 500B PRO**	Flaws published in versions **up to and including 1.12.1.**	Update to **1.13.0** or a later compatible version. Version 1.13 addresses the flaws identified in the February 2026 bulletin.
XWEB 300D EVO **XWEB 500D EVO** **XWEB 500 EVO**	No secure version indicated in the alert. Software support ended on **Mar 16, 2026**.	Keep off the public internet and plan migration to PRO. Older files do not prove a security fix.
XWEB 3000 EVO **XWEB 5000 EVO**	Same end-of-support status as the EVO family.	Isolate and replace with a supported solution. PRO firmware does not apply to EVO.



PRO: mind the sequence. For manual updates, versions up to 1.2.1 must go through 1.3.0 before 1.13.0.
Check the procedure for the model, back up and validate the restore with the integrator.

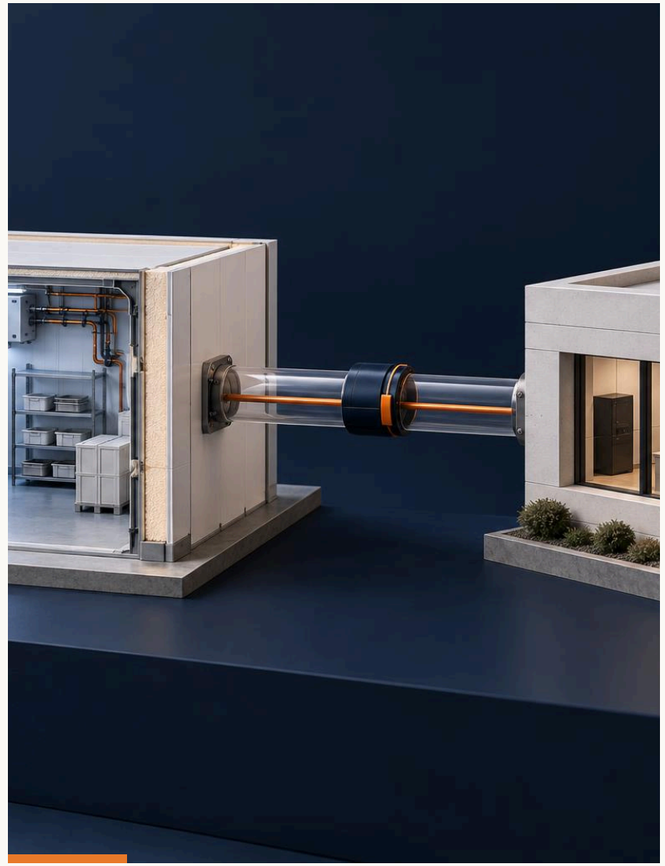
Official downloads: select the exact family and model ↗

Sources: CERT-FR ↗ · Copeland: models and versions ↗ · PRO 1.13 ↗ · EVO: end of support ↗ · Update sequence ↗

07 • PROTECT THE CONNECTION

Remote access through a VPN or protected network

IT should segment the refrigeration network and allow only the access that is needed.
Router and modem administration requires the same care.



01 **Permanent connection**

Use a VPN or protected network, individual accounts and multi-factor authentication when available.
Keep refrigeration separate from the store’s Wi-Fi and computers.

02 **Emergency measure**

If you need an IP allowlist until the VPN is complete, limit sources, ports and duration.
Record who approved it and the migration date.

03 **NEO 360 source addresses**

Ask Estech for the list of source addresses before closing access.
That way, readings keep arriving after the change.

Disable unused services and change factory passwords.
HTTPS, the encrypted web connection, protects communication but does not replace updates and access restriction.

CERT-FR · VPN and emergency filtering ↗ · NEO 360 source addresses: ask Estech for the list.

08 • PLAN THE CHANGE

Close access without losing monitoring

IT, the integrator and Estech should agree on the change and verify the result before closing the maintenance window.

01 **Before the window**

Record the model, firmware and current connection.
Back up, define how to roll back to the previous configuration and keep a local technician available.

02 **During execution**

Set up the protected path and test the integrations.
On the 800A, confirm the security level is set to Strict, which requires HTTPS and session control.

03 **Before sign-off**

Confirm that the interface is not open to the public and that readings, alarms and communication with NEO 360 are still working.

> If monitoring is interrupted, store management should run local temperature rounds at the frequency approved by quality.
> Record the start, end and owner of the interruption.



Danfoss · Strict mode and integrations ↗

09 • PREPARE FOR RECOVERY

The backup must let you rebuild the configuration

Export the configuration of each supervisory system before updating and whenever you change relevant parameters.

01 **Operating parameters**

Include setpoints, defrost schedules and limits, alarms, schedules, sensors and links to the controllers.

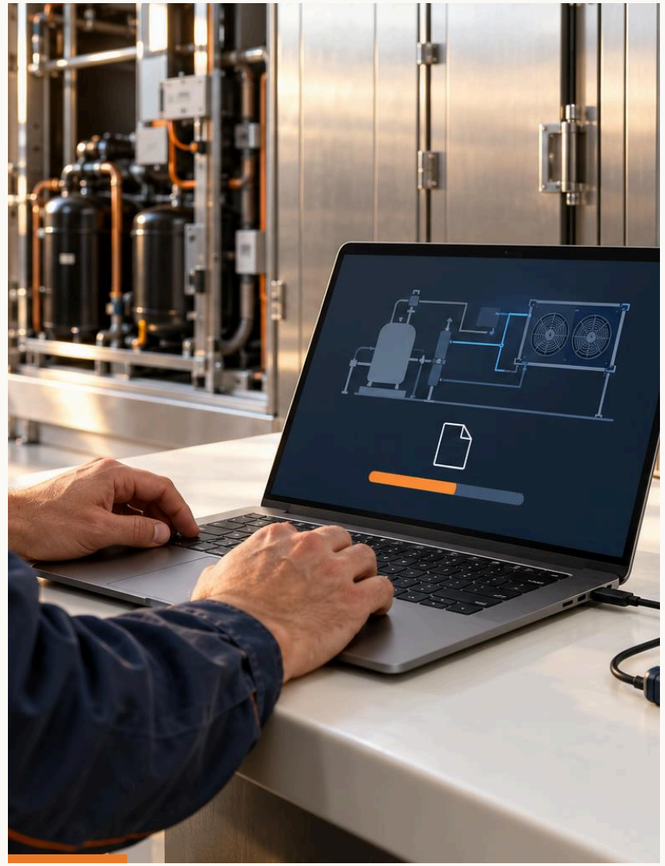
02 **Files and dependencies**

Keep the original export, device files, licenses where applicable, versions, the manual and the official installers needed for recovery.

03 **Identification and instructions**

Record the store, model, serial number, date, author and restore procedure.
Keep passwords and keys in a separate credential vault.

> Check in the manual what the export includes.
> The supervisor’s copy may not contain the configuration of each field controller.
> Save those configurations separately when needed.



10 • STORE SECURELY

Keep copies off the device and off-site

Estech recommends the 3-2-1 rule as a reference: three copies in total, on two storage media, with one copy off-site.

01 **Protection against tampering**

Keep at least one copy offline or protected against modification.
Optional: use encryption, that is, protection that requires a key to read.

02 **Controlled access**

Restrict access to IT and authorized owners.
Keep the keys in a separate vault, with tested emergency access.

03 **Version history**

Preserve the current approved configuration and earlier versions.
After an incident, choose a copy from before the unauthorized change and verify its contents.

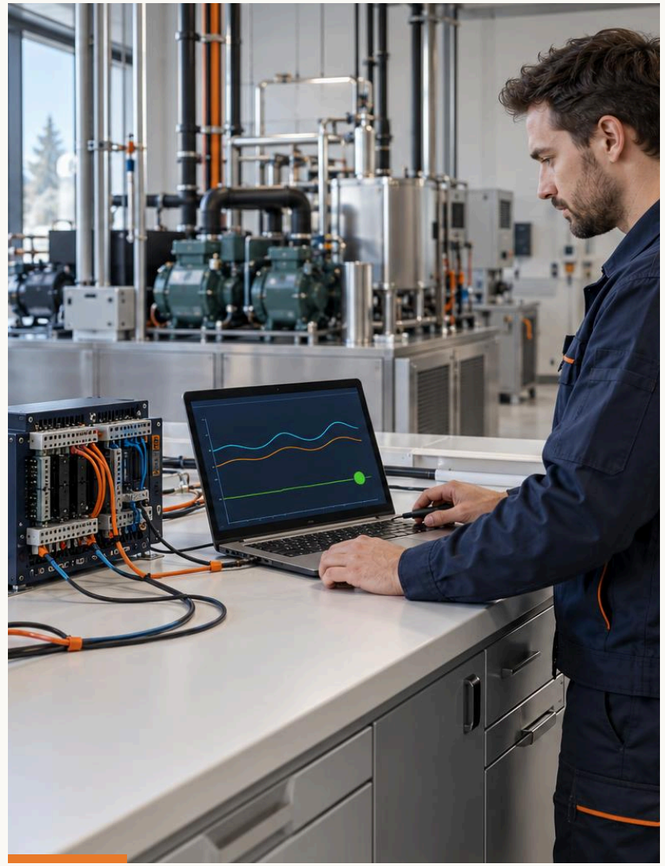


Set a retention period and check that the copies open.
A copy kept only on the integrator’s laptop or on the supervisor itself makes recovery depend on a single point.

11 • PROVE THAT IT WORKS

Test the restore for real

An exported file does not prove that recovery works.
The test must load the copy into a compatible environment and validate the result.



01 **Prepare the test**

Use compatible spare equipment or an environment approved by the manufacturer.
If only the live unit is available, book a supervised window and a rollback plan.

02 **Restore and check**

Restore the configuration and compare sensors, schedules, alarms, access and parameters.
Also verify communication with the controllers and NEO 360.

03 **Record and correct**

Note the file and version used, duration, discrepancies and owners.
If it fails, correct the process and repeat until sign-off.

> A simulator helps you prepare but does not replace a device test when recovery depends on physical interfaces.
> The test must not trigger a defrost or change refrigeration in an operating store.

12 • SET THE FREQUENCY

Choose a cycle of 3, 6 or 12 months

The frequencies below are Estech recommendations.
The decision should weigh criticality, team capacity and acceptable recovery time.



3 months

Critical operation

Many stores, higher downtime impact or legacy equipment.
A full review and a real restore test every cycle.

6 months

Recommended routine

Mid-sized operation.
Full review and real restore test every six months, with assigned owners.

12 months

Limited capacity

Proposed limit for lower-criticality operations, with risk accepted by management and an annual real test.

Do not wait for the next cycle to address a critical alert.
Update the backup at every review and after approved changes.
Reassess access and recovery when changing equipment, integrator, network or firmware.
Apply fixes according to the advisories and compatibility, without waiting for the schedule.

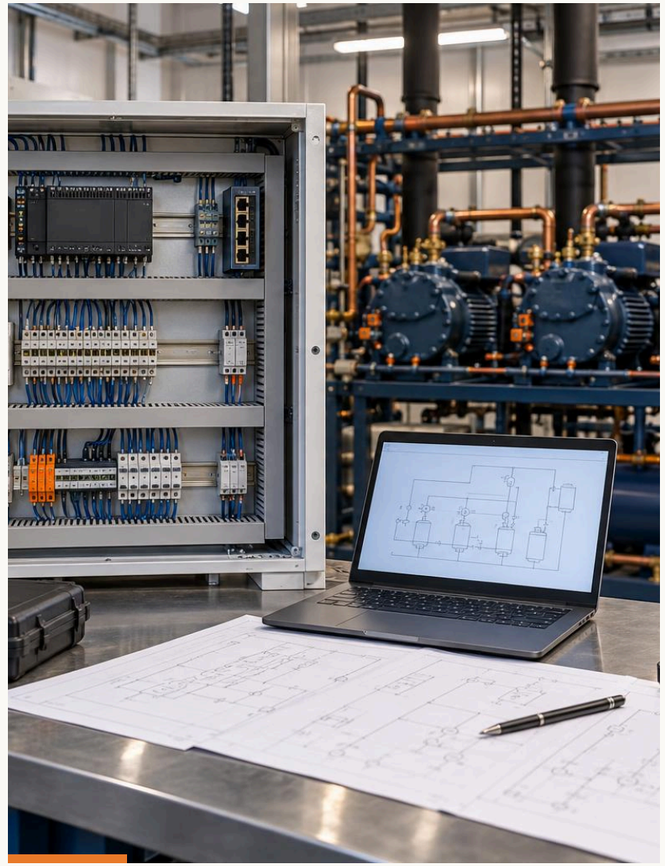
13 • ASSIGN RESPONSIBILITY

Every store needs an owner and evidence

Management approves the cycle and the priority.
IT coordinates the routine and records what was verified with the integrator and operations.

OWNER	DELIVERABLE THAT MUST BE RECORDED
Operations management	Criticality, frequency, budget, deadline and acceptance of outstanding risks.
Your IT	Inventory, access rules, accounts, backup location and next review.
Integrator / manufacturer	Compatibility, updates, export and real restore test.
Store management / quality	Contacts, product protection and validation of local operations.
Estech	Check of the integration and of readings returning to NEO 360, within the agreed scope.

Per-store record: asset and serial · firmware and Danux · owner and backup person · backup location · last restore and duration · outstanding flaws · deadline · sign-off evidence · next review.



14 • RESPOND TO THE INCIDENT

Protect the products and isolate remote access

Off-hours defrosts, unauthorized changes or simultaneous warming: check immediately.
Do not wait for an attack to be confirmed.

01 **Store management and quality: act immediately**

Check temperatures with local measurement, keep doors closed and follow the plan to protect or transfer the products.
Record the times.

02 **IT and integrator: contain the entry point**

Isolate the remote access path identified.
Do not shut down the rack, controllers or cables without identifying their function, as this can affect refrigeration control.

03 **Responsible team: escalate and preserve**

Call IT, the integrator and Estech.
Preserve access logs and photos before the reset, as long as this does not delay protecting operations.

> The signs may also have operational causes.
> The team should investigate without presuming the origin.
> If remote readings are interrupted, keep checking temperatures locally.



CERT-FR · containment and recovery ↗

15 • RECOVER FROM SCRATCH

Rebuild the equipment before reconnecting

After a compromise, the integrator should run the manufacturer’s factory recovery, with the equipment isolated and operations protected.

1. **Preserve and prepare.** Keep evidence and confirm a trusted copy, versions, licenses and the resources needed for recovery.
2. **Factory restore.** Perform the factory reset and the official reinstallation where specified.
   “Formatting” is not a universal procedure: follow the method for the model.
3. **Fix and reconfigure.** Install official packages in the required order, change credentials, load a verified pre-incident configuration.
4. **Validate in isolation.** Check parameters, accounts, communication and local functions.
   Apply the acceptance criteria on the next page.
5. **Reconnect protected.** Use a VPN or protected network and monitor operations with Estech and store management.

> If no supported firmware exists, a reset leaves the equipment exposed to the same flaw.
> Keep it isolated and approve the replacement.
> Do not restore a suspicious configuration without review.



CERT-FR · factory reset and risk of re-compromise ↗

16 • GIVE SIGN-OFF

Close out only after verifying operations

IT, the integrator and store management should record the sign-off.
Agree with Estech on how to verify that monitoring is back.

- Model and versions documented, with applicable fixes or isolation approved pending replacement.
- Interface without public access; protected path and authorized access checked.
- Accounts reviewed and passwords changed after the incident, including router and remote access.
- Setpoints, defrosts and alarms compared against the approved configuration.
- Readings and communication in NEO 360 checked; safe alarm test agreed with operations.
- New protected backup, restore test recorded and next review scheduled.

> Before the intervention, define the maximum acceptable time without the supervisory system and without readings.
> Measure the recovery and set the follow-up period based on the store's criticality.



REFERENCES • CONTACT

Sources for reference and next steps

Start with the inventory of each store.
Prioritize internet exposure, unsupported equipment and the lack of a tested copy.

01 CERT-FR · alert CERTFR-2026-ALE-012 ↗

02 Danfoss · DSA security advisories ↗

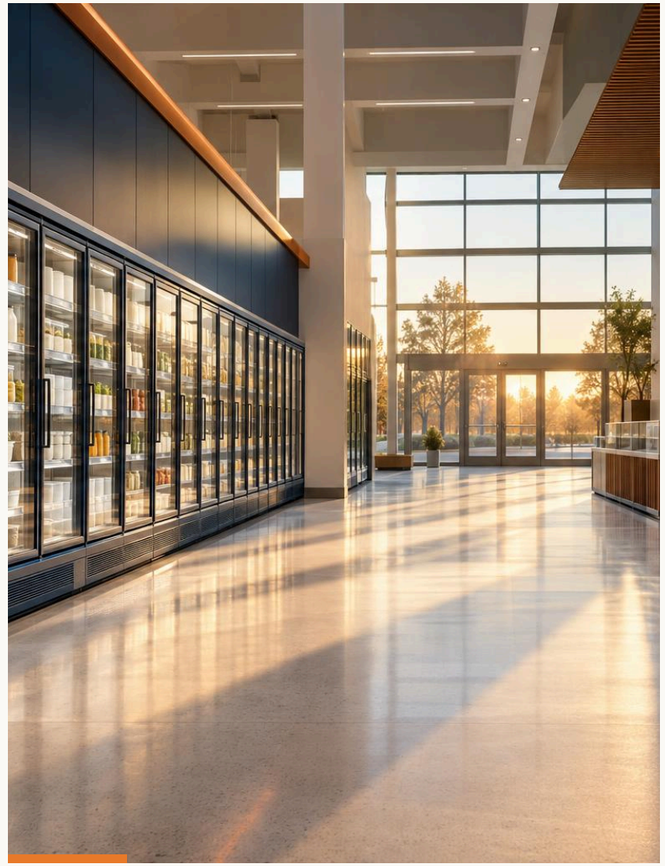
03 Danfoss · AK-SM 800A software and Danux ↗

04 Danfoss · end of service for legacy models ↗

05 Copeland / Dixell · XWEB updates ↗

06 Copeland · affected models and versions ↗

07 Copeland · end of support for the EVO family ↗



ESTECH SUPPORT / JORNADA NEO

help@neoestech.com

For incidents, also call the emergency contacts already agreed with your operations team.

Rafael Cocchiaro | Head of Tech | Digital Tech