GUIDE TECHNIQUE • ÉDITION OCTOBRE 2026

Comment protéger votre froid commercial

Sécurité et continuité des superviseurs.
Comment protéger l'accès, mettre à jour les équipements et rétablir l'exploitation en toute sécurité.



POUR LA DSI, LA MAINTENANCE ET LA DIRECTION DES OPÉRATIONS

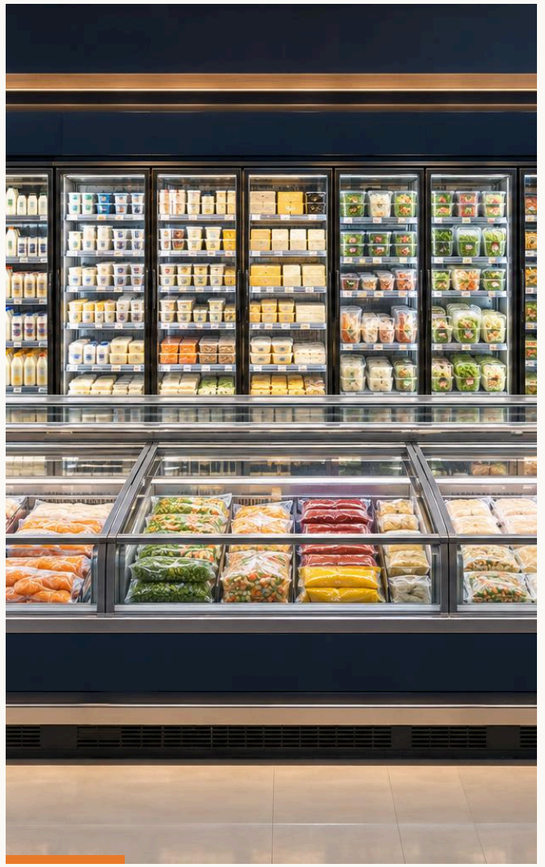
Rafael Cocchiaro
Head of Tech | Digital Tech

15 octobre 2026 · Version 2.0

RÉSUMÉ EXÉCUTIF • LECTURE RAPIDE

Ce que vous devez garantir dans chaque magasin

Voici les priorités pour décider et piloter l'exécution.
Les pages suivantes détaillent modèles, versions et procédures.



01 **Protéger l'accès à distance**

Retirez les interfaces d'administration de l'internet public et utilisez un VPN ou un réseau protégé.
Coordonnez le changement avec Estech pour préserver les relevés.

02 **Mettre à jour ou remplacer**

Vérifiez modèle et firmware : mettez à jour Danfoss 800A et XWEB PRO selon le fabricant.
Pour les équipements non supportés, comme XWEB EVO, validez la migration.

03 **Avoir une sauvegarde déjà restaurée**

Conservez des copies de la configuration hors de l'équipement et du magasin.
Testez réellement la restauration et consignez le résultat et le temps de reprise.

04 **Définir responsable et fréquence**

Adoptez une revue tous les 3, 6 ou 12 mois, selon criticité et capacité.
Alertes critiques et changements importants exigent une action hors calendrier.

05 **Préparer la réponse à incident**

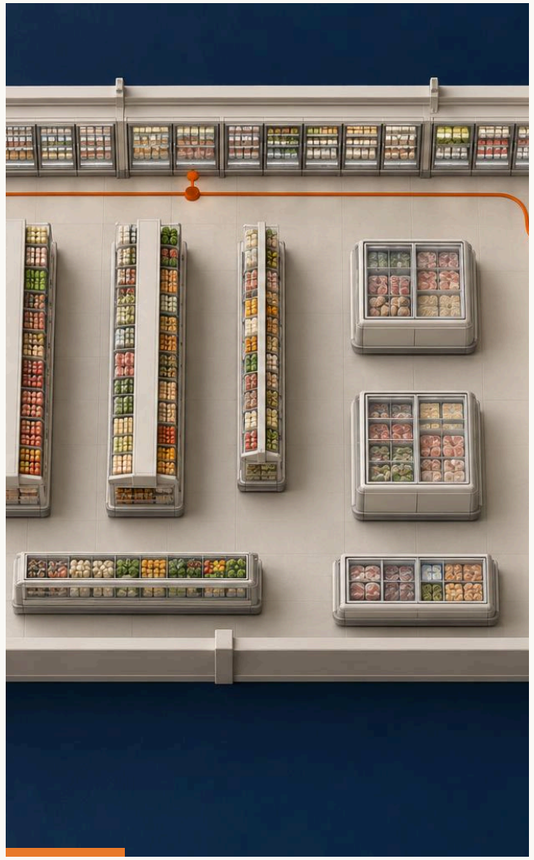
Protégez les produits, isolez l'accès à distance et alertez DSI, intégrateur et Estech.
Avant de reconnecter, reconstruisez et validez l'équipement selon le fabricant.

NAVIGATION

Sommaire

Choisissez un thème pour aller directement à la page.
Le bouton Sommaire, en pied de page, vous y ramène.

02 Résumé exécutif
04 L’alerte et la priorité
05 Modèles AK-SM 800A
06 Firmwares vulnérables
07 Anciens modèles et remplacement
08 Où trouver la mise à jour
09 XWEB EVO et PRO : versions et support
10 Accès à distance protégé
11 Changer sans perdre les relevés
12 Que mettre dans la sauvegarde
13 Où conserver les copies
14 Comment tester la restauration
15 Revues tous les 3, 6 ou 12 mois
16 Responsables et preuves
17 Première réponse à l’incident
18 Reconstruction à partir de zéro
19 Critères de remise en service
20 Sources et contact



01 • COMPRENDRE LE RISQUE

Supprimez l’accès ouvert sur internet

Le CERT-FR a signalé des compromissions de superviseurs de froid. Première mesure : bloquer l’accès public aux interfaces d’administration.



01

Familles citées dans l’alerte

Danfoss AK-SM et AK-SC, ainsi que Copeland/Dixell XWEB.
L’alerte a été publiée le 12/10/2026 et complétée le 13/10/2026.

02

Protection permanente

Utilisez un VPN (connexion privée protégée) ou un autre réseau protégé.
Le filtrage par adresse IP n’est qu’une mesure temporaire, en attendant le VPN.

03

En cas de compromission

Isolez l’accès et planifiez la réinitialisation d’usine avec l’intégrateur.
Une réinitialisation seule ne corrige pas une faille de sécurité.

CERT-FR · CERTFR-2026-ALE-012 ↗

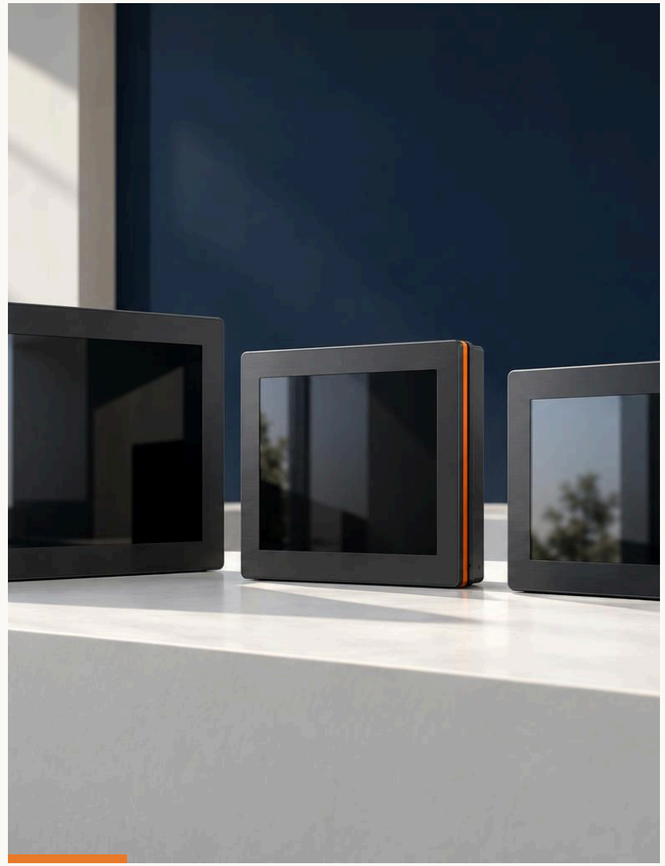
02 • IDENTIFIER L'ÉQUIPEMENT

AK-SM 800A : vérifiez chaque modèle

La famille 800A comprend les modèles ci-dessous.
La lettre A fait partie du modèle et change la procédure de mise à jour.

MODÈLE	PLAGE AVEC FAILLES PUBLIÉES[1]	ACTION
AK-SM 820A	Antérieure à 4.3.1	Mettre à jour via la page officielle
AK-SM 850A	Antérieure à 4.3.1	Mettre à jour via la page officielle
AK-SM 880A	Antérieure à 4.3.1	Mettre à jour via la page officielle

[1] Dans les bulletins consultés, les seuils sont communs à la série 8xxA.
Les failles spécifiques et leurs seuils figurent page suivante.
Incluez les versions spéciales, comme le retrofit TP78 (ancien réseau de régulateurs), selon le code de l'étiquette.



Catalogue Danfoss ↗ · Bulletins de sécurité ↗

03 • VÉRIFIER LA VERSION

Quels firmwares sont vulnérables ?

Les seuils ci-dessous valent pour AK-SM 820A, 850A et 880A.
« Antérieure à » inclut toutes les versions sous le numéro indiqué.

FIRMWARE AFFECTÉ	FAILLES PUBLIÉES (CVE)[1]	PREMIER CORRECTIF
Antérieure à 3.3	2023-25913, 2023-25914 et 2023-25915	3.3
Antérieure à 4.2	2025-41450	4.2
Antérieure à 4.3.1	2025-41451 et 2025-41452	4.3.1

Les plages se chevauchent.
La version 4.2 reste affectée par les failles corrigées en 4.3.1.
Passez à la version actuelle compatible, dans l'ordre du fabricant ; le minimum historique ne justifie pas d'arrêter les mises à jour.



[1] Un CVE est l'identifiant public d'une faille.
Cette matrice reprend les bulletins AK-SM 800A consultés le 15/10/2026 ; elle n'indique pas quelle faille a servi dans chaque incident.

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

04 • TRAITER LES ANCIENS ÉQUIPEMENTS

Sans correctif disponible, planifiez le remplacement

N’appliquez pas le firmware du 800A à un ancien modèle.
Danfoss annonce la fin de service des anciennes familles ci-dessous.

MODÈLE / FAMILLE	FIRMWARE DE SÉCURITÉ	SUITE À DONNER
AK-SM 820, 850 et 880 Famille 800, sans A	Aucun correctif dans les sources consultées	Isoler et migrer
AK-SC 255 et AK-SC 355	Aucun correctif dans les sources consultées	Isoler et remplacer
AK-SM 350 et AK-SM 720	Familles en fin de service	Étudier la migration avec Danfoss

Le CERT-FR ne détaille ni modèles ni firmwares de la série AK-SC.
Impossible de déclarer une version « sûre » de cette série sur la base de l’alerte.
Pour les anciens modèles, confirmez leur statut par le code produit auprès du support Danfoss.
La liste ci-dessus n’est pas une liste de CVE par modèle.

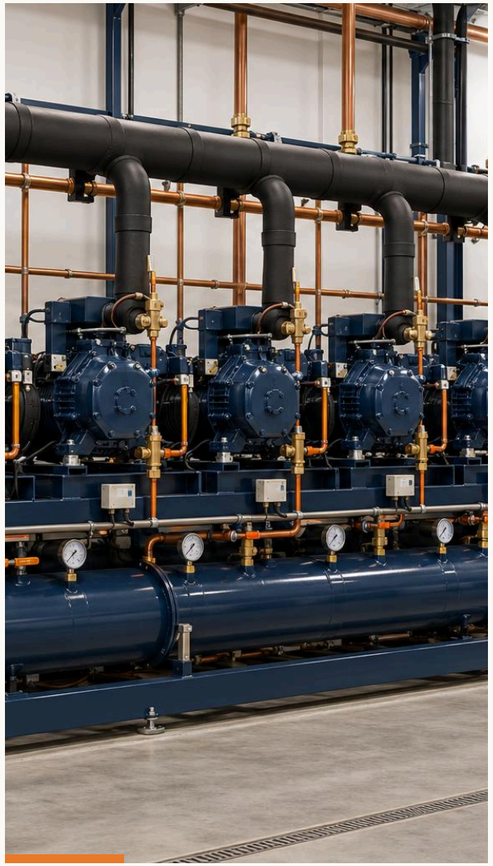


Danfoss · fin de service ↗ · CERT-FR ↗

05 • METTRE À JOUR SOUS CONTRÔLE

Téléchargez uniquement depuis la source officielle

Pour AK-SM 820A, 850A et 880A, utilisez la page Danfoss de la série 800A.
Au 15/10/2026, elle propose le paquet 5.3.x et le système Danux 4.14.017.194.



01 **AK-SM 800A : logiciel et système d’exploitation**

Ouvrir les téléchargements officiels Danfoss ↗.
Lisez les instructions, les prérequis et la compatibilité avant d’installer.

02 **Ancien AK-SM / AK-SC : support et migration**

Contacter Danfoss ↗.
Indiquez modèle, code, version et photos de l’étiquette.
N’utilisez pas de fichiers de forums ou d’un autre modèle.

03 **Copeland / Dixell XWEB : filière distincte**

Ouvrir System Software Updates ↗.
Sélectionnez la famille exacte et confirmez le correctif avec le fabricant ; n’étendez pas la matrice AK au XWEB.

Le firmware est le logiciel interne de l’équipement.
Danux est le système d’exploitation du 800A.
Notez les deux versions et suivez l’ordre d’installation exigé dans les notes du paquet.

Danfoss · téléchargements et instructions ↗

06 • COPELAND / DIXELL XWEB

XWEB EVO et PRO : vérifiez versions et support

L'alerte officielle inclut aussi Copeland/Dixell XWEB.
Le CERT-FR ne précise ni EVO/PRO ni versions ; les détails ci-dessous viennent de Copeland.

FAMILLE ET MODÈLES	FIRMWARE / SUPPORT	RECOMMANDATION
XWEB 300D PRO **XWEB 500D PRO** **XWEB 500B PRO**	Failles publiées dans les versions **jusqu'à 1.12.1 incluse.**	Passer en **1.13.0** ou version ultérieure compatible. La 1.13 corrige les failles du bulletin de février 2026.
XWEB 300D EVO **XWEB 500D EVO** **XWEB 500 EVO**	Aucune version sûre indiquée dans l'alerte. Support logiciel arrêté le **16/03/2026**.	Isoler de l'internet public et planifier la migration vers PRO. D'anciens fichiers ne prouvent aucun correctif de sécurité.
XWEB 3000 EVO **XWEB 5000 EVO**	Même fin de support que la famille EVO.	Isoler et remplacer par une solution supportée. Le firmware PRO ne s'applique pas à l'EVO.



PRO : attention à l'ordre. En mise à jour manuelle, les versions jusqu'à 1.2.1 doivent passer par la 1.3.0 avant la 1.13.0.
Vérifiez la procédure du modèle, faites une sauvegarde et validez la restauration avec l'intégrateur.

Téléchargements officiels : sélectionnez la famille et le modèle exacts ↗

Sources : CERT-FR ↗ · Copeland : modèles et versions ↗ · PRO 1.13 ↗ · EVO : fin du support ↗ · Ordre de mise à jour ↗

07 • PROTÉGER LA CONNEXION

Accès à distance par VPN ou réseau protégé

La DSI doit isoler le réseau froid et n’ouvrir que les accès nécessaires.
L’administration du routeur et du modem exige la même vigilance.

01 **Connexion permanente**

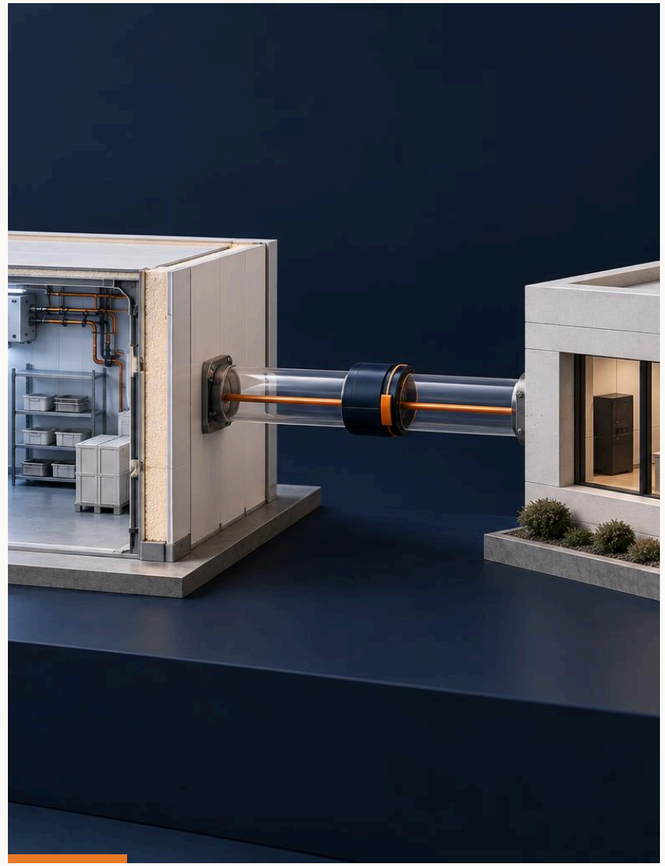
Utilisez un VPN ou un réseau protégé, des comptes nominatifs et l’authentification forte si disponible.
Séparez le froid du Wi-Fi et des ordinateurs du magasin.

02 **Mesure d’urgence**

Si un filtrage par adresse IP s’impose en attendant le VPN, limitez sources, ports et durée.
Notez qui l’a validé et la date de migration.

03 **Adresses sources du NEO 360**

Demandez à Estech la liste des adresses sources avant de fermer l’accès.
Les relevés continueront ainsi d’arriver après le changement.



Désactivez les services inutilisés et changez les mots de passe d’usine.
Le HTTPS, connexion web chiffrée, protège les échanges, mais ne remplace ni les mises à jour ni la restriction d’accès.

CERT-FR · VPN et filtrage d’urgence ↗ · Adresses sources du NEO 360 : demandez la liste à Estech.

08 • PLANIFIER LE CHANGEMENT

Fermez l’accès sans perdre la surveillance

DSI, intégrateur et Estech doivent convenir du changement et vérifier le résultat avant de clore l’intervention.

01 **Avant la fenêtre**

Notez modèle, firmware et connexion actuelle.
Faites une sauvegarde, prévoyez le retour arrière et gardez un technicien sur site.

02 **Pendant l’exécution**

Créez le chemin protégé et testez les intégrations.
Sur le 800A, vérifiez que le niveau de sécurité est sur Strict, qui impose HTTPS et contrôle de session.

03 **Avant la réception**

Vérifiez que l’interface n’est plus publique et que relevés, alarmes et lien avec le NEO 360 fonctionnent.

Si la surveillance est interrompue, la direction du magasin doit faire des rondes de température sur site, à la fréquence validée par la qualité.
Notez début, fin et responsable de l’interruption.

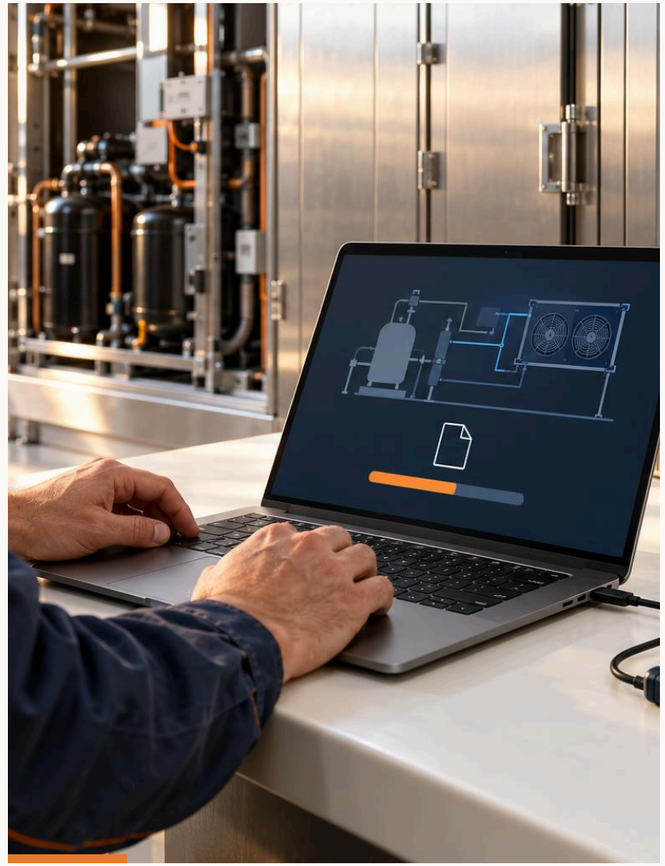


Danfoss · mode Strict et intégrations ↗

09 • PRÉPARER LA REPRISE

La sauvegarde doit permettre de reconstruire la configuration

Exportez la configuration de chaque superviseur avant la mise à jour et à chaque modification de paramètres importants.



01 **Paramètres d’exploitation**

Incluez consignes de température (setpoints), horaires et limites de dégivrage, alarmes, plannings, sondes et liens avec les régulateurs.

02 **Fichiers et dépendances**

Conservez l’export d’origine, les fichiers d’équipements, les licences le cas échéant, les versions, le manuel et les installeurs officiels nécessaires à la reprise.

03 **Identification et instructions**

Notez magasin, modèle, numéro de série, date, auteur et procédure de restauration.
Gardez mots de passe et clés dans un coffre-fort d’identifiants séparé.

> Vérifiez dans le manuel ce que contient l’export.
> La copie du superviseur peut ne pas inclure la configuration de chaque régulateur de terrain.
> Sauvegardez-les séparément si nécessaire.

10 • CONSERVER EN SÉCURITÉ

Gardez des copies hors de l’équipement et du magasin

Estech recommande la règle 3-2-1 comme référence : trois copies au total, sur deux supports, dont une hors site.

01 **Protection contre la modification**

Gardez au moins une copie déconnectée ou protégée en écriture.
En option : chiffrez-la, c’est-à-dire protégez sa lecture par une clé.

02 **Accès contrôlé**

Limitez l’accès à la DSI et aux responsables autorisés.
Gardez les clés dans un coffre séparé, avec un accès d’urgence testé.

03 **Historique des versions**

Conservez la configuration actuelle validée et les versions précédentes.
Après un incident, choisissez une copie antérieure à la modification frauduleuse et vérifiez son contenu.



Définissez une durée de conservation et vérifiez que les copies s’ouvrent.
Une copie gardée seulement sur le portable de l’intégrateur ou sur le superviseur crée un point unique de défaillance.

11 • PROUVER QUE CELA FONCTIONNE

Faites une vraie restauration

Un fichier exporté ne prouve pas que la reprise fonctionne.
Le test doit charger la copie dans un environnement compatible et valider le résultat.

01 **Préparer le test**

Utilisez un équipement de secours compatible ou un environnement validé par le fabricant.
S'il n'y a que l'unité en service, prévoyez une fenêtre supervisée et un plan de retour.

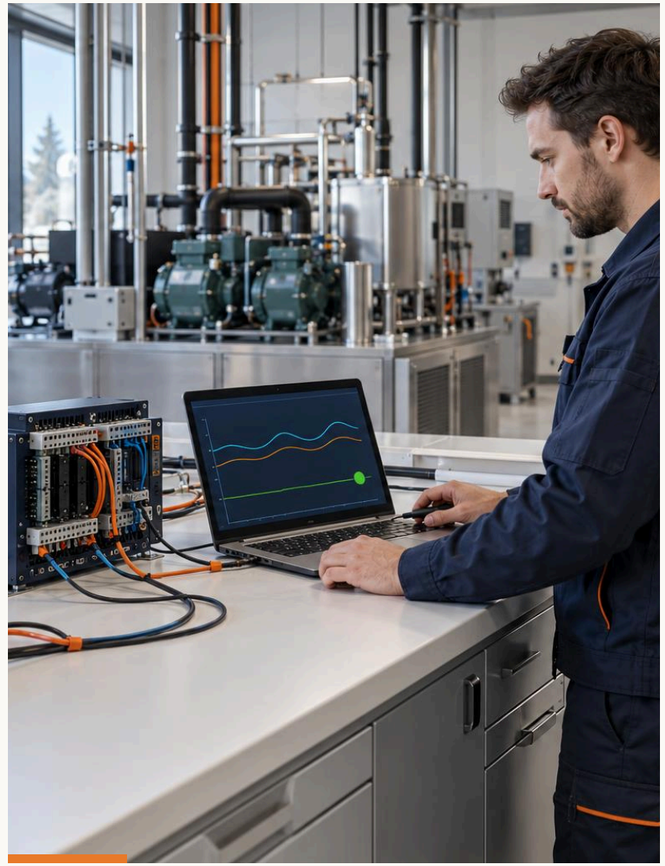
02 **Restaurer et vérifier**

Restaurez la configuration et comparez sondes, horaires, alarmes, accès et paramètres.
Vérifiez aussi la communication avec les régulateurs et le NEO 360.

03 **Consigner et corriger**

Notez fichier et version utilisés, durée, écarts et responsables.
En cas d'échec, corrigez le processus et recommencez jusqu'à la réception.

> Un simulateur aide à préparer, mais ne remplace pas le test sur l'équipement quand la reprise dépend d'interfaces physiques.
> L'essai ne doit ni déclencher de dégivrage ni modifier le froid d'un magasin en activité.



12 • DÉFINIR LA FRÉQUENCE

Choisissez un cycle de 3, 6 ou 12 mois

Les fréquences ci-dessous sont des recommandations d'Estech.
Décidez selon la criticité, la capacité de l'équipe et le temps de reprise acceptable.

3 mois

Exploitation critique

Nombreux magasins, fort impact d'un arrêt ou équipements anciens.
Revue complète et test réel de restauration à chaque cycle.

6 mois

Rythme recommandé

Organisation intermédiaire.
Revue complète et test réel de restauration chaque semestre, avec responsables désignés.

12 mois

Capacité limitée

Limite proposée pour une exploitation moins critique, avec risque accepté par la direction et test réel annuel.



N'attendez pas le prochain cycle pour traiter une alerte critique.
Mettez à jour la sauvegarde à chaque revue et après tout changement validé.
Réévaluez accès et reprise à chaque changement d'équipement, d'intégrateur, de réseau ou de firmware.
Appliquez les correctifs selon les bulletins et la compatibilité, sans attendre le calendrier.

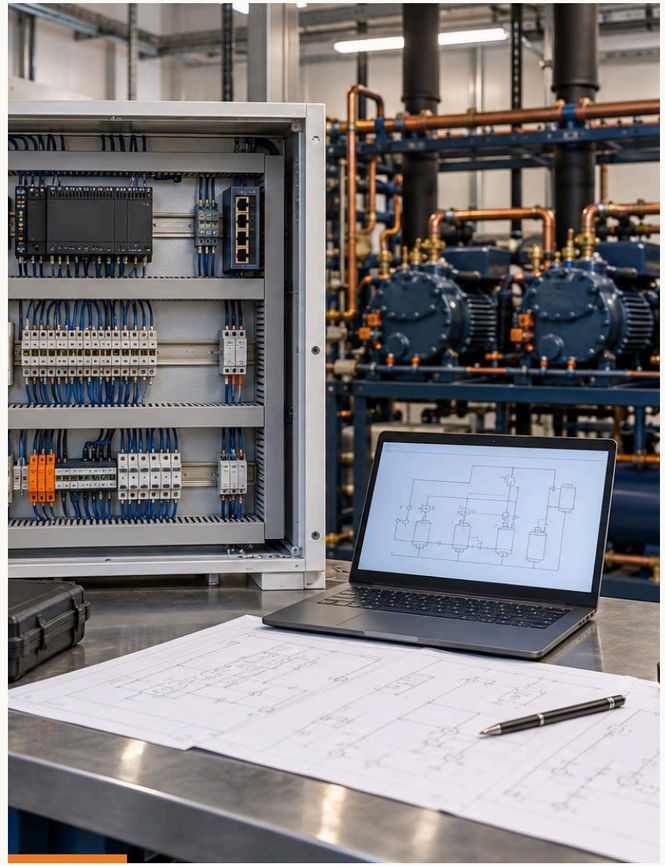
13 • ATTRIBUER LES RESPONSABILITÉS

Chaque magasin a besoin d’un responsable et de preuves

La direction valide le cycle et la priorité.
La DSI pilote la routine et consigne ce qui a été vérifié avec l’intégrateur et l’exploitation.

RESPONSABLE	LIVRABLE À CONSIGNER
Direction	Criticité, fréquence, budget, échéance et acceptation des risques résiduels.
Votre DSI	Inventaire, règles d’accès, comptes, emplacement des copies et prochaine revue.
Intégrateur / fabricant	Compatibilité, mise à jour, export et test réel de restauration.
Magasin / qualité	Contacts, protection des produits et validation de l’exploitation sur site.
Estech	Contrôle de l’intégration et des relevés dans le NEO 360, selon le périmètre convenu.

Fiche par magasin : actif et n° de série · firmware et Danux · responsable et suppléant · lieu de la sauvegarde · dernière restauration et durée · failles ouvertes · échéance · preuve de réception · prochaine revue.



14 • RÉPONDRE À L'INCIDENT

Protégez les produits et isolez l'accès à distance

Dégivrage imprévu, réglage modifié, hausse simultanée des températures : vérifiez sans délai, sans attendre la confirmation d'une attaque.

01 **Magasin et qualité : agir immédiatement**

Contrôlez les températures sur site, gardez les portes fermées et suivez le plan de protection ou de transfert des produits.
Notez les horaires.

02 **DSI et intégrateur : bloquer l'intrusion**

Isolez le chemin d'accès à distance identifié.
Ne coupez ni centrale, ni régulateurs, ni câbles sans en connaître la fonction : cela peut affecter la régulation du froid.

03 **Équipe responsable : alerter et préserver**

Alertez DSI, intégrateur et Estech.
Conservez journaux d'accès et photos avant la réinitialisation, si cela ne retarde pas la protection de l'exploitation.



Ces signes peuvent aussi avoir des causes opérationnelles.
L'équipe doit enquêter sans présumer de l'origine.
Si le relevé à distance est interrompu, maintenez le contrôle des températures sur site.

CERT-FR · confinement et reprise ↗

15 • REPARTIR DE ZÉRO

Reconstruisez l’équipement avant de le reconnecter

Après compromission, l’intégrateur fait la réinitialisation d’usine prévue par le fabricant, équipement isolé et exploitation protégée.

1. **Préserver et préparer.** Conservez les preuves et confirmez copie fiable, versions, licences et moyens de reprise.
2. **Réinitialiser.** Effectuez la réinitialisation d’usine et la réinstallation officielle si elle est prévue.
   « Formater » n’est pas une procédure universelle : suivez la méthode du modèle.
3. **Corriger et reconfigurer.** Installez les paquets officiels dans l’ordre du fabricant, changez les identifiants et chargez une configuration antérieure à l’incident, déjà vérifiée.
4. **Valider isolé.** Vérifiez paramètres, comptes, communication et fonctions locales.
   Appliquez les critères de réception de la page suivante.
5. **Reconnecter protégé.** Utilisez un VPN ou un réseau protégé et suivez l’exploitation avec Estech et le magasin.

> Sans firmware supporté, une réinitialisation laisse l’équipement exposé à la même faille.
> Maintenez l’isolement et validez le remplacement.
> Ne restaurez pas une configuration suspecte sans revue.



CERT-FR · Reset Factory et risque de nouvelle compromission ↗

16 • PRONONCER LA RÉCEPTION

Ne clôturez qu’après avoir vérifié l’exploitation

DSI, intégrateur et direction du magasin doivent consigner la réception.
Convenez avec Estech de la vérification du retour de la surveillance.

- Modèle et versions documentés, avec correctifs applicables ou isolement validé en vue du remplacement.
- Interface sans accès public ; chemin protégé et accès autorisés vérifiés.
- Comptes revus et mots de passe changés après l’incident, routeur et accès à distance compris.
- Consignes de température, dégivrages et alarmes comparés à la configuration validée.
- Relevés et communication dans le NEO 360 vérifiés ; test d’alarme sûr convenu avec l’exploitation.
- Nouvelle sauvegarde protégée, test de restauration consigné et prochaine revue planifiée.

> Définissez avant l’intervention la durée maximale acceptable sans superviseur et sans relevé.
> Mesurez la reprise et fixez la période de suivi selon la criticité du magasin.



RÉFÉRENCES • CONTACT

Sources à consulter et prochaines étapes

Commencez par l'inventaire de chaque magasin.
Priorisez l'exposition à internet, les équipements non supportés et l'absence de copie testée.

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

02 Danfoss · bulletins de sécurité DSA ↗

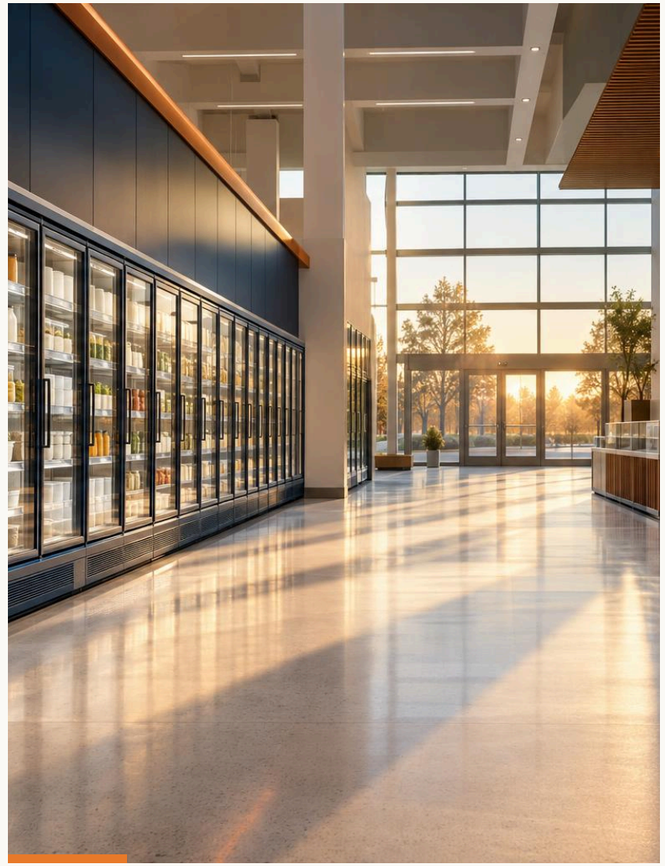
03 Danfoss · logiciel et Danux de l'AK-SM 800A ↗

04 Danfoss · fin de service des anciens modèles ↗

05 Copeland / Dixell · mises à jour XWEB ↗

06 Copeland · modèles et versions affectés ↗

07 Copeland · fin du support de la famille EVO ↗



SUPPORT ESTECH / JORNADA NEO

help@neoestech.com

En cas d'incident, alertez aussi les contacts d'urgence déjà convenus avec votre exploitation.

Rafael Cocchiaro | Head of Tech | Digital Tech