Vytalx

Checklist : Sauvegarde & Protection OT

Sécuriser la continuité de production : couverture, restauration, contraintes OT (30 minutes)

Vytalx

Comment utiliser cette checklist ?

Cochez chaque point selon votre situation.
L'objectif étant d'identifier rapidement les zones à risque
et de prioriser les actions qui améliorent réellement la résilience de votre infrastructure OT

Mode d'emploi

1. **Choisissez un périmètre :**
   Ligne/atelier, site, ou une "cellule" (SCADA, serveurs industriels, postes d'ingénierie, historien, postes opérateur)

2. **Cochez chaque point :**
   - ✅ Oui = en place et compatible production
   - ⚠️ Partiel = existe, mais incomplet / non standardisé / non prouvé
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   Inventaire, rapport, procédure, ticket, test daté, ou photo/capture (utile en OT).

Exemple

"Tests de restauration mensuels"

- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

Scoring simple

- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

Les 5 preuves attendues

1. Cartographie OT minimale (actifs critiques, dépendances, versions)
2. Dernier test de restauration daté (même partiel)
3. Procédure de reprise terrain (qui fait quoi, où sont les médias, accès)
4. Copie protégée contre suppression/chiffrement (ou mécanisme équivalent)
5. Journal des sauvegardes (succès/échecs) + traitement des échecs

Piège classique : Une sauvegarde "IT standard" peut être incompatible OT (fenêtres d'arrêt, matériel ancien, dépendances non documentées). En OT, la restauration doit être pensée "terrain".

Vytalx

Périmètre OT & criticité

Avant de cocher la checklist, identifiez ce qui doit repartir en priorité.
En OT, la dépendance au matériel, aux versions et aux configurations est déterminante.

Vos actifs OT critiques (à compléter)

Objectifs de reprise (RPO / RTO)

- **RTO :** délai maximal d'arrêt acceptable (par actif)
- **RPO :** perte de données acceptable (recettes, historiques, logs, paramètres)

Consigne : Renseignez un RTO/RPO cible même approximatif.
En OT, on précise aussi : "reprise sur matériel identique" ou "reprise tolérante au changement".

Périmètres à couvrir

Actif / Système	Criticité (Haute / Moyenne / Basse)	RTO cible (Nombres de jours)	RPO cible (équipe / personne)	Dépendances	Support matériel	Dernier test de restauration	Responsable terrain

Signaux de risque immédiat :

- Actifs critiques sans inventaire (versions, licences, dépendances)
- Matériel ancien / spécifique, sans pièce de rechange ni image restaurable
- Sauvegardes existantes mais aucun test de restauration daté
- Reprise dépendante d'une personne "clé" non remplaçable
- Sites distants : pas de procédure terrain ni kit de reprise

Vytalx

Checklist : Fondations OT (couverture & compatibilité production)

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Le périmètre OT critique est cartographié (actifs, versions, dépendances)	☐	☐	☐	☐	
Les systèmes OT critiques sont couverts par une sauvegarde (serveurs, SCADA, historian, postes d'ingénierie, configs)	☐	☐	☐	☐	
Les sauvegardes respectent les contraintes de production (fenêtres, performances, indisponibilité limitée)	☐	☐	☐	☐	
Les postes d'ingénierie sont inclus (souvent oubliés, mais critiques)	☐	☐	☐	☐	
Les configurations OT sont sauvegardées (projets, recettes, paramètres, fichiers de config)	☐	☐	☐	☐	
Les sauvegardes tiennent compte des versions figées (OS, drivers, applis, dépendances)	☐	☐	☐	☐	
Les licences et dépendances sont documentées (dongles, clés, serveurs de licence)	☐	☐	☐	☐	
Les chemins de restauration sont définis (sur matériel identique / alternatif)	☐	☐	☐	☐	
Les sauvegardes sont supervisées (échecs, absence d'exécution, dérive capacité)	☐	☐	☐	☐	
Les échecs sont traités rapidement (délai cible, responsabilité claire)	☐	☐	☐	☐	
La documentation de reprise est accessible sur site (même si le SI IT est indisponible)	☐	☐	☐	☐	
La reprise OT peut être déclenchée par une équipe non-IT (procédure terrain simplifiée)	☐	☐	☐	☐	

OT reality check :
En environnement industriel, "tout sauvegarder" ne suffit pas :
il faut savoir restaurer une version précise,
avec ses dépendances, dans un ordre maîtrisé, sur site.

Vytalx

Checklist : Résilience (anti-suppression & incident cyber en OT)

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Une copie OT est protégée contre suppression/modification (immutabilité ou mécanisme équivalent).	☐	☐	☐	☐	
Les accès admin sauvegarde OT sont séparés et protégés (MFA, comptes dédiés, moindre privilège)	☐	☐	☐	☐	
Le dépôt de sauvegarde est isolé (droits stricts, réseau segmenté, accès limité)	☐	☐	☐	☐	
Les postes OT n'ont pas d'accès direct aux dépôts (pas de partage "à plat")	☐	☐	☐	☐	
Une copie hors site / hors segment OT existe (selon faisabilité)	☐	☐	☐	☐	
Les sauvegardes OT ne dépendent pas d'un seul identifiant (break-glass / accès de secours)	☐	☐	☐	☐	
Procédure "incident cyber OT" documentée (restaurer propre, éviter réinfection)	☐	☐	☐	☐	
Reprise sur environnement isolé possible (au moins pour valider avant remise en prod)	☐	☐	☐	☐	
Surveillance des événements critiques sauvegarde (échecs, suppressions, changements de politique)	☐	☐	☐	☐	
Le réseau OT est segmenté (au minimum : séparation OT/IT et contrôle des flux)	☐	☐	☐	☐	
Accès distants OT maîtrisés (jump server, VPN, comptes nominatif, journalisation)	☐	☐	☐	☐	
Gestion des supports "terrain" (médias, exports, images) sécurisée et traçable	☐	☐	☐	☐	

Erreur fréquente : Une sauvegarde OT stockée sur un partage accessible depuis le domaine (ou depuis des postes) peut être chiffrée/supprimée en même temps que la production.

Vytalx

Checklist : Restaurabilité (tests terrain & preuves)

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Un test de restauration OT a été réalisé récemment (≤ 6 mois sur actifs critiques)	☐	☐	☐	☐	
Les tests couvrent au moins 2 niveaux (fichier/config → poste/serveur → service SCADA/MES)	☐	☐	☐	☐	
Les délais réels sont mesurés (RTO réel vs RTO cible)	☐	☐	☐	☐	
La perte de données est évaluée (RPO réel vs RPO cible : historian, recettes, configs)	☐	☐	☐	☐	
La restauration inclut les dépendances (drivers, versions, licences, certificats)	☐	☐	☐	☐	
La restauration est faisable sans IT central (procédure terrain)	☐	☐	☐	☐	
Un “kit de reprise site” existe (accès, docs, médias, contacts, pièces)	☐	☐	☐	☐	
Validation applicative réalisée (au-delà du démarrage : I/O, communications, recettes)	☐	☐	☐	☐	
Validation opérationnelle/métier (opérateur/maintenance)	☐	☐	☐	☐	
Ordre de reprise défini (dépendances réseau/serveurs → SCADA → postes → production)	☐	☐	☐	☐	
Procédure de retour en production (failback / remise en service) envisagée	☐	☐	☐	☐	
Les preuves sont conservées (tests, écarts, corrections) et réutilisables	☐	☐	☐	☐	
Après changement OT majeur, un test est déclenché (mise à jour, remplacement matériel)	☐	☐	☐	☐	
Scénario “incident cyber” testé ou au minimum simulé (restaurer propre)	☐	☐	☐	☐	

Règle d’or : En OT, la restauration se prouve sur le terrain : versions, dépendances, ordre de reprise et validation opérationnelle.

Vytalx

Synthèse & plan d'action

Votre résultat

Score total : ____ / ____

Niveau : ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

Barème :	**Calcul :**
✅ Oui = 2 pts ⚠️ Partiel = 1 pt ❌ Non = 0 pt	**Score obtenu** = somme des points **Score Max** = 2 × (nb de lignes évaluées)

Zones rouges

Vos 5 écarts prioritaires :

_____

_____

_____

_____

_____

Points bloquants

☐ Aucun test de restauration OT daté
☐ Inventaire OT incomplet (versions, dépendances, licences)
☐ Aucune copie protégée contre suppression/chiffrement
☐ Procédure de reprise terrain absente (non-IT)
☐ Dépôt non isolé / accessible depuis postes ou domaine

Plan d'action

Phase 1 : Cartographie & preuves minimales

- Finaliser la cartographie OT (actifs, versions, dépendances, licences)
- Identifier le top 5 critique + fixer des RTO/RPO cibles
- Mettre en place un reporting simple : jobs OK/KO + responsables

Phase 2 : Sécuriser la sauvegarde

- Mettre en place une copie protégée contre suppression/modification
- Isoler les dépôts (droits/réseau) + sécuriser les comptes admin
- Clarifier la stratégie multi-sites / sites distants

Phase 3 : Prouver la restauration

- Réaliser 2 tests terrain (config → service)
- Mesurer RTO/RPO réels + produire un CR (photos/captures)
- Documenter dépendances critiques (drivers, licences, accès)

Phase 4 : Standardiser la reprise

- Rédiger / simplifier le runbook terrain (qui fait quoi, ordre de reprise)
- Constituer le kit de reprise site (docs, accès, contacts, médias)
- Définir un déclencheur "test après changement OT majeur"

Évaluer une approche OT par briques, alignée sur vos contraintes et budget

Une approche par modules : activez uniquement les briques nécessaires (sauvegarde, protection, reprise, preuves), là où le risque et le coût d'arrêt le justifient.
L'objectif : sécuriser la continuité sans engager un chantier disproportionné.

contact/vytalx.fr contact@vytalx.fr