Vytalx

Note de cadrage : Cybersécurité des systèmes industriels (OT)

Périmètre, livrables et trajectoire pour une reprise démontrable.

Périmètre OT • Sauvegarde & reprise • Tests & preuves • Exploitation managée

Vytalx

Objectif

Sécuriser la continuité des opérations industrielles en structurant une capacité de sauvegarde et de reprise exécutable, testée et démontrable, adaptée aux contraintes OT.

Périmètre de cette note

Cette note de cadrage définit le périmètre OT à couvrir, les livrables attendus et une trajectoire de mise en œuvre. Elle vise à aligner les équipes IT/OT sur une approche pragmatique, centrée sur la disponibilité et la reprise.

Périmètre OT cible

Systèmes et environnements concernés :

- Postes d'exploitation et de supervision (HMI)
- Serveurs SCADA / supervision
- Serveurs d'ingénierie / postes de maintenance
- Historian / collecte industrielle
- Services d'infrastructure OT (AD local, fichiers, applicatifs OT, selon contexte)

Sites / zones :

- Sites de production et sites distants
- Zones OT critiques (cellules, lignes, ateliers), selon priorisation

Livrables attendus

1. **Inventaire OT priorisé :** actifs, criticité, dépendances majeures
2. **Stratégie de sauvegarde OT :** quoi / où / quand / combien de temps
3. **Objectifs de reprise :** RTO/RPO par service critique
4. **Runbook de restauration :** étapes, rôles, prérequis, points de contrôle
5. **Plan de tests :** scénarios, fréquence, critères de réussite
6. **Preuves exportables :** compte rendu de test daté + éléments de traçabilité

Vytalx

Contexte OT : contraintes et principes de conception

Les environnements industriels imposent des contraintes différentes de l'IT classique. Le cadrage doit donc viser une cybersécurité compatible avec l'exploitation : disponibilité, maîtrise des changements et reprise exécutable sur site.

Contraintes OT

En OT, l'arrêt de production a un coût immédiat et les fenêtres de maintenance sont limitées. Les systèmes sont souvent hétérogènes et parfois anciens, avec des dépendances fortes à des équipements et à des prestataires. La sécurité doit donc être conçue pour limiter les perturbations et favoriser des procédures simples, testées et reproductibles.

- **Disponibilité prioritaire :** éviter toute perturbation de la production
- **Legacy et hétérogénéité :** OS variés, applications spécifiques, contraintes éditeurs
- **Maintenance rare :** patching et changements plus lents
- **Sites distants :** autonomie locale, intervention parfois sans IT sur place
- **Dépendances fortes :** réseau, équipements, partenaires, sous-traitants

Risques opérationnels typiques

Les scénarios les plus fréquents combinent incident cyber et contrainte terrain : poste OT indisponible, serveur de supervision altéré, perte de configuration, ou indisponibilité d'un site. La priorité est d'éviter l'escalade et de pouvoir restaurer un service critique rapidement, sans improviser.

Principes de conception

Limiter l'impact : privilégier des mécanismes non intrusifs et industrialisables

Rendre la reprise exécutable : runbooks simples, rôles clairs, prérequis identifiés

Tester et prouver : tests datés, résultats observés, corrections suivies

Isoler et protéger la sauvegarde : éviter que l'incident n'altère la capacité de reprise

Standardiser : mêmes méthodes et preuves sur tous les sites

Objectif opérationnel :
restaurer un service critique en conditions réelles, avec une preuve exploitable et reproductible.

Vytalx

Structurer le périmètre : zones, dépendances et priorités

Les environnements industriels imposent des contraintes différentes de l'IT classique. Le cadrage doit donc viser une cybersécurité compatible avec l'exploitation : disponibilité, maîtrise des changements et reprise exécutable sur site.

Zones OT

Zone
Production / Cellule

Équipements et systèmes au plus près de la ligne

Zone
Supervision

HMI, SCADA, serveurs de supervision

Zone
Ingénierie / Maintenance

Postes et outils d'administration OT

Zone
Services OT

AD local, DNS, fichiers, Historian

Zone
Interconnexion IT / Accès distant

passerelles, bastion, VPN prestataires

Service OT critique	Dépendances clés	Opérateur / équipe	Mode de reprise attendu
Supervision (SCADA)	• Serveur • Réseau • Comptes	OT / IT	• Restauration • validation applicative
Postes HMI	• Poste • Image • Configuration	OT	• Remise en état rapide • Configuration
Historian	• Serveur • Stockage	OT / IT	• Restauration • Cohérence
Poste ingénierie	• Poste • Outils	OT	• Restauration • Contrôle d'intégrité

À prioriser dans l'ordre :

1. Ce qui stoppe une ligne
2. Ce qui permet de piloter/restaurer
3. Ce qui sert de point d'entrée

Vytalx

Exigences opérationnelles : mesures minimales et preuves attendues

L'objectif n'est pas d'empiler des contrôles, mais d'obtenir une capacité exécutable et démontrable. Pour chaque exigence ci-dessous, la preuve attendue doit être simple, exportable et reproductible.

Résilience et reprise

Exigence : pouvoir restaurer un service OT critique dans un délai compatible avec l'exploitation.

Preuves attendues :

- Test de restauration daté
- Résultat observé
- Compte rendu et actions correctives

Sauvegarde protégée contre l'altération

Exigence : garantir qu'une copie de sauvegarde reste disponible même en cas de compromission.

Preuves attendues :

- Configuration de stockage protégé et contrôle d'accès
- Règles de rétention documentées
- Revue périodique des échecs et des exceptions

Restauration "sûre"

Exigence : éviter de restaurer un système déjà compromis (ou altéré) sur un périmètre critique.

Preuves attendues :

- Procédure de contrôle avant restauration
- Résultat de contrôle sur un échantillon de sauvegardes
- Traçabilité des restaurations

Détection et qualification (OT/IT)

Exigence : réduire le temps de qualification et standardiser l'escalade en cas de signal faible ou d'incident.

Preuves attendues :

- Liste des signaux et journaux OT prioritaires et points de collecte
- Règles d'escalade
- Chronologie type d'incident

Exploitation et pilotage

Exigence : maintenir la posture dans la durée

Preuves attendues :

- Routine mensuelle
- Registre des écarts / exceptions
- Historique des corrections et re-tests

Vytalx

Capacités de mise en œuvre : rendre la reprise OT exécutable et démontrable

Une capacité OT efficace repose sur des mécanismes peu intrusifs, standardisables et exploitables à l'échelle. L'approche consiste à couvrir la sauvegarde, la restauration et la preuve, tout en s'intégrant dans l'existant IT/OT.

Sauvegarde et restauration OT

La base est de disposer d'une sauvegarde opérationnelle des systèmes OT critiques (postes et serveurs), avec une restauration fiable et reproductible. L'objectif est de pouvoir restaurer un poste ou un serveur OT sans réinstallation longue, puis de valider le bon fonctionnement applicatif.

Preuves attendues : rapports d'exécution, couverture par périmètre, restauration testée et datée.

Protection de la sauvegarde

La capacité de reprise dépend de la protection de la copie de sauvegarde : contrôle d'accès, rétention et mécanismes limitant l'altération ou la suppression. Cette protection permet de conserver une "ligne de vie" même si un incident touche le SI de production.

Preuves attendues : configuration de stockage protégé, règles de rétention, revue des échecs et exceptions.

Contrôle des sauvegardes avant restauration

Pour un périmètre OT critique, la restauration doit intégrer un contrôle préalable afin d'éviter de remettre en production un système déjà altéré. Le principe est de vérifier les sauvegardes (au minimum contre les codes malveillants) et de tracer les restaurations réalisées.

Preuves attendues : procédure de contrôle, résultat de scan sur un échantillon, journal des restaurations.

Pilotage et preuves exportables

Au-delà des opérations, l'industrialisation passe par le reporting : couverture, exécutions, échecs, tests, et éléments de preuve exportables. C'est ce pilotage qui permet d'objectiver la posture et de préparer une revue interne, une cyberassurance ou un audit.

Preuves attendues : reporting périodique, historique des tests, registre d'écarts et actions correctives.

Intégration dans l'existant

L'intégration doit éviter l'empilement : capitaliser sur les contraintes OT, les pratiques IT existantes, et les rôles terrain. La trajectoire est progressive : pilote sur un périmètre représentatif, généralisation, puis régime de croisière avec routines et tests réguliers.

Preuves attendues : périmètre pilote validé, critères de sortie, plan de généralisation, cadence de revue.

Vytalx

Plan de déploiement : pilote, généralisation, régime de croisière

Un déploiement OT doit minimiser le risque d'exploitation : on commence par un pilote représentatif, on valide la restauration en conditions réelles, puis on industrialise site par site avec des critères de sortie explicites.

Étape 1 : Cadrage & inventaire

Livrables :

- Inventaire OT priorisé (actifs, criticité, dépendances)
- RTO/RPO préliminaires par service critique
- Architecture cible de sauvegarde (où et comment)

Critères de succès :

- Périmètre validé IT/OT
- Liste des systèmes critiques signée et versionnée
- Première stratégie de sauvegarde documentée

Étape 2 : Pilote

Livrables :

- Sauvegarde opérationnelle sur le périmètre pilote
- 1 à 2 scénarios de restauration testés (poste + serveur, par exemple)
- Runbook de restauration + compte rendu de test

Preuves attendues :

- Test daté réalisé, résultat validé (temps observé, étapes, validation)
- Écarts identifiés et corrigés
- Règles d'exploitation et d'alerte définies

Étape 3 : Généralisation

Livrables :

- Déploiement progressif par zones/sites
- Reporting de couverture et de réussite
- Registre d'écarts/exceptions

Critères de sortie :

- Couverture des systèmes critiques atteinte
- Taux d'échec maîtrisé et traité
- Preuves exportables disponibles par site

Étape 4 : Régime de croisière

Livrables :

- Tests périodiques planifiés
- Revue mensuelle : échecs, changements, exceptions
- Amélioration continue

Critères de sortie :

- Tests récurrents réalisés et tracés
- Écarts traités dans des délais définis
- Capacité de reprise démontrable à tout moment

Vytalx

Annexes :
Outils de cadrage et modèles de preuve

Checklist de cadrage OT

- ☐ Les services OT critiques sont listés et priorisés (par site / ligne).
- ☐ Les dépendances majeures sont documentées (réseau, comptes, stockage, prestataires).
- ☐ Les fenêtres de maintenance et contraintes d'exploitation sont formalisées.
- ☐ Les RTO/RPO cibles sont définis pour chaque service critique.
- ☐ Les points d'entrée (accès distant, prestataires, interco IT) sont identifiés.
- ☐ Le périmètre pilote est choisi (représentatif, validé par l'exploitation).
- ☐ Le stockage de sauvegarde est défini et protégé (accès, rétention).
- ☐ Les rôles et responsabilités sont clarifiés (IT/OT/prestataires).
- ☐ Les scénarios de test sont définis (poste, serveur, perte config, indisponibilité).
- ☐ Les preuves attendues sont listées (rapport, CR test, journal, actions correctives).

Modèle de compte rendu de test de restauration

Compte rendu de restauration

Test n° : … / **Date :** … / **Site :** …

Service restauré : … (SCADA / HMI / Historian / poste ingénierie / etc.)

Scénario : … (poste indisponible / serveur altéré / perte config / etc.)

Objectif (RTO/RPO) : RTO … / RPO …

Étapes réalisées :

1.
2.
3.

Résultat :

Temps total observé : …

Validation applicative : Oui / Non (commentaire)

Écarts constatés : …

Actions correctives :

Preuves jointes : rapport / capture / export / journal / etc.

Validation : OT … / IT … / Prestataire …