Fondamentaux BOS – Infrastructure numérique et supervision

Cours sur l'infrastructure numérique en BOS (Building Operating System), IT/OT, modèles en couches, supervision avancée (KPI, alertes, observabilité), cybersécurité (défense en profondeur, NIS 2, IEC 62443), droits d'accès (RBAC/ABAC, segmentation Purdue), MCO et PRA/PCA bâtiment, détection d'anomalies (statistique et ML).

Systèmes 60 min de lecture Niveau Avancé

Document généré le 27/06/2026 à 21h38 · nouvy.fr/wiki/fondamentaux-bos-infrastructure-supervision

Sommaire

57 section(s) · 60 min de lecture

Cours sur l'infrastructure numérique dans le contexte du BOS (Building Operating System), la convergence IT/OT, les modèles en couches et la supervision avancée.

Introduction

Ce cours couvre les fondamentaux de l'infrastructure numérique appliquée au bâtiment intelligent : définition ingénieur, opposition IT/OT, niveaux d'infrastructure, chaîne de valeur de la donnée, typologies d'architectures et enjeux techniques. Il aborde ensuite la supervision en approche avancée (définition experte, supervision vs observabilité, axes de supervision BOS) et les indicateurs, alertes et observabilité. Des travaux pratiques de cartographie d'infrastructure et de stratégie de supervision complètent la formation.

Objectifs d'apprentissage

- Définir l'infrastructure numérique et la situer dans un BOS (approche hybride IT/OT).
- Distinguer IT et OT et comprendre la zone de convergence BOS.
- Maîtriser le modèle en couches (terrain, contrôle, supervision, BOS/IT).
- Décrire la chaîne complète de valeur de la donnée et les typologies d'architectures.
- Définir la supervision experte et la distinguer de l'observabilité.
- Identifier les KPI techniques et bâtiment, et les types d'alertes (simples et avancées).
- Réaliser une cartographie d'infrastructure et une stratégie de supervision opérationnelle.

Prérequis

- Notions de base en systèmes et réseaux.
- Intérêt pour le bâtiment connecté et la donnée.

---

1. Fondamentaux de l'infrastructure numérique

1.1 Définition (approche ingénieur)

Infrastructure numérique : ensemble cohérent de ressources matérielles, logicielles, réseau et organisationnelles permettant :

- la **collecte** des données ;
- le **transport** des données ;
- le **traitement** des données ;
- le **stockage** des données ;
- l'**exploitation** des données.

Dans un BOS (Building Operating System), l'infrastructure est **hybride IT / OT** : elle associe le monde informatique (serveurs, applications, données) et le monde opérationnel (automates, capteurs, bus terrain).

1.2 IT vs OT (fondamental)

IT	OT
Serveurs	Automates
Applications	Capteurs
Réseaux IP	Bus terrain
Données structurées	Données physiques (mesures)
Virtualisation	Temps réel

Points clés :

- Le **BOS** est la zone de **convergence IT/OT**.
- La **supervision** doit couvrir **les deux mondes** (technique et métier).

1.3 Niveaux d'infrastructure (modèle en couches)

Niveau 0 – Terrain

- Capteurs
- Actionneurs
- Mesures physiques

Niveau 1 – Contrôle

- Automates
- Régulation
- Logique locale

Niveau 2 – Supervision

- SCADA / GTB (Gestion Technique du Bâtiment)
- Interfaces opérateurs

Niveau 3 – BOS / IT

- Serveurs
- Données
- APIs
- Dashboards

Erreur classique : superviser uniquement le niveau 3, alors que les pannes naissent souvent au niveau 0 ou 1. Une vision transversale des couches est indispensable.

---

2. Architecture d'un BOS – Version détaillée

2.1 Chaîne complète de valeur de la donnée

Flux typique :

1. **Phénomène physique** (température, présence, etc.)
2. **Capteur** (mesure)
3. **Automate** (acquisition, logique)
4. **Gateway** (convergence protocoles)
5. **Réseau** (transport)
6. **Serveur** (agrégation)
7. **Base de données** (stockage)
8. **Analyse** (traitement)
9. **Décision** (consignes, alertes, rapports)

Chaque maillon peut tomber en panne. La **supervision doit être transversale** sur toute la chaîne.

2.2 Typologies d'architectures

Type	Caractéristiques	Avantages	Inconvénients
Centralisée	Données centralisées, décisions globales	Vision unifiée, simplicité de déploiement	Risque de SPOF (Single Point of Failure)
Distribuée	Intelligence locale, traitement en bord de champ	Résilience, réactivité	Complexité accrue, coordination à gérer
Hybride (cas réel BOS)	Local pour le critique, central pour l'analytique	Compromis réaliste pour le bâtiment	Nécessite une conception claire des périmètres

2.3 Enjeux techniques

- **Disponibilité** (24/7) : continuité de service.
- **Latence** : temps de remontée et de réaction.
- **Volume de données** : capacité à ingérer et stocker.
- **Interopérabilité** : protocoles et formats (OT/IT).
- **Scalabilité** : évolution du nombre de points et des usages.

La transition vers des architectures scalables et résilientes est naturelle dès que le volume et la criticité augmentent.

2.4 Exemple BOS réel

Contexte : immeuble tertiaire – 12 étages.

- 3 000 capteurs
- 120 automates
- 1 plateforme BOS
- 1 supervision énergétique

Question clé : que se passe-t-il si un automate cesse de publier des données ? Sans supervision adaptée (détection d'absence de données, alertes sur équipements silencieux),

on est en **aveuglement total** sur une partie du bâtiment.

---

3. Supervision – Approche avancée

3.1 Définition experte

Supervision : discipline consistant à observer l'état, le comportement et la performance d'un système complexe, afin de :

- **détecter** les anomalies ;
- **anticiper** les défaillances ;
- **déclencher** des actions correctives.

Elle s'appuie sur des métriques, des seuils, des tableaux de bord et des procédures.

3.2 Supervision vs Observabilité

Supervision	Observabilité
Seuils prédéfinis	Comportements et corrélations
Alertes sur états connus	Analyse d'états émergents
Réactif	Proactif
Métriques ciblées	Traces, logs, métriques combinées

L'observabilité va au-delà de la supervision classique ; la **data science** et l'analyse de tendances trouvent ici leur place (détection d'anomalies, prédiction).

3.3 Axes de supervision BOS

- **Technique** : CPU, RAM, réseau, disponibilité des serveurs et des équipements.
- **Fonctionnel** : cohérence des données (ex. température plausible), données plausibles, logique métier.
- **Métier** : performance énergétique, confort usager, respect des consignes.

3.4 Supervision comme prérequis à l'IA

- **Sans supervision** : données de mauvaise qualité ou incomplètes → apprentissage biaisé, décisions dangereuses.
- **Avec supervision** : qualité de la donnée maîtrisée → bases saines pour modèles et IA.

La supervision est donc un **prérequis** à toute exploitation avancée (analytics, IA) en BOS.

---

4. Indicateurs, alertes et observabilité

4.1 KPI techniques

- Taux de **disponibilité** des équipements et des services.
- **Temps de réponse** (requêtes, APIs).
- **Perte de paquets** (réseau).
- **Taux de données manquantes** (points non remontés).

4.2 KPI bâtiment

- **Dérive énergétique** (écart par rapport à une référence ou une tendance).
- **Incohérence capteurs** (ex. capteurs contradictoires sur une même zone).
- **Équipements silencieux** (plus de remontée de données).
- **Non-respect des consignes** (température, éclairage, etc.).

4.3 Types d'alertes

Alertes simples :

- Seuil dépassé (température, puissance, etc.).

Alertes avancées :

- **Absence de données** : un équipement ou un point ne remonte plus.
- **Valeur aberrante** : mesure hors plage plausible.
- **Rupture de tendance** : changement de régime (dérive, panne naissante).

Ces mécanismes constituent la base de la **détection d'anomalies** (approfondie en séances dédiées).

---

5. Introduction à la cybersécurité

5.1 Définition

Cybersécurité : ensemble des moyens techniques, organisationnels et humains mis en œuvre pour protéger les systèmes d'information, les équipements et les données contre les menaces (accès non autorisé, compromission, destruction, indisponibilité).

Dans un contexte BOS, elle couvre :

- l'**IT** classique (serveurs, applications, réseaux) ;
- l'**OT** (automates, capteurs, bus terrain) — historiquement peu sécurisé ;
- la **zone de convergence IT/OT** — surface d'attaque amplifiée.

5.2 Piliers DIC (Disponibilité, Intégrité, Confidentialité)

Pilier	Définition	Exemple BOS
Disponibilité (A)	Le service reste accessible quand il le faut	Redondance des serveurs SCADA
Intégrité (I)	La donnée n'est pas altérée (en transit ou au repos)	Signature des consignes envoyées aux automates
Confidentialité (C)	Seuls les acteurs autorisés accèdent aux données	Chiffrement des remontées capteurs

Ajouts fréquents : **traçabilité** (logs) et **non-répudiation** (preuve d'action).

5.3 Menaces spécifiques BOS / OT

- **Malwares OT** : Stuxnet, Triton/Trisis, Industroyer — ciblent automates et SCADA.
- **Rançongiciels** : chiffrement des serveurs de supervision → arrêt bâtiment.
- **Attaques sur la chaîne d'approvisionnement** : équipements compromis avant installation.
- **Menaces internes** : erreur ou malveillance d'un opérateur avec accès physique/logique.
- **Shadow IT/OT** : équipements non déclarés connectés sans contrôle.

5.4 Cadre réglementaire

- **NIS 2** : directive européenne — élargit le périmètre aux bâtiments et infrastructures critiques.
- **RGPD** : données personnelles (badges, caméras, présence, comptage).
- **LPM** (Loi de Programmation Militaire) : opérateurs d'importance vitale (OIV).
- **ISO/IEC 27001** : management de la sécurité de l'information.
- **IEC 62443** : référentiel spécifique systèmes d'automatisation industrielle.

5.5 Défense en profondeur

Principe : **plusieurs couches de protection** pour qu'une faille ne suffise pas à compromettre l'ensemble.

1. **Physique** — contrôle d'accès aux locaux techniques, armoires verrouillées.
2. **Réseau** — segmentation, VLAN, DMZ, pare-feu inter-couches.
3. **Système** — durcissement OS, patch management.
4. **Application** — authentification forte, moindre privilège.
5. **Données** — chiffrement, sauvegarde, contrôle d'intégrité.
6. **Humain** — sensibilisation, formation, procédures.

---

6. Sécurisation et droits d'accès aux ressources

6.1 Principe du moindre privilège

Règle : chaque utilisateur, processus ou équipement ne dispose **que des droits strictement nécessaires** à sa fonction — ni plus, ni moins.

Application BOS :

- un technicien CVC → accès CVC uniquement ;
- un SCADA → lecture sur les capteurs, écriture sur les automates de son périmètre ;
- un prestataire externe → accès temporaire, tracé, limité dans le temps.

6.2 Authentification (AuthN) et autorisation (AuthZ)

Authentification : prouver **qui on est**.

- Mot de passe (faible si utilisé seul).
- **MFA / 2FA** (SMS, TOTP, clé FIDO2) — recommandé.
- Certificats (équipements, machines, services).
- Biométrie (badge + empreinte).

Autorisation : déterminer **ce qu'on a le droit de faire**.

- **RBAC** (Role-Based Access Control) — droits par rôle (technicien, exploitant, admin).
- **ABAC** (Attribute-Based Access Control) — droits selon attributs (heure, localisation, type de demande).
- **MAC / DAC** — obligatoire (politique imposée) / discrétionnaire (propriétaire décide).

6.3 Gestion des identités (IAM)

- **Annuaire central** (LDAP, Active Directory, Entra ID) : source unique de vérité.
- **SSO** (Single Sign-On) : une authentification unique pour plusieurs services.
- **Provisionnement automatisé** : création/suppression des comptes liées au cycle RH.
- **Revue périodique** des droits : trimestrielle minimum, annuelle impérative.

6.4 Segmentation réseau — modèle Purdue adapté BOS

Niveau	Zone	Typologie
5	Entreprise IT	Bureautique, internet
4	Zone tampon / DMZ	Historians, passerelles
3	BOS / MES	Supervision, données
2	Supervision locale	SCADA, IHM
1	Contrôle	Automates (PLC)
0	Terrain	Capteurs, actionneurs

Règle clé : les flux entre niveaux passent par une **DMZ** avec pare-feu ; **aucune liaison directe** entre IT et OT profond.

6.5 Sécurisation des accès distants

- **VPN** avec MFA pour les mainteneurs.
- **Bastion** (jump server) : point d'entrée unique, enregistrement de session.
- **Accès just-in-time** : droits temporaires et expirables.
- **Jamais d'accès direct internet** sur les équipements OT.

6.6 Traçabilité et audit

- **Logs centralisés** (SIEM) : toutes les authentifications, accès, actions critiques.
- **Rétention** : 6 mois minimum, 1 an recommandé, davantage selon la réglementation.
- **Alertes SIEM** : comportements anormaux (connexion hors plage, escalade de privilèges).
- **Revue** : audit régulier des logs et des droits.

6.7 Protection des données

- **Chiffrement en transit** : TLS 1.2+ (HTTPS, MQTT-S, OPC UA sécurisé).
- **Chiffrement au repos** : bases de données, sauvegardes, postes.
- **Gestion des secrets** : coffres-forts (HashiCorp Vault, Azure Key Vault, AWS Secrets Manager).
- **Jamais de mot de passe en clair** dans les scripts ou fichiers de configuration.

---

7. MCO – Maintien en Condition Opérationnelle (PRA/PCA bâtiment)

7.1 Définition

MCO (Maintien en Condition Opérationnelle) : ensemble des activités et processus visant à garantir le **fonctionnement nominal** d'un système sur la durée, à travers :

- la **maintenance préventive** (planifiée, périodique) ;
- la **maintenance corrective** (sur incident) ;
- l'**évolution** (mises à jour, patches, améliorations) ;
- le **suivi de performance** (KPI MCO).

Objectif : préserver la **disponibilité**, la **performance** et la **sécurité** du BOS dans la durée.

7.2 Indicateurs MCO

- **MTBF** (Mean Time Between Failures) — durée moyenne entre deux pannes.
- **MTTR** (Mean Time To Repair) — temps moyen de réparation.
- **MTTD** (Mean Time To Detect) — temps entre panne et détection.
- **Taux de disponibilité** : `Disponibilité = MTBF / (MTBF + MTTR)`.

Niveau	Disponibilité	Indispo / an
99 %	"Deux neufs"	~3,65 jours
99,9 %	"Trois neufs"	~8h46
99,99 %	"Quatre neufs"	~52 min
99,999 %	"Cinq neufs"	~5 min

Autres KPI : taux de succès des sauvegardes, âge du dernier patch, nombre d'incidents majeurs.

7.3 Politique de sauvegarde — règle 3-2-1

- **3** copies de la donnée
- **2** supports différents
- **1** copie **hors site** (offline ou immuable)

À définir contractuellement :

- **RPO** (Recovery Point Objective) — perte de données acceptable (ex. 1h).
- **RTO** (Recovery Time Objective) — temps de remise en service (ex. 4h).

Règle absolue : tests de restauration périodiques et documentés. Une sauvegarde non testée = pas de sauvegarde.

7.4 PCA – Plan de Continuité d'Activité

PCA : ensemble de mesures permettant à l'activité de **continuer malgré un sinistre** — sans interruption ou avec interruption minimale.

Exemples BOS :

- redondance des automates critiques ;
- supervision de secours sur site distant ;
- alimentation : onduleurs + groupes électrogènes ;
- **modes dégradés** : pilotage manuel si la supervision tombe ;
- procédures opérationnelles testées régulièrement.

7.5 PRA – Plan de Reprise d'Activité

PRA : procédures et ressources permettant de **redémarrer** le SI après un sinistre majeur (incendie, inondation, cyberattaque destructrice, perte de site).

Composantes :

- **Site de repli** (chaud, tiède ou froid) — choix selon RTO/RPO ;
- **Sauvegardes externalisées** + procédures de restauration ;
- **Arbre de décision** : qui décide du déclenchement, et quand ;
- **Tests PRA** — exercices annuels minimum ;
- **Documentation à jour** : schémas, configurations, contacts, procédures.

7.6 Spécificités bâtiment

Un **PRA/PCA bâtiment** doit prendre en compte :

- **Continuité de service usager** : éclairage, CVC, accès, sécurité incendie ;
- **Priorisation** : zones critiques (data center, salle serveurs) vs zones de confort ;
- **Modes dégradés physiques** : commandes manuelles si automates hors-service ;
- **Interdépendances** : BOS ↔ SSI (Sécurité Incendie) ↔ GTB ↔ alarmes ;
- **Coordination** multi-acteurs : exploitation, maintenance, sécurité, DSI, prestataires.

7.7 Gestion des vulnérabilités et patching

- **Veille sécurité** : CERT-FR, CISA, éditeurs, alertes équipementiers.
- **CVSS** : scoring des vulnérabilités (gravité de 0 à 10).
- **Fenêtres de maintenance** : planification hors heures de pointe.
- **Validation préalable** des patchs en environnement de test — critique en OT.
- **Rollback** documenté pour chaque changement.

7.8 Documentation vivante

- **DAT** (Dossier d'Architecture Technique) maintenu à jour.
- **Cartographie** des équipements et des flux.
- **Runbooks** : procédures pas-à-pas pour les incidents fréquents.
- **Plan d'astreinte** : qui contacter, quand, comment.

---

8. Détection des anomalies

8.1 Objectifs

Aller au-delà des alertes simples (seuils) pour identifier :

- des **états émergents** non prévus par les règles ;
- des **dérives progressives** (panne naissante) ;
- des **corrélations** anormales entre signaux.

8.2 Méthodes statistiques (classiques)

- **Seuils statiques** : min/max absolus (simple, mais peu fin).
- **Seuils adaptatifs** : moyennes mobiles, saisonnalité.
- **Z-score / écart-type** : mesure hors de N×σ = anomalie.
- **IQR** (Interquartile Range) : détection d'outliers.

8.3 Méthodes par apprentissage (machine learning)

- **Isolation Forest** — isole les points rares.
- **DBSCAN** — clustering, points hors cluster = anomalies.
- **Autoencodeurs** (réseaux de neurones) — forte erreur de reconstruction = anomalie.

- **LSTM** (séries temporelles) — écart entre valeur prédite et observée.

8.4 Cas d'usage BOS

Phénomène	Signal	Méthode recommandée
Équipement silencieux	Absence de données > seuil	Heartbeat + watchdog
Dérive de consommation	Courbe énergétique	Saisonnalité + écart-type
Capteur bloqué	Valeur constante anormalement longue	Stationnarité
Zone incohérente	Températures contradictoires	Corrélation multi-capteurs
Panne naissante CVC	Vibrations, températures, courants	ML multivarié

8.5 Pipeline de détection

1. **Collecte** — métriques temps réel + historiques.
2. **Prétraitement** — nettoyage, agrégation, normalisation.
3. **Modélisation** — choix de la méthode selon le signal.
4. **Seuillage / scoring** — décision binaire ou score.
5. **Alerte & contexte** — enrichissement (localisation, criticité, historique).
6. **Feedback** — qualifier les alertes (vrai/faux positif) pour améliorer le modèle.

8.6 Pièges à éviter

- **Fatigue d'alerte** : trop d'alertes → plus personne ne lit.
- **Modèle entraîné sur données polluées** : garbage in, garbage out.
- **Absence de boucle de retour** : modèle qui ne s'améliore jamais.
- **Confusion anomalie statistique / anomalie métier** : une anomalie statistique n'est pas toujours une alerte opérationnelle.

8.7 Qualité de la donnée (prérequis)

Une détection fiable suppose :

- **Complétude** — peu de trous.
- **Fraîcheur** — latence maîtrisée.
- **Exactitude** — capteurs calibrés et vérifiés.
- **Traçabilité** — savoir d'où vient chaque mesure.

Boucle vertueuse : **supervision → qualité → détection → IA → optimisation**.

---

9. Travaux pratiques

TP 1 – Cartographie d'infrastructure

Objectif : comprendre où se situent les risques dans une infrastructure BOS.

Énoncé : vous êtes responsable de la supervision d'un bâtiment connecté.

- Dessinez l'**architecture complète** (couches 0 à 3, flux de données).
- Identifiez : **points critiques**, **dépendances**, **flux de données**.
- Classez les composants par **criticité**.

Livrable : schéma commenté + justification orale.

TP 2 – Stratégie de supervision

Objectif : passer de l'infrastructure à une stratégie opérationnelle.

Énoncé : à partir de votre architecture (TP 1),

- Définissez : **quoi** superviser, **comment**, **pourquoi**.
- Proposez : **au moins 5 KPI**, **3 types d'alertes**.
- Expliquez les **conséquences** si la supervision échoue (technique, métier, données, IA).

Niveau attendu : raisonnement systémique, justification technique, vision long terme (MCO, qualité des données, préparation à l'IA).

TP 3 – Audit de sécurité et matrice d'accès

Objectif : appliquer les principes de moindre privilège et de segmentation à un BOS réel.

Énoncé : pour le bâtiment du TP 1,

- Identifiez les **acteurs** (rôles) : exploitant, technicien CVC, technicien GTB, prestataire externe, admin DSI, usager.
- Construisez une **matrice d'accès** (RBAC) : qui a le droit de faire quoi sur quel périmètre.
- Proposez un **schéma de segmentation réseau** façon Purdue (niveaux 0 à 5, DMZ, règles de flux).
- Listez **3 menaces** prioritaires et les **mesures** (techniques et organisationnelles) associées.

Livrable : matrice d'accès + schéma de segmentation + plan d'action menaces.

TP 4 – PCA/PRA pour un bâtiment tertiaire

Objectif : construire un plan de continuité et de reprise d'activité opérationnel.

Énoncé : le bâtiment subit un sinistre majeur (incendie salle serveurs).

- Identifiez les **services critiques** (CVC zones sensibles, sécurité incendie, accès, éclairage sécurité).
- Définissez **RPO** et **RTO** par service.
- Proposez un **PCA** : redondances, modes dégradés, procédures de bascule.
- Rédigez un **PRA** : site de repli, stratégie de sauvegarde 3-2-1, arbre de décision,

chronologie de reprise.
- Définissez **5 KPI MCO** pour piloter la démarche.

Livrable : document PCA/PRA synthétique (2–3 pages) + tableau de KPI MCO.

- L'**infrastructure** est un **système complexe** (matériel, logiciel, réseau, organisation).
- La **supervision** est un **outil d'aide à la décision** et un levier de performance.
- **Sans supervision** → pas de maîtrise de la performance → pas d'IA fiable.
- La **cybersécurité** et la **gestion des droits** sont des prérequis non négociables dès qu'un bâtiment est connecté.
- Le **MCO** et les plans **PRA/PCA** garantissent la continuité de service et la résilience face aux sinistres.
- La **détection d'anomalies** transforme la supervision en levier proactif (détection précoce, prédiction).
- Le **BOS** est un objet à la croisée de l'**IT**, du **bâtiment** et de la **donnée** ; la supervision, la sécurité et la résilience doivent couvrir ces trois dimensions.