HYPERVISION

PLATEFORME UNIFIÉE



UN CADRE COMMUN POUR COMPRENDRE, DÉCIDER ET AGIR.





Participer à l'AN2V,
c'est gagner du temps, élargir son réseau
et construire la sécurité de demain, ensemble !

TRAVAIL COLLECTIF DES MEMBRES DE L'AN2V

Ce LIVRE BLANC est le fruit d'un travail collectif mené par les membres de l'AN2V.

Leur engagement, leur disponibilité et la qualité des échanges ont permis de confronter les points de vue, d'enrichir les analyses et de rester fidèles à ce qui fait l'identité de l'Association depuis son origine : partir des contraintes réelles des élus locaux, du droit en vigueur et des capacités opérationnelles nécessaires sur nos territoires.

PAR ORDRE ALPHABÉTIQUE !

ACTIA · advancis · ALYCE Outsmart mobility · AXON · AZURSOFT Solutions de sécurité unifiée · CASD Solutions de vidéoprotection
DG Advisory Global · prysm · simple help · sopra steria · UBICITÉ

SOMMAIRE

Travail COLLECTIF DES **MEMBRES DE L'AN2V** 3

1. AVANT-PROPOS 6
1.1. Positionnement du Groupe de Travail Plateforme Unifiée Scalable 6
1.1.1. Articulation avec les autres GT AN2V (R2A, Cloud) 6
1.1.2. Publics cibles et usages du document 6
1.1.3. Distinction des espaces juridiques et opérationnels 7
1.2. Pourquoi un livre blanc PUS 8
1.2.1. Pourquoi la PUS est devenue un sujet stratégique 8
1.2.2. Ce que ce livre blanc n'est volontairement pas 8

INTRODUCTION

2. INTRODUCTION GÉNÉRALE 12
2.1. Limites de l'approche historique 12
2.1.1. Silos métiers et fragmentation 12
2.1.2. Limites des architectures existantes 13
2.2. Clarification des notions clés 14
2.2.1. De la supervision à la PUS : évolution des approches 14
2.2.2. Enjeux architecturaux et opérationnels 15

3. COMPRENDRE LA PUS 17
3.1. Ce que permet une PUS 17
3.1.1. Vision globale, cohérence opérationnelle et aide à la décision 17
3.2. Ce que la PUS ne fait pas 19
3.2.1. Absence de décision automatisée 20
3.2.2. Mythes fréquents autour de l'hypervision et de l'IA 21

4. INVARIANTS ET PRINCIPES FONDATEURS 22
4.1. La PUS comme socle commun multi-contextes 22
4.1.1. Invariants fonctionnels 22
4.1.2. Invariants organisationnels 23
4.2. Architectures de référence 24
4.2.1. Centralisée, distribuée, hybride 26
4.2.2. Avantages, limites et contextes d'usage 27
4.2.3. Synchronisation temporelle et cohérence des événements 28
4.3. Interopérabilité et résilience opérationnelle 29
4.3.1. Gouvernance des accès et des habilitations 30
4.3.2. Continuité opérationnelle et fonctionnement en mode dégradé 31
4.4. Souveraineté, maîtrise et pérennité des architectures 32
4.4.1. Dépendance technologiques éditeur et réversibilité 32
4.4.2. Localisation, gouvernance et maîtrise des données 33
4.4.3. Pérennité et évolutivité des architectures 34

PARTIE 1 : PUS EN ESPACES OUVERTS AU PUBLIC

5. PUS EN ESPACES OUVERTS AU PUBLIC 38
5.1. S – STRATÉGIE 39
5.1.1. Finalités opérationnelles et intérêt général 39
5.1.2. Ce qui n'est pas souhaitable 39
5.2. O – ORGANISATION 41
5.2.1. Gouvernance, coordination et structuration du projet 41
5.2.2. Coordination opérationnelle et exploitation quotidienne 42
5.3. T – TECHNOLOGIE 43
5.3.1. Contraintes des espaces ouverts au public 43
5.3.2. Interopérabilité, cybersécurité et résilience 43
5.3.3. Supervision augmentée et automatisation 44
5.4. A – ASPECTS FINANCIERS 44
5.4.1. Mutualisation, soutenabilité et modèles économiques 44
5.4.2. Limites des approches ROI simplistes 45
5.5. J – JURIDIQUE 46
5.5.1. CSI, RGPD, IA Act, NIS2, CRA et gouvernance des usages 46
5.5.2. Responsabilités, partage des données et zones grises 47
5.6. E – ÉTHIQUE 48
5.6.1. Proportionnalité, acceptabilité et contrôle des usages 48
5.6.2. Rôle du DPO/DPD (Délégué à la Protection des Données) 49

PARTIE 2 : PUS EN ESPACES PRIVÉS ET SITES SENSIBLES

6. PUS EN ESPACES PRIVÉS ET SITES SENSIBLES 52
6.1. S – STRATÉGIE 52
6.2. O – ORGANISATION 54
6.3. T – TECHNOLOGIE 56
6.4. A – ASPECTS FINANCIERS 58
6.4.1. Logiques d'investissement et d'exploitation 58
6.4.2. Création de valeur mesurable 59
6.5. J – JURIDIQUE 60
6.5.1. Responsabilité du responsable de traitement 60
6.5.2. Cadre contractuel et conformité 61
6.5.3. OIV, NIS2, CRA et obligations renforcées des sites sensibles 62
6.6. E – ÉTHIQUE ET ACCEPTABILITÉ 64
6.6.1. Risques d'usage et dérives possibles 64
6.6.2. Cadre de confiance et gouvernance 65

CONCLUSION

7. CONCLUSION 68

ANNEXES

8. ANNEXES 72
8.1 LEXIQUE 72
8.2 RETOUR D'EXPERIENCE STRUCTURANT 74

1. AVANT-PROPOS

1.1. POSITIONNEMENT DU GROUPE DE TRAVAIL PLATEFORME UNIFIÉE SCALABLE

Le Groupe de Travail Plateforme Unifiée Scalable (**GT PUS**) de l'AN2V réunit des acteurs publics et privés impliqués dans la conception, le déploiement et l'exploitation de plateformes d'hypervision et de coordination opérationnelle.
Ses travaux reposent sur le croisement d'expériences de terrain, d'expertises techniques et de problématiques opérationnelles concrètes rencontrées dans les territoires, les infrastructures et les sites sensibles.
L'objectif du GT PUS est de proposer un cadre de réflexion commun permettant d'éclairer les choix des décideurs, de structurer les approches et de favoriser une meilleure cohérence des projets liés aux plateformes unifiées.
Les travaux du GT PUS s'inscrivent dans un contexte de convergence progressive entre systèmes métiers, systèmes d'information et outils opérationnels, dans des environnements de plus en plus interconnectés et multi-acteurs.
Cette évolution soulève des enjeux qui dépassent le seul cadre technologique et concernent notamment l'organisation, la gouvernance, l'interopérabilité, la gestion des données, la cybersécurité et la continuité opérationnelle.

1.1.1. Articulation avec les autres GT AN2V (R2A, Cloud)

Les travaux du GT PUS s'inscrivent en complémentarité avec ceux des autres groupes de travail de l'AN2V, notamment le GT R2A et le GT Cloud.
Le GT R2A (Vidéoprotection/IA) apporte une expertise sur les mécanismes de remontée d'alerte et de traitement des événements, qui constituent des briques essentielles dans une logique de plateforme unifiée.
Le GT Cloud traite des enjeux d'hébergement, de scalabilité et de gestion des données, directement liés aux architectures de plateformes unifiées.
Cette articulation permet d'assurer une cohérence globale des travaux de l'AN2V et d'éviter une approche fragmentée des sujets.

1.1.2. Publics cibles et usages du document

Ce livre blanc s'adresse en priorité aux décideurs publics et privés, aux directions opérationnelles, ainsi qu'aux acteurs techniques impliqués dans des projets de sécurité, de sûreté et de gestion opérationnelle.
Il vise à fournir des repères pour comprendre les enjeux, structurer une réflexion et accompagner la prise de décision. Le document peut être utilisé comme base de cadrage en amont d'un projet, comme outil de dialogue entre parties prenantes pour un projet concret, ou comme support de montée en compétence sur les plateformes unifiées existantes.
Afin de répondre à la diversité des profils et des niveaux de maturité du lecteur, le document propose une lecture à trois niveaux, identifiés par un code couleur :

- Noir pour les essentiels : une lecture accessible, orientée vers les décideurs et les élus, permettant de comprendre les enjeux, les finalités et les impacts sans prérequis technique
- Bleu foncé niveau technique intermédiaire : une lecture approfondie, destinée aux acteurs disposant déjà d'une première expérience du sujet, des plateformes de supervision, permettant de mieux appréhender les mécanismes opérationnels et organisationnels
- Violet foncé niveau technique Expert : une lecture experte, intégrant des notions techniques, architecturales et réglementaires avancées, destinée aux spécialistes impliqués dans la conception, le déploiement ou l'exploitation de ces solutions.

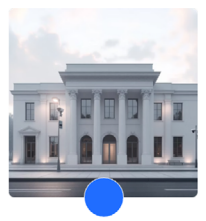
Cette structuration permet à chaque lecteur d'accéder à sa guise directement au niveau d'information pertinent, tout en conservant une cohérence globale de lecture.

1.1.3. Distinction des espaces juridiques et opérationnels

Une distinction structurante a été également prise en compte dans ce document pour les projets de Plateforme Unifiée Scalable : celle des espaces juridiques et des contextes d'exploitation.
Les usages, les responsabilités, les contraintes réglementaires et les finalités opérationnelles ne sont pas identiques selon que les dispositifs sont déployés :

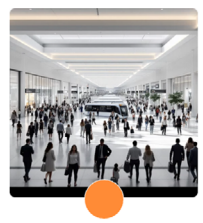
- en espace public ;
- en espace privé ouvert au public ;
- ou en espace privé strict.

Cette distinction est essentielle, car ce n'est pas uniquement la technologie qui détermine la faisabilité d'un projet, mais également le cadre juridique dans lequel il s'inscrit.
Les espaces publics concernent principalement les collectivités territoriales et les acteurs de la sécurité publique. Les enjeux portent notamment sur la vidéoprotection urbaine, la gestion bâtimentaire publique, la coordination multi-acteurs (CSU, CSUi, CSD), la gestion de l'espace public et le respect des libertés publiques.
Les espaces privés ouverts au public, comme les transports, centres commerciaux, stades, hôpitaux ou campus, répondent à des logiques différentes. Les exploitants doivent concilier sécurité, continuité d'activité, gestion des flux et de leurs bâtiments, et responsabilité vis-à-vis du public accueilli.
Les espaces privés stricts, tels que les industries, infrastructures critiques, data centers ou sites sensibles, s'inscrivent davantage dans des problématiques de sûreté, de cybersécurité, de résilience opérationnelle et de protection des actifs stratégiques.
Ces trois environnements peuvent utiliser des technologies proches et partager des méthodes communes de conception, d'intégration et d'exploitation. Toutefois, les attentes opérationnelles, les niveaux de risque, les obligations réglementaires et les modèles de gouvernance restent profondément différents.
Une même fonctionnalité peut ainsi être autorisée dans un contexte, fortement encadrée dans un autre, voire interdite selon la nature de l'espace concerné.
Comprendre cette distinction permet d'éviter des approches trop uniformes ou des comparaisons inadaptées entre projets. Elle constitue un élément essentiel pour définir une architecture cohérente, choisir les bons niveaux de gouvernance et adapter les usages aux réalités juridiques et opérationnelles de chaque environnement.
C'est la raison pour laquelle ce livre blanc distingue ensuite trois approches dédiées, identifiées par les couleurs bleu, orange et vert, correspondant à ces trois grands espaces juridiques et opérationnels.



Espaces publics

Communes, intercommunalités, métropoles, départements, régions.
Sécurité publique, vidéoprotection urbaine, coordination multi-acteurs.



Espaces privés ouverts au public

Transports, centres commerciaux, stades, hôpitaux, campus.
Gestion des flux, responsabilité d'exploitant, continuité d'activité.



Espaces privés

Industries, OIV, data centers, infrastructures critiques.
Périmètres de sécurité, convergence cyber/physique, résilience opérationnelle.

1.2. POURQUOI UN LIVRE BLANC PUS

Les collectivités, infrastructures et sites sensibles doivent gérer des situations plus rapides, plus complexes et plus interconnectées. Les outils existent déjà, les données aussi, mais leur dispersion limite encore la compréhension des événements, la coordination des acteurs et la rapidité d'action.

La difficulté ne vient donc plus seulement du manque d'équipements, mais de l'empilement de systèmes spécialisés, souvent peu coordonnés entre eux. Cette fragmentation crée des ruptures d'information, augmente la charge des opérateurs et complique la gestion des incidents, des crises ou l'efficacité des modes dégradés.

Ce livre blanc vise à proposer un cadre commun pour comprendre, concevoir et gouverner les **Plateformes Unifiées Scalable**. Il ne s'agit pas de promouvoir une solution technique, mais de clarifier les conditions de réussite : finalités, organisation, interopérabilité, cybersécurité, résilience, responsabilités, conformité et maîtrise des usages.
L'objectif est de donner aux décideurs publics et privés des repères pour éviter les projets construits autour de la technologie seule, et privilégier des plateformes réellement exploitables, gouvernées et durables.

1.2.1. Pourquoi la PUS est devenue un sujet stratégique

La PUS devient stratégique parce que les organisations ne peuvent plus piloter des environnements complexes avec des outils isolés. Les situations à traiter impliquent simultanément plusieurs systèmes, plusieurs métiers et plusieurs niveaux de décision.

Sa valeur ne réside pas dans la centralisation maximale, mais dans la capacité à transformer des informations dispersées en une compréhension exploitable et en actions coordonnées.

Elle devient ainsi une couche opérationnelle structurante entre les systèmes d'information, les équipements terrain, les procédures et les équipes d'exploitation. Sa conception engage durablement la gouvernance, la cybersécurité, la continuité d'activité, la souveraineté des données et la responsabilité des directions.

1.2.2. Ce que ce livre blanc n'est volontairement pas

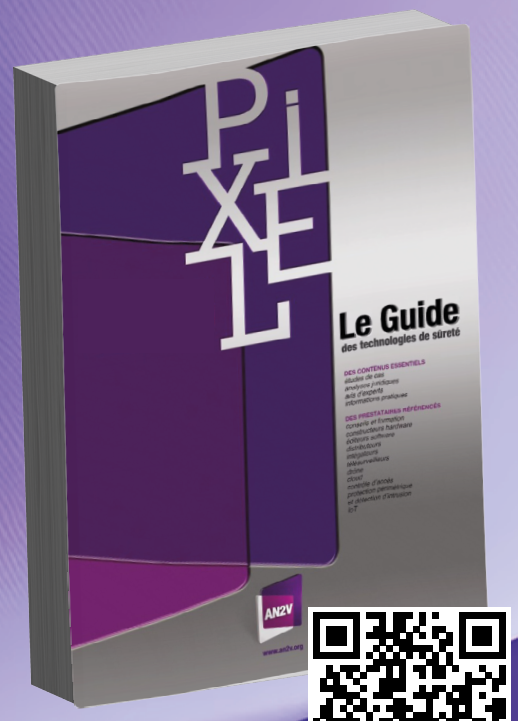
Ce livre blanc n'est ni un catalogue de solutions, ni un comparatif d'éditeurs, ni un modèle unique applicable à tous les contextes.

Il ne présente pas la PUS comme une réponse technologique automatique. Une plateforme mal gouvernée peut ajouter de la complexité au lieu d'en retirer.

Ce document propose donc **une doctrine de cadrage** : comprendre les usages, identifier les responsabilités, décrire la méthode pour aboutir à un dispositif optimal, maîtriser les dépendances et inscrire la plateforme dans une organisation capable de l'exploiter dans la durée.

AN2V

LA RÉFÉRENCE DE LA PROFESSION :
LA RESSOURCE POUR TOUS !



www.an2v.org

INTRODUCTION

2. INTRODUCTION GÉNÉRALE

2.1. LIMITES DE L'APPROCHE HISTORIQUE

2.1.1. Silos métiers et fragmentation

Les systèmes utilisés aujourd'hui fonctionnent souvent de manière séparée.
D'un côté, les systèmes informatiques gèrent les données, les applications et les traitements numériques.
De l'autre, les équipements terrain assurent la surveillance, les actions et le pilotage opérationnel.
Dans une situation réelle, ces systèmes ne sont pas toujours reliés entre eux, ce qui oblige les équipes à multiplier les outils pour comprendre ce qui se passe et coordonner leurs actions.
Cette séparation correspond à deux univers distincts :

- IT (Information Technology) : systèmes d'information, données, applications, cybersécurité
- OT (Operational Technology) : équipements terrain, vidéo, contrôle d'accès, capteurs, infrastruc tures urbaines.

Ces deux mondes ont longtemps été conçus et exploités séparément, avec des logiques et des priorités différentes.
Résultat : l'information reste fragmentée.
Un même événement peut être détecté par plusieurs systèmes sans être automatiquement mis en relation.
Exemple : une alarme intrusion détecte une situation sur une zone d'un bâtiment → une alerte est générée → mais les données ne sont pas croisées avec les autres systèmes dont la vidéo → l'opérateur doit reconstituer lui-même la situation, les portes de fuite possible, voiture garée à l'extérieur avec 2 individus…

Les architectures historiques reposent sur une séparation structurelle entre IT et OT.
L'IT est principalement orientée vers la gestion des données, la gouvernance et la sécurité des systèmes d'information.
L'OT est orientée vers l'exploitation terrain, le temps réel et la continuité opérationnelle.
Cette séparation produit plusieurs effets :

- systèmes spécialisés faiblement interopérables ;
- flux d'informations non corrélés ;
- multiplication des interfaces et des outils ;
- dépendance forte à l'intervention humaine pour analyser les situations.

Dans ce modèle, la donnée circule, mais reste cloisonnée. Les organisations disposent d'informations nombreuses, sans toujours pouvoir les exploiter de manière coordonnée et immédiate.

Les limites des architectures historiques proviennent principalement de l'absence d'une couche transverse capable d'assurer la corrélation, l'orchestration et la contextualisation des flux IT et OT en temps réel.
Les systèmes ont été conçus selon des logiques verticales indépendantes, avec des modèles d'intégration hétérogènes, des protocoles spécifiques et des mécanismes d'échange souvent limités à des interactions ponctuelles.
Cette fragmentation entraîne :

- une faible interopérabilité réelle entre systèmes ;
- des traitements partiels ou non synchronisés ;
- une difficulté à produire une vision opérationnelle cohérente ;
- une dépendance croissante aux opérateurs pour reconstituer les événements.

La difficulté ne réside plus principalement dans la captation ou le stockage des données, mais dans la capacité à relier, contextualiser et exploiter ces informations en temps réel dans des environnements multi-systèmes.

2.1.2. Limites des architectures existantes

Les systèmes actuels ont généralement été conçus pour répondre à des besoins spécifiques, chacun dans son domaine.
Ils fonctionnent souvent correctement de manière isolée, mais deviennent plus difficiles à faire évoluer ou à coordonner lorsque les environnements se complexifient.
Dans des situations impliquant plusieurs systèmes et plusieurs acteurs, cette organisation atteint rapidement ses limites.
Les principales difficultés rencontrées sont :

- des intégrations complexes entre outils ;
- une dépendance à des solutions spécifiques ;
- des évolutions longues et coûteuses ;
- une difficulté à partager et exploiter les informations en temps réel.

Exemple : l'ajout d'un nouveau capteur ou l'intégration d'un nouveau système nécessite souvent des développements spécifiques et des adaptations importantes.
Ces architectures peuvent fonctionner efficacement dans un périmètre limité, mais deviennent plus difficiles à exploiter dès qu'il faut coordonner plusieurs sources d'information simultanément.

Les architectures historiques reposent souvent sur des modèles conçus pour des usages isolés, sans mécanisme natif de coordination globale entre systèmes.
Cette situation produit plusieurs limites structurelles :

- couplage fort entre composants ;
- multiplication des interfaces spécifiques ;
- dépendance élevée à certains éditeurs ou intégrateurs ;
- faible capacité d'adaptation à de nouveaux usages ;
- difficulté à synchroniser les informations et les décisions opérationnelles.

Deux approches opposées produisent fréquemment les mêmes difficultés opérationnelles :

- les architectures monolithiques, fortement intégrées mais rigides ;
- les architectures fragmentées ("best-of-breed"), composées de multiples systèmes spécialisés peu coordonnés.

Dans les deux cas, la complexité est reportée vers les opérateurs, qui doivent reconstituer manuellement la situation à partir d'informations dispersées.

Les limites des architectures existantes proviennent principalement de modèles d'intégration hétérogènes et faiblement découplés.
Les intégrations "point à point" multiplient les dépendances techniques et rendent chaque évolution plus complexe à maintenir dans le temps.
L'absence de mécanisme unifié de pilotage des flux et des événements empêche la production d'une vision opérationnelle cohérente en temps réel.
Cette fragmentation entraîne plusieurs conséquences :

- latence dans la circulation des informations ;
- traitements non synchronisés entre systèmes ;
- perte de contexte lors des échanges ;
- difficulté à rapprocher des événements provenant de sources différentes ;
- augmentation des risques opérationnels lors des évolutions d'architecture.

La difficulté ne réside donc plus uniquement dans la capacité à collecter des données, mais dans la capacité à les exploiter de manière coordonnée afin de produire une continuité opérationnelle entre systèmes, acteurs et processus.

2.2. CLARIFICATION DES NOTIONS CLÉS

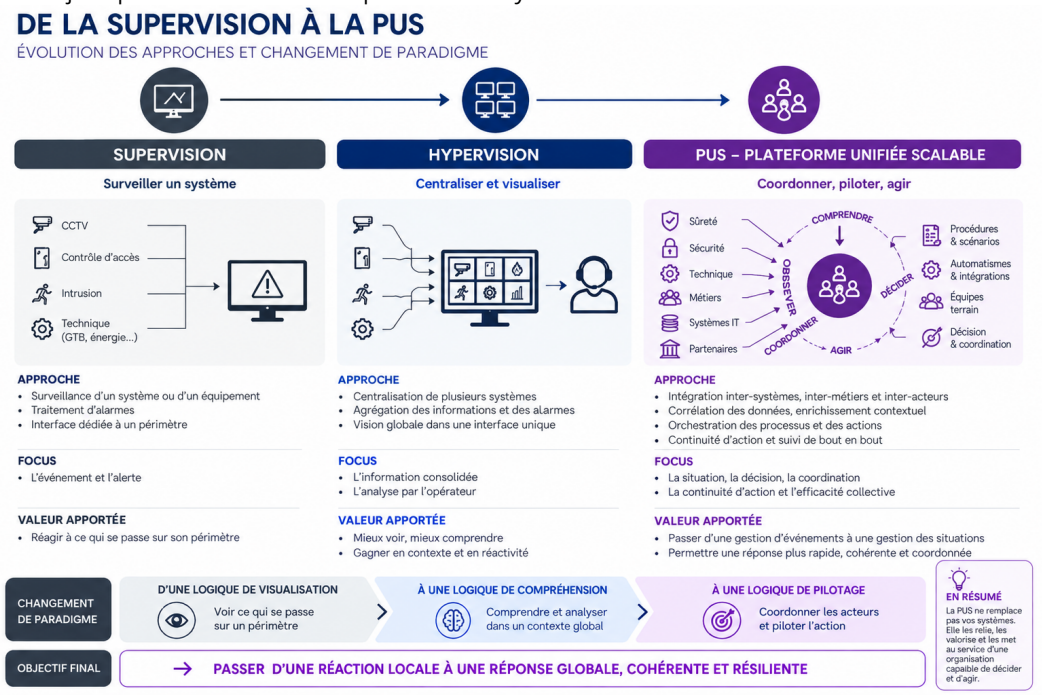
2.2.1. De la supervision à la PUS : évolution des approches

Les termes supervision, hypervision et plateforme unifiée sont souvent utilisés de manière interchangeable. Pourtant, ils correspondent à des approches différentes.

- La supervision consiste principalement à surveiller un système et à traiter ses alertes.
- L'hypervision ajoute une capacité de centralisation en regroupant plusieurs systèmes dans une même interface afin d'obtenir une vision plus globale des événements.

La PUS introduit une logique plus large : elle ne se limite pas à afficher ou centraliser des informations, mais vise à coordonner les actions et à faciliter la gestion opérationnelle des situations.
Comprendre ces différences est essentiel. Confondre ces notions conduit souvent à des projets mal définis, à des attentes irréalistes ou à des choix techniques inadaptés.

Les enjeux précédemment décrits peuvent être synthétisés de la manière suivante :

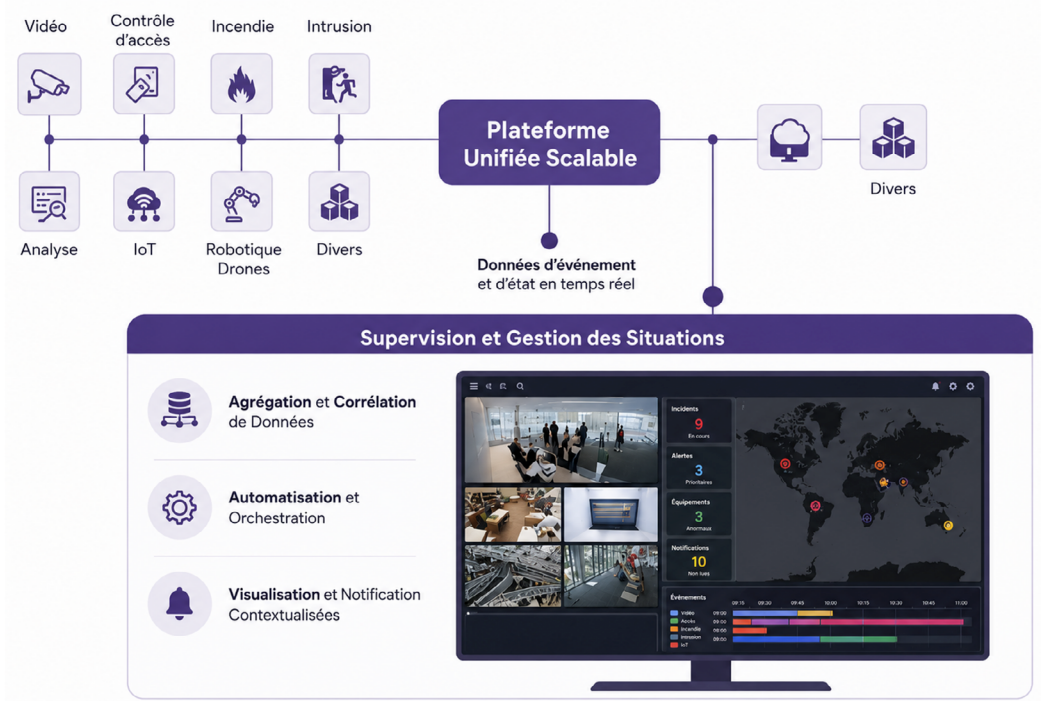


La différence entre supervision, hypervision et PUS ne repose pas uniquement sur le nombre de systèmes connectés, mais sur la manière dont les informations sont exploitées.
La supervision reste généralement centrée sur un domaine spécifique avec une logique réactive : surveiller, détecter et traiter des alertes.

L'hypervision améliore la visualisation globale grâce à l'agrégation de plusieurs sources d'information, mais conserve souvent une approche centrée sur la consultation et l'analyse par l'opérateur.
La PUS introduit une approche orientée coordination opérationnelle. Elle permet de passer :

- d'une gestion d'alertes à une gestion des situations ;
- d'une juxtaposition d'informations à une continuité d'action ;
- d'une logique de visualisation à une logique de pilotage.

L'objectif n'est plus seulement de voir ce qui se passe, mais de permettre une réponse plus rapide, plus cohérente et mieux coordonnée entre systèmes et acteurs.



2.2.2. Enjeux architecturaux et opérationnels

La mise en œuvre d'une PUS implique des enjeux qui dépassent la simple centralisation des informations.
Elle suppose de pouvoir faire interagir des systèmes hétérogènes, partager des données en temps réel et coordonner plusieurs domaines métier dans une même logique opérationnelle.
Cette approche nécessite des architectures capables d'assurer :

- l'interopérabilité ;
- l'évolutivité ;
- la continuité opérationnelle ;
- la synchronisation des informations et des actions ;
- l'intégration progressive de nouveaux services et usages.

La PUS devient ainsi un point de convergence entre systèmes d'information, équipements terrain et processus opérationnels.

Les architectures de PUS reposent sur des mécanismes d'intégration permettant d'articuler des environnements IT et OT historiquement séparés.
Cette convergence implique :

- la gestion de flux multi-sources en temps réel ;
- des mécanismes de médiation et d'échange entre protocoles hétérogènes ;
- des capacités de résilience et de continuité de service ;
- une gouvernance maîtrisée des accès, des données et des traitements.

Ces architectures doivent également limiter les dépendances techniques afin de préserver l'évolutivité des systèmes et la capacité d'intégrer de nouveaux équipements, services ou usages dans le temps.



3. COMPRENDRE LA PUS

Une Plateforme Unifiée Scalable (PUS) a pour objectif d'améliorer la compréhension des situations et la coordination des actions dans des environnements complexes. Elle ne remplace pas les systèmes existants, mais permet de mieux exploiter les informations qu'ils produisent afin de faciliter le pilotage opérationnel.
Une PUS peut ainsi regrouper des données issues de plusieurs domaines : vidéoprotection, contrôle d'accès, supervision technique, cybersécurité, capteurs IoT, gestion bâtimentaire ou outils métiers : éclairage public, application citoyenne…
L'objectif n'est pas uniquement de centraliser des informations, mais de permettre une lecture plus cohérente des événements, une meilleure circulation des informations et une réponse plus rapide et mieux coordonnée entre les acteurs concernés, donc les services techniques concernés.
Cette approche permet notamment :

- de réduire les délais de compréhension et de qualification des situations ;
- de faciliter la coordination entre services et systèmes ;
- d'améliorer le suivi des événements et des actions engagées ;
- de limiter les ruptures d'information entre les différents environnements opérationnels.

Dans un fonctionnement classique, les opérateurs doivent souvent consulter plusieurs outils séparés, rapprocher manuellement les informations et coordonner eux-mêmes les actions à engager.
Une PUS permet de regrouper ces informations dans une même logique opérationnelle afin de faciliter la prise de décision et le suivi des actions.
Exemple : lors d'un incident, les flux vidéo, les alarmes, la localisation des équipements et les moyens disponibles peuvent être regroupés afin de fournir une vision plus rapide et plus exploitable de la situation.
La valeur d'une PUS ne repose donc pas uniquement sur le nombre de systèmes connectés, mais sur sa capacité à structurer les informations, à afficher des fiches réflexes pré-enseignées, à faciliter la coordination des acteurs et à accompagner la gestion opérationnelle des situations.

3.1. CE QUE PERMET UNE PUS

3.1.1. Vision globale, cohérence opérationnelle et aide à la décision

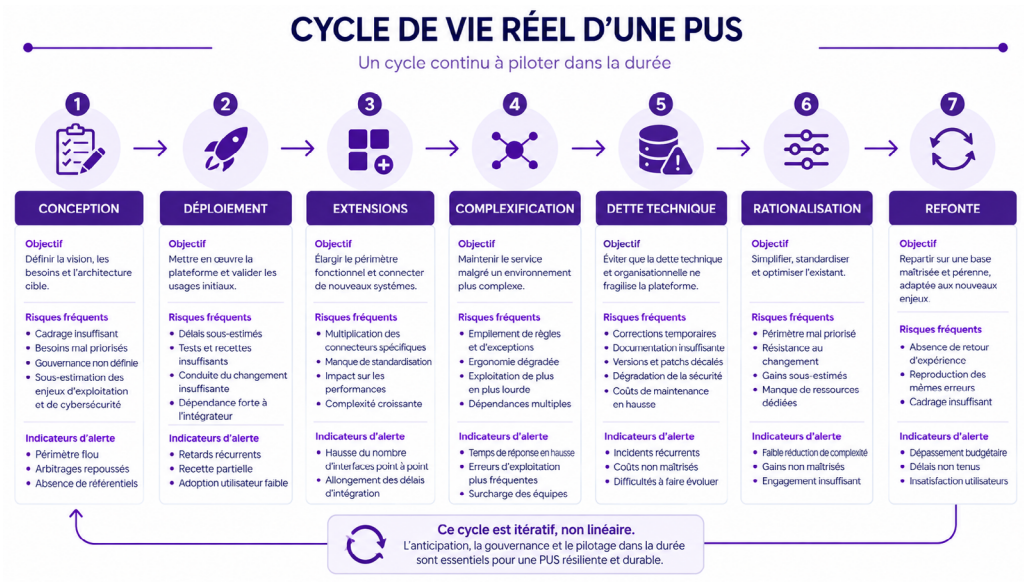
Une PUS permet de mieux comprendre une situation et de coordonner plus efficacement les actions à engager.
Au lieu de consulter plusieurs outils séparés, les opérateurs disposent d'une vision unifiée regroupant les informations utiles à la gestion d'un événement.
Cette approche permet :

- de réduire les délais de compréhension ;
- de limiter les ruptures d'information ;
- d'améliorer la coordination entre services ;
- et de faciliter le suivi des actions engagées.

Par exemple, lors d'un accident, les flux vidéo, la localisation de l'événement et les moyens disponibles peuvent être affichés immédiatement (fiche réflexe sur le mur d'image) afin d'accélérer l'évaluation de la situation et l'intervention des équipes.
Sans PUS, les informations restent souvent dispersées entre plusieurs systèmes et plusieurs interfaces. Les opérateurs doivent alors rechercher les données, les rapprocher et coordonner manuellement les actions nécessaires (au téléphone).
La PUS permet au contraire de structurer les informations dans une même logique opérationnelle afin de produire une réponse plus cohérente et plus réactive.

Une PUS peut également s'appuyer sur **des scénarios opérationnels prédéfinis** permettant d'automatiser certaines actions ou d'assister les opérateurs dans la gestion des événements.
Ces mécanismes reposent sur des règles définies en amont, adaptées aux procédures et aux besoins de l'organisation.
Exemple : un accident est détecté → les flux vidéo concernés sont affichés automatiquement sur le mur d'images → l'éclairage public est renforcé → les équipes les plus proches sont identifiées → une main courante est ouverte → le suivi de l'intervention est centralisé, en appui avec les équipes (PM, GN, SDIS…).
L'objectif n'est surtout pas de remplacer les opérateurs (besoin de travailler en h24, 365j/an), mais de réduire les délais de réaction, de limiter les oublis et d'améliorer la cohérence des actions engagées.
La valeur d'une PUS ne repose donc pas uniquement sur la centralisation des systèmes, mais sur sa capacité à produire une information exploitable, structurée et directement utile à la gestion opérationnelle.

Les problématiques précédemment évoquées s'inscrivent généralement dans un cycle d'évolution relativement classique des plateformes PUS :



3.2. CE QUE LA PUS NE FAIT PAS

Une PUS ne décide pas à la place des équipes et ne fonctionne pas de manière autonome !
Elle doit être préparée et organisée en amont afin de définir :

- les situations à traiter ;
- les actions à engager ;
- les acteurs concernés ;
- et les modalités de coordination.

La PUS ne remplace donc ni les procédures opérationnelles, ni les opérateurs, ni les décisions humaines.
Son efficacité dépend directement de la qualité des scénarios préparés, des règles définies et de l'organisation mise en place autour des systèmes.
Par exemple, lorsqu'un commerçant déclenche une alerte, la PUS peut afficher automatiquement les caméras concernées en affichant les 3 caméras les plus proches (préréglage des 3 PTZ), localiser l'événement et faciliter la mobilisation des équipes. Mais ce fonctionnement suppose que les mécanismes de traitement aient été définis et configurés à l'avance, mais aussi testées régulièrement afin de s'assurer du bon fonctionnement le jour J.
Sans cette préparation, les systèmes restent juxtaposés et les opérateurs doivent reconstruire eux-mêmes la situation à partir de plusieurs outils séparés, et souvent perdre un temps précieux.

La mise en œuvre d'une PUS repose généralement sur des scénarios opérationnels permettant de structurer les réponses en fonction des événements détectés.
Ces scénarios peuvent intégrer :

- des déclencheurs ;
- des règles de priorisation ;
- des actions automatiques ou semi-automatiques ;
- des notifications ;
- des affichages dynamiques ;
- des mécanismes de suivi et de traçabilité.

Exemple : déclenchement d'une alerte → affichage automatique des flux vidéo concernés avec auto-zoom sur les PTZ → géolocalisation de l'événement → identification des équipes disponibles → ouverture d'une main courante → suivi des actions engagées.

L'objectif de ces mécanismes n'est pas d'automatiser entièrement la décision, mais de réduire les délais de réaction, de limiter les oublis et d'améliorer la cohérence des réponses opérationnelles. Cela permet aussi une traçabilité optimisée de tout ce qu'il s'est passé !

Les architectures avancées de PUS s'appuient sur des moteurs de règles capables d'exécuter des chaînes d'actions conditionnelles basées sur des logiques de type IF / THEN.
Ces mécanismes permettent de transformer un événement brut en scénario opérationnel structuré, en combinant plusieurs sources d'information et plusieurs niveaux de traitement.
Chaque scénario peut intégrer :

- des événements déclencheurs ;
- des conditions de contexte ;
- des mécanismes de priorisation ;
- des actions automatiques ;
- des validations humaines ;
- des boucles de retour d'état et de traçabilité.

Exemple :
détection d'une intrusion + anomalie de contrôle d'accès + mouvement vidéo confirmé → qualification automatique de l'incident → affichage dynamique des flux concernés → repositionnement de caméras des PTZ réorientées sur le fait → renforcement d'éclairage, ou allumage si bâtiment → ouverture d'une procédure en MCI → notification des équipes compétentes → suivi temps réel des actions engagées.
Certaines architectures reposent également sur des modèles de graphes relationnels permettant de relier dynamiquement :

- événements ;
- équipements ;
- zones ;
- acteurs ;
- historiques ;
- ressources opérationnelles.

Cette approche facilite la production d'une vision exploitable de situations complexes impliquant plusieurs systèmes et plusieurs domaines métier simultanément.
La valeur d'une PUS avancée ne repose donc pas uniquement sur la centralisation des données, mais sur sa capacité à structurer dynamiquement les interactions entre événements, ressources et processus opérationnels.

3.2.1. Absence de décision automatisée

Une PUS peut automatiser certaines actions, mais **elle ne prend pas de décision à la place des équipes** ou des autorités compétentes.
Les décisions restent de la responsabilité des opérateurs, des services concernés ou des autorités disposant de la légitimité et des compétences nécessaires.
La PUS exécute des règles, des scénarios et des procédures définis en amont. Elle peut afficher des informations, générer des alertes, faciliter la coordination des acteurs ou déclencher certaines actions prévues dans les procédures opérationnelles.
En revanche, elle ne remplace ni l'analyse du contexte, ni l'appréciation humaine de la situation, ni la responsabilité de décision.
Il est essentiel de distinguer :

- l'automatisation d'actions ou de traitements ;
- et la prise de décision.

Les mécanismes d'automatisation utilisés dans une PUS reposent sur des règles conditionnelles définies à l'avance et ne disposent pas d'une capacité autonome d'interprétation ou de jugement.
Cette distinction constitue un point structurant au regard des exigences réglementaires, notamment en matière :

- de supervision humaine ;
- de transparence des traitements ;
- de traçabilité des actions ;
- et de responsabilité des décisions prises.

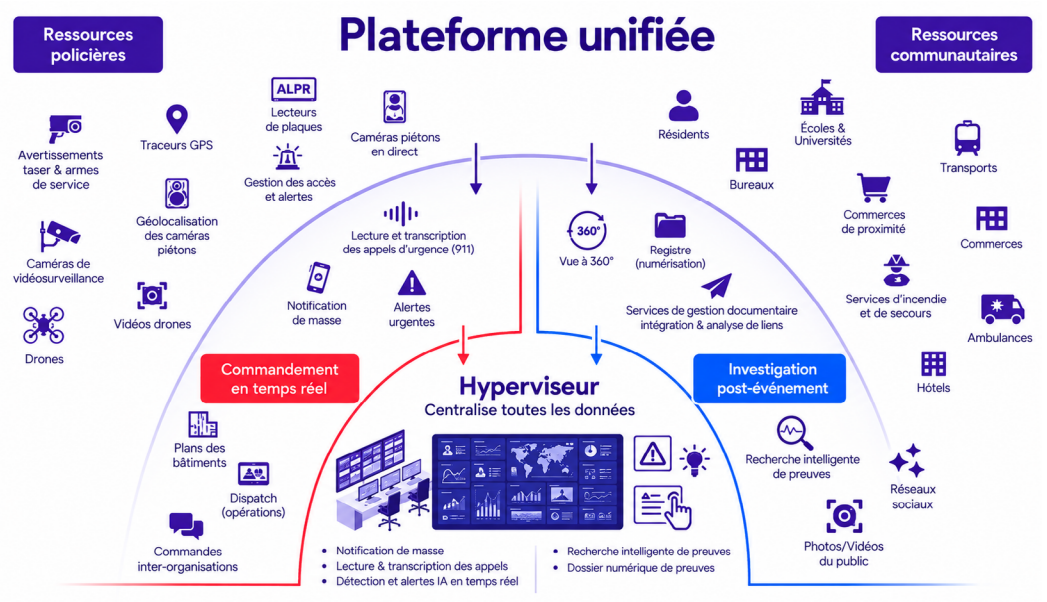
Toute confusion entre automatisation et décision peut entraîner des risques opérationnels, organisationnels, réglementaires ou juridiques importants.

3.2.2. Mythes fréquents autour de l'hypervision et de l'IA

L'augmentation du nombre d'équipements et/ou l'ajout de fonctionnalités d'intelligence artificielle ne garantissent pas, à eux seuls, une meilleure efficacité opérationnelle. Une PUS ne devient pas performante par accumulation de technologies, mais par la qualité de l'organisation, des scénarios opérationnels et des usages définis autour des systèmes.
Plusieurs idées reçues compliquent encore de nombreux projets. Connecter plusieurs systèmes ne crée pas automatiquement de la coordination, pas plus que l'IA ne permet de détecter ou d'anticiper toutes les situations. De la même manière, une plateforme ne peut fonctionner efficacement sans préparation préalable des procédures, des usages et de la formation des opérateurs.
En réalité, la performance d'une PUS repose principalement sur :

- la structuration des informations ;
- la qualité des scénarios opérationnels ;
- la cohérence des procédures ;
- la capacité des équipes à exploiter les outils dans une logique coordonnée.

Certaines dérives proviennent également d'une confusion entre potentiel technologique et réalité opérationnelle. L'accumulation de données sans hiérarchisation claire des informations, la multiplication des alertes générant une surcharge cognitive pour les opérateurs, ou encore la surestimation des capacités de l'IA peuvent rapidement dégrader l'efficacité globale du dispositif. Ces difficultés sont souvent renforcées par la recherche de solutions "clé en main" déployées sans véritable travail préalable sur les usages, les besoins fonctionnels, les procédures et la gouvernance.
Une PUS performante ne repose donc pas uniquement sur la technologie déployée, mais sur la capacité de l'organisation à transformer les informations disponibles en actions cohérentes, coordonnées et adaptées aux situations rencontrées.



4. INVARIANTS ET PRINCIPES FONDATEURS

4.1. LA PUS COMME SOCLE COMMUN MULTI-CONTEXTES

Une PUS peut être déployée dans des contextes très différents : collectivités territoriales CSU, CSUi (intercommunal), CSD (départemental), transports, infrastructures critiques, industries, sites sensibles, réseaux multi-sites ou grands ensembles immobiliers.
Les environnements, les organisations, les contraintes réglementaires et les usages peuvent fortement varier. Pourtant, certains principes fondamentaux restent constants dans la conception et l'exploitation d'une PUS.
Une PUS doit permettre de :

- collecter et exploiter des informations provenant de plusieurs systèmes ;
- qualifier des événements et coordonner des actions ;
- assurer une continuité opérationnelle adaptée aux contraintes du terrain ;
- et permettre une évolution progressive des usages et des architectures dans le temps.

La performance d'une PUS ne repose pas uniquement sur les technologies utilisées, mais sur la manière dont les systèmes, les données, les procédures et les acteurs sont organisés et articulés entre eux.
Les choix réalisés lors de la conception ont un impact direct sur :

- la robustesse opérationnelle ;
- la résilience face aux incidents et aux défaillances ;
- la capacité d'évolution et de montée en charge ;
- l'interopérabilité entre systèmes ;
- la cybersécurité ;
- la maîtrise et la localisation des données ;
- la réversibilité des architectures ;
- la dépendance vis-à-vis des fournisseurs ;
- ainsi que les coûts d'exploitation, de maintenance et d'évolution dans la durée.

Une architecture mal maîtrisée peut rapidement générer des coûts cachés importants : multiplication des développements spécifiques, dépendances techniques, difficultés d'intégration, complexité de maintenance ou impossibilité d'ajouter de nouveaux usages sans remise en cause globale du système.
À l'inverse, une architecture pensée pour la modularité, la scalabilité et la réversibilité permet d'intégrer progressivement de nouveaux équipements, services ou fonctions, sans reconstruire l'ensemble de la plateforme à chaque évolution.
Les principes présentés dans ce chapitre visent ainsi à identifier les invariants fonctionnels, organisationnels et techniques nécessaires à la conception d'une PUS robuste, évolutive, interopérable et durable.

4.1.1. Invariants fonctionnels

Quel que soit le contexte d'exploitation, une PUS repose toujours sur un ensemble de fonctions essentielles permettant de transformer des informations dispersées en actions opérationnelles cohérentes.
Ces fonctio
ns restent globalement identiques, qu'il s'agisse d'une collectivité, d'un réseau de transport, d'un site industriel ou d'une infrastructure critique.

Une PUS doit notamment permettre de :

- recevoir des informations provenant de plusieurs systèmes ;
- qualifier et hiérarchiser les événements ;
- restituer les informations utiles aux opérateurs ;
- faciliter le déclenchement des actions adaptées ;
- assurer le suivi et la traçabilité des opérations engagées.

Ces fonctions peuvent paraître simples en apparence, mais leur efficacité dépend directement de la fluidité de leur enchaînement et de la cohérence globale du système.

Les invariants fonctionnels d'une PUS reposent sur une chaîne continue de traitement de l'information :

- acquisition des données ;
- qualification des événements ;
- mise en relation des informations utiles ;
- restitution contextualisée ;
- déclenchement des actions ;
- traçabilité et exploitation des événements.

La qualité d'une PUS dépend moins de la performance isolée des composants que de la continuité entre ces différentes fonctions.
Toute rupture dans cette chaîne dégrade la capacité opérationnelle globale.

Exemple : une alerte non contextualisée ralentit la qualification, une information non partagée limite la coordination, une action non tracée complique l'analyse a posteriori, tandis qu'une donnée mal hiérarchisée augmente la charge cognitive des opérateurs. Ces différentes ruptures dégradent progressivement la capacité globale de la plateforme à produire une réponse cohérente et exploitable.
Les invariants fonctionnels doivent donc être conçus comme un ensemble cohérent garantissant :

- la fluidité des traitements ;
- la lisibilité des informations ;
- la continuité opérationnelle ;
- la traçabilité des actions engagées.

4.1.2. Invariants organisationnels

Une PUS ne fonctionne pas seule. Son efficacité dépend directement de l'organisation mise en place autour des systèmes et des équipes qui les exploitent.
Quel que soit le contexte, une PUS repose toujours sur :

- une définition claire des rôles ;
- des circuits de décision identifiés ;
- des procédures partagées ;
- et une coordination structurée entre les acteurs concernés.

La technologie peut accélérer la circulation de l'information et faciliter la coordination, mais elle ne remplace ni l'organisation, ni les responsabilités humaines.
Une organisation peu structurée apparaîtra rapidement comme telle dans une PUS : informations mal qualifiées, traitements incohérents, responsabilités floues ou absence de coordination entre services.
À l'inverse, une organisation claire et formalisée permet à la PUS de devenir un véritable levier de performance opérationnelle.

Exemple : lors d'un incident, plusieurs acteurs peuvent être impliqués simultanément : opérateurs, services techniques, sécurité, forces d'intervention ou partenaires externes. Sans règles de coordination définies en amont, la multiplication des informations peut ralentir la prise de décision au lieu de l'améliorer, surtout en cas de crise grave.

Les invariants organisationnels reposent principalement sur :

- la répartition claire des responsabilités ;
- la maîtrise des circuits d'information ;
- la formalisation des procédures opérationnelles ;
- la gestion des priorités ;
- et la capacité à coordonner plusieurs acteurs dans une même chaîne de traitement.

Une PUS impose également une gouvernance explicite des événements :

- qualification ;
- validation ;
- escalade ;
- suivi ;
- clôture ;
- et exploitation a posteriori, Retex.

Chaque événement peut ainsi suivre un cycle de traitement impliquant plusieurs niveaux d'intervention et plusieurs métiers.
La continuité opérationnelle dépend alors autant de la qualité de l'organisation que des performances techniques de la plateforme.
Une architecture performante ne compense pas une gouvernance insuffisante. À l'inverse, une organisation structurée permet souvent d'exploiter efficacement des environnements techniques hétérogènes et évolutifs.

4.2. ARCHITECTURES DE RÉFÉRENCE

Une PUS ne repose pas sur un système unique, mais sur l'association de plusieurs composants capables d'échanger des informations et de fonctionner dans une même logique opérationnelle. Ces composants peuvent couvrir des domaines très différents : systèmes vidéo (VMS), contrôle d'accès, capteurs IoT, GTB/GTC, systèmes d'alerte, supervision technique, outils métiers ou encore services de cybersécurité.
L'architecture d'une PUS correspond à la manière dont ces différents éléments sont organisés afin de permettre :

- la circulation des informations ;
- la coordination des traitements ;
- la continuité des opérations ;
- l'évolution progressive des usages.

Une architecture de PUS repose généralement sur plusieurs couches fonctionnelles, comprenant les systèmes sources, les mécanismes d'intégration et d'échange, les moteurs de traitement, les interfaces de restitution ainsi que les outils de supervision, de reporting et de traçabilité.
L'objectif n'est pas uniquement de connecter des systèmes, mais de garantir une circulation cohérente et exploitable de l'information entre plusieurs environnements techniques et opérationnels.
La fluidité entre ces différentes couches constitue un point critique. Une architecture mal maîtrisée peut rapidement générer des délais de traitement, des pertes d'information, des ruptures de chaîne opérationnelle, des limitations d'évolution ou encore des dépendances techniques difficiles à corriger après déploiement.

Deux grands modèles d'architecture coexistent généralement :

- les architectures centralisées ;
- les architectures distribuées ou hybrides.

Le choix dépend notamment des contraintes opérationnelles, des volumes de données, des besoins de scalabilité, des exigences de résilience, des contraintes de cybersécurité ainsi que du niveau d'autonomie attendu sur les sites distants.
L'enjeu n'est donc pas de privilégier un modèle unique, mais de trouver un équilibre cohérent entre centralisation, réactivité locale, continuité opérationnelle et capacité d'évolution dans le temps.

Les architectures modernes de PUS reposent généralement sur des approches modulaires et orientées services permettant de découpler les composants fonctionnels et de limiter les dépendances fortes entre systèmes.
Elles s'appuient fréquemment sur :

- des API REST documentées et versionnées ;
- des bus de messages et mécanismes de publication/souscription (MQTT, AMQP, Kafka) ;
- des architectures orientées services (SOA) ;
- des couches d'abstraction ;
- et des mécanismes d'intégration capables de faire communiquer des systèmes hétérogènes sans dépendance directe entre composants.

Cette approche facilite :

- l'interopérabilité ;
- l'intégration progressive de nouveaux systèmes ;
- la réversibilité ;
- la montée en charge ;
- et l'évolution des usages dans le temps.

Les flux temps réel imposent des contraintes spécifiques :

- synchronisation des événements ;
- maîtrise de la latence ;
- hiérarchisation des priorités ;
- résilience des échanges ;
- continuité de service ;
- et cohérence des traitements distribués.

Les architectures distribuées de type edge computing permettent de rapprocher certains traitements des équipements terrain afin :

- de réduire les volumes remontés ;
- d'améliorer la réactivité ;
- de maintenir certaines fonctions en mode dégradé ;
- et de limiter les dépendances à une infrastructure centrale unique.

Exemple : analyse locale d'un flux vidéo → qualification d'un événement au niveau edge → transmission d'un événement enrichi vers la plateforme centrale → corrélation avec d'autres sources (contrôle d'accès, IoT, cybersécurité) → déclenchement coordonné d'un scénario opérationnel (fiche réflexe, graphe).
Les principaux arbitrages d'architecture portent notamment sur :

- la centralisation ou non des traitements ;
- la répartition des flux ;
- la segmentation IT/OT ;
- la résilience des infrastructures ;
- la scalabilité ;
- la réversibilité ;
- et la limitation des dépendances éditeurs.

Une architecture insuffisamment maîtrisée peut rapidement générer :

- des points de défaillance critiques ;
- des difficultés d'évolution ;
- des limitations de performance ;
- des dépendances contractuelles et techniques fortes ;
- ou des vulnérabilités de cybersécurité impactant l'ensemble de la chaîne opérationnelle.

4.2.1. Centralisée, distribuée, hybride

Le choix d'architecture d'une PUS ne repose pas sur un modèle unique, mais sur un compromis entre contraintes techniques, besoins opérationnels et exigences de résilience.
Une architecture centralisée privilégie le regroupement des traitements et des données au sein d'une plateforme principale. Elle facilite :

- la gouvernance ;
- l'unification des règles ;
- la supervision globale ;
- la cohérence des traitements.

Ce modèle est particulièrement adapté aux environnements disposant d'une connectivité maîtrisée, d'une organisation fortement centralisée et d'un besoin important de pilotage unifié.
À l'inverse, une architecture distribuée rapproche certains traitements du terrain afin :

- d'améliorer la réactivité ;
- de réduire les flux remontés ;
- de maintenir certaines fonctions localement en cas de dégradation réseau.

La plupart des architectures modernes combinent aujourd'hui ces deux approches dans des modèles hybrides. Le choix dépend alors principalement des volumes de données, des contraintes réseau, des exigences de cybersécurité, du niveau d'autonomie attendu sur les sites distants et des objectifs de continuité opérationnelle.
L'enjeu consiste moins à opposer centralisation et distribution qu'à définir une répartition cohérente des traitements, des flux et des responsabilités en fonction des contraintes réelles d'exploitation.
Les principales caractéristiques, limites et contextes d'usages des différents modèles d'architecture peuvent être résumés comme suit :

ARCHITECTURE	AVANTAGES	LIMITES	CAS D'USAGE TYPIQUES
Centralisée	Simplicité de mise en œuvre Supervision et contrôle unifiés Cohérence des données facilitée Sécurité centralisée	Point de défaillance unique Faible tolérance aux pannes Possible latence pour sites distants	Site unique Collectivité non mutualisée
Distribuée	Haute disponibilité Pas de point unique de panne Scalabilité élevée Autonomie locale des sites Performances locales optimisées	Complexité de conception Synchronisation difficile Sécurité plus difficile à homogénéiser	Réseaux multi-sites (banques, retail, collectivités mutualisées) Infrastructures critiques (transport, énergie) Environnements avec contraintes réseau
Hybride	Équilibre entre centralisation et autonomie Résilience améliorée Scalabilité progressive Optimisation des performances globales	Architecture complexe Gestion des synchronisations délicate Gouvernance nécessaire	Grandes entreprises multi-sites Aéroports, smart cities Systèmes de sûreté intégrés (PSIM) Organisations avec supervision centrale + opérations locales (CSD, CSUI...)

Les architectures distribuées de type edge computing permettent d'exécuter localement certains traitements :

- analyse vidéo ;
- filtrage d'événements ;
- pré-corrélation ;
- ou maintien de fonctions critiques en mode dégradé.

Exemple : des événements qualifiés localement peuvent être remontés vers une plateforme centrale via des mécanismes de publication/souscription ou des bus de messages, afin de limiter les flux bruts et de préserver la réactivité opérationnelle.
Les principaux arbitrages portent alors sur :

- la localisation des traitements ;
- la cohérence des règles distribuées ;
- la segmentation IT/OT ;
- la résilience en cas de perte de liaison ;
- et la scalabilité globale de l'architecture.

Une mauvaise répartition des traitements peut créer :

- des points de saturation ;
- des incohérences opérationnelles ;
- des dépendances excessives ;
- ou des difficultés d'évolution à long terme.

4.2.2. Avantages, limites et contextes d'usage

Une PUS repose sur la capacité à faire fonctionner ensemble plusieurs systèmes issus d'environnements différents.
En pratique, cette interopérabilité reste souvent partielle.
De nombreux équipements ou logiciels proposent des connecteurs ou des API permettant certains échanges, sans pour autant garantir une intégration complète des fonctionnalités.
Exemple : un système vidéo peut remonter des alertes vers une PUS sans pour autant permettre le pilotage avancé des équipements, l'accès aux métadonnées spécifiques du constructeur ou l'intégration complète dans des scénarios automatisés.
À l'inverse, certains systèmes fortement intégrés peuvent créer une dépendance importante vis-à-vis d'un éditeur ou d'un écosystème spécifique, limitant :

- les possibilités d'évolution ;
- l'intégration de nouveaux composants ;
- la réversibilité de l'architecture.

L'interopérabilité ne doit donc pas être considérée comme acquise ou uniquement déclarative. Elle doit être vérifiée dans des conditions réelles d'exploitation, en tenant compte des usages opérationnels, des contraintes d'évolution et des dépendances techniques effectivement constatées sur le terrain.

La majorité des architectures reposent sur des mécanismes d'intégration hétérogènes :

- API propriétaires ;
- SDK spécifiques ;
- connecteurs éditeurs ;
- protocoles partiellement ouverts ;
- ou couches d'abstraction limitées à certains usages.

Ces mécanismes permettent généralement une communication fonctionnelle, mais rarement une interopérabilité complète entre systèmes.

Le principal risque réside dans le verrouillage technologique :
• dépendance contractuelle ;
• limitations d'évolution ;
• difficultés de réversibilité ;
• incompatibilités lors des mises à jour ;
•nécessité de développements spécifiques pour chaque évolution majeure.
Exemple : une plateforme fortement couplée à un VMS propriétaire peut exploiter certaines fonctions standard, tout en nécessitant des développements spécifiques pour accéder à certaines capacités avancées, comme les métadonnées constructeur, les fonctions PTZ étendues, les mécanismes analytics ou les workflows complexes.
Les architectures pérennes privilégient donc :
- des interfaces documentées ;
- des mécanismes ouverts et versionnés ;
- des tests d'interopérabilité réels ;
- une limitation des dépendances critiques entre composants.

L'objectif n'est pas uniquement de connecter des systèmes, mais de préserver dans le temps l'évolutivité, la scalabilité, la résilience et la capacité de réversibilité de l'architecture.

4.2.3. Synchronisation temporelle et cohérence des événements

Dans une PUS, , la valeur opérationnelle des informations ne repose pas uniquement sur leur disponibilité ou leur capacité à être partagées. Elle dépend également de la cohérence temporelle entre des événements issus de sources multiples, parfois réparties sur plusieurs sites, réseaux ou environnements techniques. Une chronologie imprécise fragilise immédiatement la capacité à corréler les informations, à qualifier une situation et à coordonner efficacement les décisions.

Un des pièges récurrents consiste à considérer que des événements apparaissant simultanément à l'écran sont nécessairement synchrones. En réalité, les différences de latence entre les chaînes de capture, de traitement, de transmission ou d'affichage peuvent atteindre plusieurs secondes, voire davantage, y compris au sein d'un même système. À cela s'ajoutent des décalages d'horloge parfois beaucoup plus importants entre équipements ou plateformes : mauvaise configuration, dérive temporelle, fuseaux horaires différents, gestion incohérente de l'heure d'été ou coexistence entre heure locale et UTC/GMT. Cette illusion de simultanéité constitue une source fréquente d'erreurs d'analyse et de corrélation.

Dans une architecture PUS, la référence temporelle ne peut donc pas reposer sur l'instant d'affichage ou de réception des informations, mais sur une datation absolue à la capture, cohérente et partagée entre les systèmes. Cette cohérence repose généralement sur des mécanismes de synchronisation de type NTP ou PTP associés à des serveurs de temps ou horloges de référence centralisées, parfois synchronisés eux-mêmes sur des sources GNSS/GPS dans les architectures critiques ou multisites.

La synchronisation temporelle constitue ainsi un invariant d'architecture souvent sous-estimé. Une PUS agrège des flux vidéo, des événements de contrôle d'accès, des alertes techniques, des journaux cybersécurité, des données IoT ou des mécanismes d'automatisation qui doivent pouvoir être reconstruits dans une séquence fiable et opposable. Sans référence temporelle maîtrisée, les mécanismes de corrélation perdent en pertinence, les scénarios automatisés deviennent fragiles et les investigations peuvent être partiellement remises en cause.

Dans les environnements multi-acteurs et multisites, cette exigence devient encore plus critique. À mesure que les plateformes intègrent davantage d'automatisation, d'analyses temps réel et de coordination inter-systèmes, la maîtrise de la cohérence temporelle devient une condition structurante de la continuité opérationnelle, de la fiabilité décisionnelle et de la confiance globale dans la donnée opérationnelle.

Une PUS mature ne doit donc jamais considérer la synchronisation temporelle comme un simple paramètre technique d'infrastructure, mais comme un élément fondamental de gouvernance de la donnée et de crédibilité opérationnelle de l'ensemble de la chaîne de supervision.

4.3. INTEROPÉRABILITÉ ET RÉSILIENCE OPÉRATIONNELLE

L'interopérabilité constitue un enjeu central d'une PUS. Connecter des systèmes ne garantit pas, à lui seul, une interopérabilité réelle ni une continuité opérationnelle cohérente.
En pratique, certains équipements ou logiciels permettent des échanges limités sans assurer la cohérence des données, la synchronisation des états, le pilotage croisé des équipements ou l'intégration complète dans des scénarios opérationnels.
Une interopérabilité insuffisamment maîtrisée peut alors générer :
- des ruptures de chaîne opérationnelle ;
- des pertes de contexte ;
- des dépendances fortes entre technologies ou fournisseurs ;
- des limitations d'évolution et d'intégration future.

Les enjeux dépassent donc largement la simple compatibilité technique. La maîtrise des échanges, des flux et des dépendances conditionne directement la résilience globale, l'évolutivité et la cohérence opérationnelle de la PUS.

Les architectures modernes reposent généralement sur :
- des API documentées et versionnées ;
- des mécanismes de publication/souscription ;
- des bus de messages (MQTT, AMQP, Kafka) ;
- des couches d'abstraction ;
- des architectures orientées services permettant de découpler les composants.

Ces mécanismes facilitent l'intégration progressive de nouveaux systèmes, la scalabilité, la réversibilité et la limitation des dépendances technologiques. Ils introduisent toutefois de nouvelles contraintes liées à la synchronisation des flux, à la cohérence des événements distribués, à la segmentation IT/OT, à la supervision des échanges, à la sécurisation des interfaces et à la gestion des dépendances critiques.
La résilience repose notamment sur :
- la redondance des composants critiques ;
- des mécanismes de reprise (PRA/PCA) ;
- des modes dégradés ;
- des capacités locales de fonctionnement ;
- une supervision continue des flux et des accès (IAM, SIEM, SOC).

Une architecture résiliente ne dépend donc pas uniquement de la robustesse des composants individuels, mais de la capacité globale du système à maintenir des échanges cohérents, sécurisés et exploitables, y compris en situation dégradée.
Exemple : une compromission d'un système périphérique ne doit pas permettre une propagation latérale vers l'ensemble de la plateforme ou une interruption globale des opérations.
Une PUS résiliente ne repose donc pas uniquement sur la robustesse technique des composants, mais sur la maîtrise globale :
- des échanges ;
- des dépendances ;
- des flux ;
- des accès ;
- et des mécanismes de gouvernance associés.

4.3.1. Gouvernance des accès et des habilitations

Une PUS centralise des informations sensibles, des capacités d'action et des mécanismes de coordination pouvant impacter directement les opérations. La gestion des accès constitue donc un enjeu majeur de gouvernance et de sécurité.

Tous les utilisateurs ne doivent pas disposer des mêmes droits. Selon les contextes et les responsabilités, les habilitations peuvent notamment concerner :

- la consultation ;
- le pilotage ;
- l'administration ;
- le déclenchement d'actions ;
- l'export de données ;
- l'accès aux fonctions critiques.

Ces droits doivent être définis en fonction des rôles, des responsabilités, des besoins opérationnels et du niveau de sensibilité des informations manipulées. Une mauvaise gestion des accès peut entraîner des erreurs de manipulation, des pertes de confidentialité, des actions non autorisées ou des difficultés d'analyse en cas d'incident.
La traçabilité des actions constitue également un point essentiel afin de garantir l'auditabilité, le suivi des opérations et la responsabilité des interventions réalisées.

Les architectures avancées de PUS reposent généralement sur des mécanismes de gestion centralisée des identités et des habilitations (IAM), intégrant :

- RBAC (Role-Based Access Control) ;
- ABAC (Attribute-Based Access Control) ;
- fédération d'identité ;
- SSO ;
- comptes de service ;
- journalisation des actions sensibles.

Ces mécanismes permettent de renforcer la maîtrise des accès, de limiter les privilèges excessifs et de conserver une vision exploitable des opérations réalisées au sein de la plateforme, ils permettent

- de segmenter les droits ;
- de limiter les privilèges excessifs ;
- de contrôler les accès inter-systèmes ;
- de renforcer la traçabilité des opérations critiques.

Les environnements multi-acteurs imposent également une séparation claire des responsabilités, une gestion fine des accès temporaires ainsi qu'un contrôle rigoureux des échanges entre environnements IT et OT.

Exemple : un opérateur peut visualiser certains flux vidéo sans pour autant disposer des droits d'export, des capacités d'administration ou du pilotage des équipements critiques.
Une gouvernance insuffisamment maîtrisée des accès peut rapidement compromettre :

- la sécurité globale ;
- la conformité réglementaire ;
- la résilience opérationnelle ;
- la confiance dans les mécanismes de coordination de la PUS.

Dans une architecture fortement interconnectée, la maîtrise des habilitations devient donc un élément structurant de la gouvernance opérationnelle autant que de la cybersécurité.

4.3.2. Continuité opérationnelle et fonctionnement en mode dégradé

Une PUS doit permettre de maintenir des capacités opérationnelles essentielles même en cas :

- de panne ;
- de perte réseau ;
- de perte d'énergie (220V)
- d'incident technique ;
- ou d'indisponibilité partielle de l'infrastructure.

L'objectif n'est pas uniquement d'éviter l'arrêt du système, mais de garantir la continuité des fonctions critiques nécessaires à l'exploitation opérationnelle.
En situation dégradée, certaines fonctions peuvent être maintenues localement :

- supervision ;
- gestion des alertes ;
- accès aux flux essentiels ;
- ou coordination des interventions.

Exemple : une perte de connexion avec un site distant ne doit pas empêcher les équipes locales de continuer à exploiter les équipements essentiels et à assurer les premières actions opérationnelles.
La continuité opérationnelle peut également reposer sur des mécanismes de repli organisationnel ou de mutualisation entre plusieurs structures :

- CSU,
- CSUi / CSD,
- PC de télésurveillance,
- Centres opérationnels partenaires,
- Police Nationale / Gendarmerie,
- ou exploitants multisites.

Une PUS bien conçue doit permettre de maintenir une capacité minimale de coordination et de supervision, même dans des conditions fortement dégradées.

Les architectures résilientes reposent généralement sur :

- des mécanismes de redondance ;
- des PCA/PRA ;
- des infrastructures distribuées ;
- des capacités de bascule ;
- et des modes de fonctionnement autonomes ou synchronisés.

Les architectures distribuées de type edge computing permettent notamment de maintenir localement certaines fonctions critiques :

- analyse vidéo ;
- gestion d'alarmes ;
- contrôle d'accès ;
- exécution de scénarios ;
- ou conservation des journaux opérationnels.

Les événements peuvent ensuite être resynchronisés avec la plateforme centrale après rétablissement des communications.
Les principaux arbitrages portent notamment sur :

- les délais de reprise ;
- la cohérence des données distribuées ;
- la priorisation des fonctions critiques ;
- la tolérance aux pannes ;
- et le maintien des capacités opérationnelles sous contrainte.

Exemple : attaque ransomware sur l'infrastructure centrale → bascule vers des capacités locales isolées → maintien des fonctions critiques → reprise progressive après restauration → consolidation et analyse des événements en main courante.

La continuité opérationnelle repose également sur une préparation organisationnelle :

- scénarios de crise ;
- rôles définis ;
- circuits de décision adaptés ;
- procédures de repli ;
- et exercices réguliers.

Une PUS insuffisamment préparée aux situations dégradées peut devenir inopérante au moment même où elle est la plus critique.

4.4. SOUVERAINETÉ, MAÎTRISE ET PÉRENNITÉ DES ARCHITECTURES

4.4.1. Dépendance technologiques éditeur et réversibilité

Une PUS doit permettre de faire évoluer l'architecture sans remettre en cause l'ensemble du système. Certaines solutions offrent une intégration forte, mais créent également des dépendances importantes liées à des technologies propriétaires, des interfaces fermées, des mécanismes d'échange limités ou des difficultés d'intégration avec d'autres systèmes.

Une dépendance excessive peut rapidement compliquer l'ajout de nouveaux équipements, le changement de fournisseur, l'évolution des usages ou encore la maîtrise des coûts dans le temps.

La réversibilité correspond précisément à la capacité de faire évoluer ou remplacer certaines briques techniques sans reconstruire l'ensemble de la plateforme. Une architecture pérenne privilégie donc

- des interfaces ouvertes ;
- des API documentées ;
- des formats d'échange standardisés ;
- une séparation claire des composants.

L'objectif n'est pas uniquement de limiter les dépendances techniques, mais de conserver dans le temps une capacité réelle d'évolution, d'intégration et de maîtrise de l'architecture.

Le verrouillage technologique apparaît fréquemment au niveau des API propriétaires, des métadonnées non exportables, des moteurs de scénarios, des workflows ou encore des mécanismes de corrélation spécifiques à un éditeur. Ces dépendances deviennent souvent visibles lors des évolutions majeures, des migrations ou des changements d'intégrateur.

Une réversibilité réellement exploitable suppose notamment :

- la portabilité des scénarios IF/THEN ;
- l'export des historiques et métadonnées ;
- le découplage des couches fonctionnelles ;
- l'indépendance des moteurs métier vis-à-vis des systèmes sources.

Sans cette capacité de réversibilité, chaque évolution importante risque de transformer la plateforme en architecture difficilement maintenable, coûteuse à faire évoluer et fortement dépendante de choix techniques réalisés plusieurs années auparavant.

Exemple : le remplacement d'un VMS ne devrait pas imposer la reconstruction complète des scénarios opérationnels ou la perte des historiques exploitables.

4.4.2. Localisation, gouvernance et maîtrise des données

Une PUS centralise et échange des données sensibles : flux vidéo, événements, historiques, données techniques ou informations opérationnelles. La maîtrise de ces données constitue donc un enjeu majeur de gouvernance, de sécurité et de conformité.
Les questions essentielles portent notamment sur :

- la localisation des données ;
- les droits d'accès ;
- les capacités d'export ;
- les durées de conservation ;
- le partage entre acteurs ou systèmes.

Selon les choix d'architecture retenus (local, cloud ou hybride), les données peuvent être réparties entre plusieurs infrastructures ou prestataires. Une gouvernance insuffisamment maîtrisée peut alors entraîner une perte de contrôle, des difficultés d'audit, des risques réglementaires ou une dépendance excessive à certains fournisseurs.
Une PUS doit donc garantir :

- la traçabilité des accès ;
- l'intégrité des données ;
- la maîtrise des flux ;
- la capacité à conserver une exploitation cohérente dans le temps.

La problématique ne concerne donc pas uniquement le stockage des données, mais la capacité globale de l'organisation à conserver durablement la maîtrise des usages, des échanges et des responsabilités associés à ces informations sensibles.

Les architectures avancées doivent intégrer :

- segmentation IT/OT ;
- contrôle d'accès granulaire ;
- journalisation des échanges ;
- politiques de conservation ;
- et auditabilité des traitements.

Les enjeux critiques concernent notamment :

- les flux inter-organisations ;
- les dépendances cloud ;
- la maîtrise des métadonnées ;
- et les contraintes de souveraineté réglementaire (RGPD, NIS2, CRA).

Une architecture maîtrisée doit permettre :

- l'export exploitable des données ;
- la reconstruction des événements ;
- et la vérification des traitements réalisés.

4.4.3. Pérennité et évolutivité des architectures

Une PUS s'inscrit dans une durée d'exploitation longue. Les choix techniques réalisés lors de sa conception auront un impact pendant de nombreuses années.
Une architecture trop rigide peut rapidement devenir difficile à faire évoluer :

- ajout de nouveaux équipements ;
- intégration de nouveaux usages ;
- évolutions réglementaires ;
- évolution des versions logicielles des composants hypervisés ;
- ou augmentation des volumes de données.

La pérennité d'une PUS repose donc sur sa capacité à évoluer progressivement sans remise en cause globale du système.
Une architecture évolutive privilégie :

- la modularité ;
- le découplage des composants ;
- des interfaces standardisées ;
- et une intégration progressive des nouvelles briques techniques.

L'objectif n'est pas uniquement de répondre au besoin immédiat, mais de conserver une capacité d'adaptation dans le temps.

Les architectures pérennes reposent généralement sur :

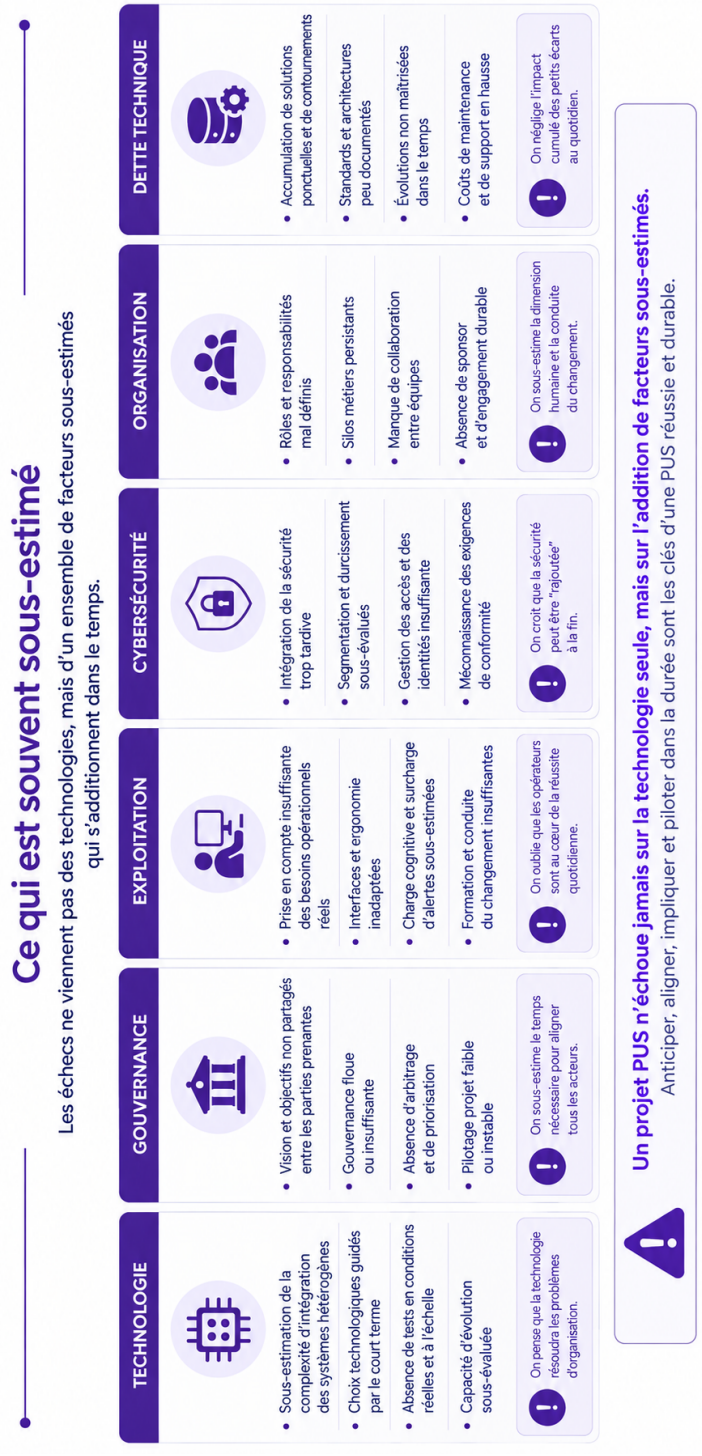
- des API versionnées ;
- des mécanismes d'abstraction ;
- des composants faiblement couplés ;
- et une séparation claire entre :
  - o données,
  - o logique métier,
  - o interfaces,
  - o et moteurs de traitement.

Les principaux risques d'évolution concernent la dette technique, les dépendances non maîtrisées, les workflows non portables, les composants non substituables ou encore les montées de version incompatibles. Avec le temps, ces fragilités peuvent fortement compliquer l'exploitation et limiter les capacités d'évolution de la plateforme.
Une architecture insuffisamment évolutive peut ainsi transformer chaque évolution :

- en projet complexe ;
- en interruption opérationnelle ;
- en refonte partielle du système.

La pérennité d'une PUS dépend donc autant de la qualité des choix techniques initiaux que de la capacité à gouverner les évolutions, les dépendances et la complexité dans le temps.

Les principales causes d'échec ou de fragilité des projets PUS peuvent être résumées comme suit



Ce qu'il est indispensable de maitriser pour réussir l'implantation d'une PUS.

PARTIE 1 :
PUS EN ESPACES OUVERTS AU PUBLIC

5. PUS EN ESPACES OUVERTS AU PUBLIC

Cette partie regroupe les espaces publics et les espaces privés ouverts au public, initialement distingués dans ce document en bleu et orange. Malgré des contextes d'exploitation différents, ces environnements partagent des contraintes proches : multiplicité des acteurs, accueil du public, continuité d'exploitation, gestion des flux et coordination opérationnelle en temps réel.
Les attentes ne sont toutefois pas identiques selon les usages. Une collectivité territoriale, une gare, un centre commercial, un stade ou un campus ne poursuivent pas les mêmes objectifs et ne gèrent pas les mêmes niveaux de risque. La PUS ne peut donc pas être pensée comme un modèle uniforme.
Dans ces environnements, la valeur d'une PUS repose principalement sur sa capacité à agréger des informations hétérogènes, à réduire les ruptures d'information et à faciliter la coordination entre acteurs publics, exploitants et services opérationnels.
L'enjeu n'est pas de tout centraliser, mais de disposer d'une vision exploitable des situations afin d'améliorer la réactivité, la continuité de service et la gestion des événements.



Vue fonctionnelle d'un territoire et de services interconnectés autour d'une logique PUS

5.1. S – STRATÉGIE

5.1.1. Finalités opérationnelles et intérêt général

Dans les espaces ouverts au public, une PUS ne peut pas être pensée comme une simple évolution technologique des centres de supervision existants. Elle modifie la manière dont plusieurs acteurs :

- partagent l'information ;
- coordonnent leurs actions ;
- gèrent les incidents ;
- arbitrent les priorités ;
- et pilotent certaines fonctions opérationnelles du territoire ou du site exploité.

Les attentes diffèrent fortement selon les contextes. Une collectivité cherchera principalement à améliorer la coordination territoriale, la gestion de crise ou la continuité de certains services publics. À l'inverse, un exploitant de transport, un centre commercial ou un site événementiel accordera souvent une priorité plus forte :

- à la fluidité des usages ;
- à la continuité d'exploitation ;
- à la gestion des incidents ;
- à l'image du site ;
- ou à la qualité d'expérience des usagers.

Ces objectifs peuvent d'ailleurs entrer en tension.
Une logique de sécurité maximale peut par exemple dégrader :

- la fluidité ;
- l'accessibilité ;
- l'exploitation ;
- ou l'acceptabilité du dispositif.

Inversement, une approche centrée uniquement sur l'expérience usager ou l'optimisation des flux peut conduire à sous-estimer certains enjeux de sûreté, de résilience ou de gestion de crise.
La difficulté stratégique consiste précisément à arbitrer entre ces priorités sans transformer la PUS en outil de centralisation excessive ou en démonstrateur technologique déconnecté des besoins réels du terrain.
Une PUS efficace repose donc moins sur le nombre de systèmes connectés que sur la clarté :

- des objectifs poursuivis ;
- des cas d'usage réellement utiles ;
- des responsabilités ;
- et des limites fixées au dispositif.

Dans ce cadre, la plateforme doit s'inscrire dans une stratégie opérationnelle cohérente avec :

- les politiques publiques ou d'exploitation ;
- les contraintes juridiques ;
- les capacités humaines réelles ;
- le niveau de maturité des organisations ;
- et les ressources disponibles dans la durée.

5.1.2. Ce qui n'est pas souhaitable

L'un des risques fréquents consiste à considérer la PUS comme une finalité en soi, avec une logique de centralisation systématique ou d'hyperconnexion généralisée des systèmes disponibles.
Dans les espaces ouverts au public, certaines approches doivent au contraire être explicitement évitées :

- accumulation de flux sans doctrine d'exploitation claire ;

- multiplication des cas d'usage sans gouvernance ;
- automatisation excessive ;
- dépendance forte à un intégrateur ou à un fournisseur unique ;
- empilement de fonctionnalités peu exploitées ;
- ou création de "centres de commandement" surdimensionnés sans besoins opérationnels réels.

Les projets les plus fragiles sont souvent ceux qui démarrent par la technologie avant d'avoir défini :

- les responsabilités ;
- les priorités opérationnelles ;
- les chaînes de décision ;
- les conditions d'exploitation ;
- et les limites du dispositif.

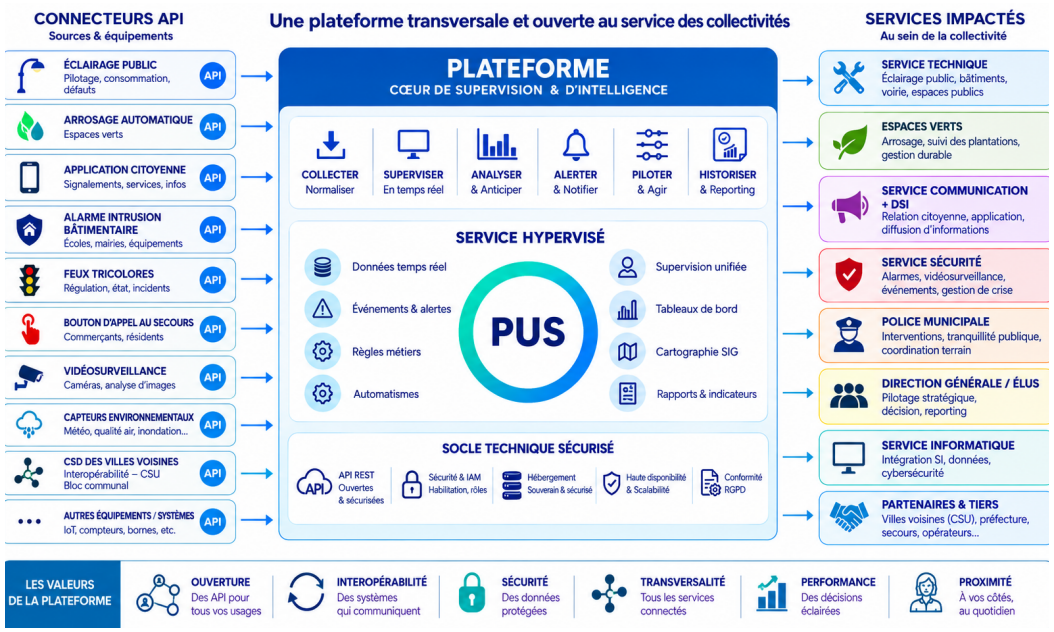
Dans certains cas, la promesse de convergence peut même produire l'effet inverse :

- surcharge informationnelle ;
- dilution des responsabilités ;
- dépendance technique accrue ;
- complexité d'exploitation ;
- ou perte de lisibilité pour les opérateurs.

Une PUS n'a donc pas vocation à «tout superviser». Elle doit avant tout permettre une meilleure compréhension des situations réellement utiles à l'exploitation, à la sécurité et à la continuité de service.

Dans les espaces ouverts au public, la maturité stratégique d'un projet se mesure souvent moins à l'ampleur de l'architecture déployée qu'à la capacité à dire clairement :

- ce qui doit être connecté ;
- ce qui ne doit pas l'être ;
- pourquoi et par qui ;
- et dans quelles limites !



Exemple d'écosystème interopérable autour d'une plateforme unifiée de supervision territoriale

5.2. O – ORGANISATION

5.2.1. Gouvernance, coordination et structuration du projet

La mise en œuvre d'une PUS dans des espaces ouverts au public ne peut pas être abordée comme un simple projet technique ou informatique. Elle modifie les modes de coordination, les chaînes de décision et les interactions entre plusieurs services ou exploitants disposant souvent de priorités différentes.

Le principal risque consiste à construire la plateforme avant d'avoir réellement structuré les besoins opérationnels, les responsabilités et les usages attendus. Dans ce type de projet, une mauvaise organisation initiale produit généralement des conséquences durables : architecture inadaptée, fonctionnalités peu exploitées, surcharge des opérateurs, multiplication des demandes correctives ou dépendance excessive à l'intégrateur.

La phase amont constitue donc un **point critique**. Elle impose la mise en place d'une équipe projet pluridisciplinaire associant :

- directions métiers ;
- exploitation ;
- sécurité/sûreté ;
- services techniques ;
- systèmes d'information ;
- cybersécurité ;
- opérateurs terrain ;
- maintenance ;
- DGS ou directions générales selon les organisations ;
- ainsi qu'une assistance à maîtrise d'ouvrage (AMO) capable de structurer les besoins et les arbitrages.

Cette gouvernance amont doit permettre de définir :

- les finalités réelles du projet ;
- les cas d'usage prioritaires ;
- les scénarios opérationnels ;
- les niveaux de responsabilité ;
- les conditions de partage des données ;
- les systèmes à intégrer ;
- ainsi que les limites assumées du périmètre fonctionnel.

Ces arbitrages sont structurants.

Exemple :

- faut-il intégrer l'éclairage public dans la PUS ?
- les systèmes GTB/GTC doivent-ils être hypervisés ?
- une application citoyenne doit-elle être intégrée ? ou flux des réseaux sociaux ?
- quels services disposent d'un accès temps réel ?
- quelles actions peuvent être automatisées ?
- quels événements relèvent d'une coordination interservices ?
- quelles données doivent rester cloisonnées ?

Ces décisions ne relèvent pas uniquement de la technique. Elles engagent directement l'organisation future, les responsabilités opérationnelles, la cybersécurité, les contraintes juridiques ainsi que les capacités réelles d'exploitation du dispositif.

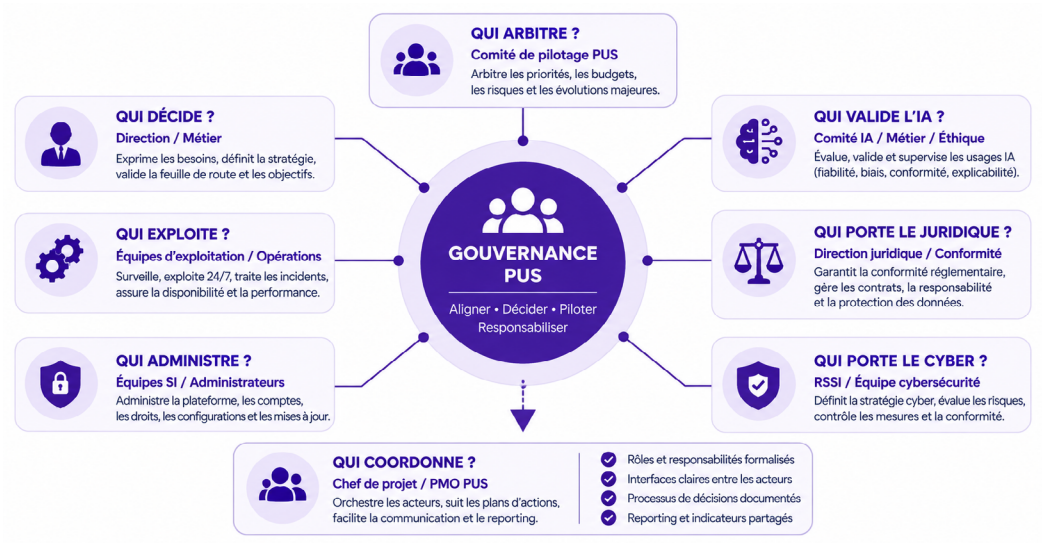
Une PUS efficace repose donc autant sur la qualité de cette structuration initiale que sur les performances des solutions déployées. Sans gouvernance claire et sans doctrine d'exploitation partagée, la plateforme risque de devenir un empilement supplémentaire de systèmes plutôt qu'un véritable outil de coordination opérationnelle.

5.2.2. Coordination opérationnelle et exploitation quotidienne

Une fois déployée, une PUS impose également une organisation d'exploitation claire :

- rôles des opérateurs ;
- responsabilités du chef de salle ;
- coordination avec les services techniques ;
- articulation avec les exploitants et partenaires externes ;
- gestion des escalades et des situations dégradées ;
- contrat de maintenance efficace.

Dans les espaces ouverts au public, plusieurs acteurs peuvent être simultanément impliqués dans un même événement : sécurité, mobilité, maintenance, exploitation technique, secours ou autorités publiques. La plateforme ne remplace pas cette organisation ; elle la rend immédiatement visible.
L'enjeu n'est donc pas uniquement de partager des informations, mais de garantir une capacité réelle de coordination entre acteurs disposant de compétences, de responsabilités et de temporalités différentes.
Une PUS mal gouvernée accélère la circulation des alertes.
Une PUS bien gouvernée accélère la résolution des situations.



Une gouvernance claire est le socle d'une PUS fiable, sécurisée et évolutive

5.3. T – TECHNOLOGIE

5.3.1. Contraintes des espaces ouverts au public

Les espaces ouverts au public présentent des contraintes techniques et opérationnelles particulières : contraintes des marchés publics, multiplicité des équipements, environnements évolutifs, variabilité des usages, gestion du temps réel et forte exposition aux incidents ou aux situations imprévues.

Une PUS doit donc pouvoir intégrer des systèmes hétérogènes souvent déployés progressivement au fil du temps :

- vidéoprotection ;
- contrôle d'accès ;
- GTB/GTC ;
- capteurs IoT ;
- mobilité ;
- supervision technique ;
- systèmes métiers ;
- outils de gestion d'incident ou de crise.

Dans ces environnements, la valeur opérationnelle dépend fortement :

- de la qualité de contextualisation des événements ;
- de la capacité de corrélation entre systèmes ;
- de la réactivité des échanges ;
- et du maintien de capacités opérationnelles même en mode dégradé.

Les architectures doivent également rester suffisamment évolutives pour intégrer de nouveaux usages, de nouveaux équipements ou de nouveaux acteurs sans remise en cause globale du dispositif.

5.3.2. Interopérabilité, cybersécurité et résilience

L'interopérabilité constitue l'un des enjeux techniques majeurs d'une PUS ouverte au public. Une plateforme peut connecter plusieurs systèmes sans pour autant produire une réelle coordination opérationnelle.

Les choix d'architecture doivent donc privilégier :

- des standards ouverts ;
- des API documentées ;
- des mécanismes d'intégration auditables ;
- une limitation des dépendances éditeurs ;
- des capacités d'évolution dans le temps.

Cette interopérabilité concerne autant les systèmes que les organisations elles-mêmes. Les données utiles à la gestion d'un événement peuvent provenir simultanément d'une collectivité, d'un exploitant de transport, d'un centre commercial, d'un gestionnaire d'infrastructure ou encore d'un partenaire institutionnel. La plateforme doit permettre ces échanges sans ambiguïté sur les responsabilités, les droits d'accès ou l'origine des données.

Dans ces environnements fortement interconnectés, la cybersécurité devient également structurante. Une PUS concentre des flux critiques, des capacités d'action et des informations sensibles pouvant impacter directement l'exploitation ou la continuité de service.

Les exigences principales concernent notamment :
- la maîtrise des accès et des habilitations ;
- la traçabilité des actions ;
- la sécurisation des interfaces ;
- la segmentation des environnements ;
- la supervision des échanges ;
- les capacités de continuité d'activité en cas d'incident ou d'attaque.

La robustesse d'une PUS ne dépend donc pas uniquement des logiciels déployés, mais de la capacité globale de l'architecture à rester exploitable, résiliente et gouvernable dans le temps.

5.3.3. Supervision augmentée et automatisation

Les PUS modernes permettent également d'automatiser certains traitements ou certaines actions opérationnelles :
- affichage dynamique de flux vidéo ;
- ouverture de fiches réflexes ;
- remontée contextualisée d'événements ;
- pilotage coordonné d'équipements ;
- ou déclenchement de scénarios conditionnels.

L'objectif n'est pas de remplacer les opérateurs, mais de réduire leurs délais de réaction, de limiter les ruptures d'information et d'améliorer la coordination entre services.
Dans les espaces ouverts au public, ces mécanismes doivent toutefois rester proportionnés, supervisés et compatibles avec les responsabilités humaines de décision et d'exploitation.

5.4. A – ASPECTS FINANCIERS

5.4.1. Mutualisation, soutenabilité et modèles économiques

Dans les espaces ouverts au public, la question financière ne peut pas être réduite au seul coût d'acquisition de la plateforme, mais doit également intégrer les coûts de fonctionnement dans la durée. Une PUS engage durablement l'organisation, l'exploitation, la cybersécurité, la maintenance, les évolutions fonctionnelles, la gouvernance des données ainsi que les capacités humaines nécessaires au fonctionnement du dispositif.

Le coût réel d'un projet dépend notamment :
- des choix d'architecture ;
- du périmètre fonctionnel ;
- de l'organisation retenue ;
- du niveau d'interopérabilité recherché ;
- de la solution technique elle-même.

Dans les collectivités et les environnements ouverts au public, plusieurs modèles coexistent : déploiement porté par une collectivité ou un exploitant principal, mutualisation entre plusieurs acteurs, centres de supervision partagés, exploitation multisites ou intégration progressive dans une stratégie plus large de transformation numérique territoriale.

La mutualisation constitue souvent un levier économique important, notamment pour :
- l'hébergement ;
- la cybersécurité ;
- les infrastructures ;
- certaines fonctions d'exploitation ;
- les capacités de supervision h24, 365j/an.

Elle suppose toutefois une gouvernance claire, des responsabilités identifiées et des besoins réellement convergents. Une mutualisation mal structurée peut rapidement déplacer la complexité organisationnelle au lieu de réduire durablement les coûts.

Les choix financiers doivent également intégrer la durée de vie réelle du dispositif :
- évolutions réglementaires ;
- maintien en condition de sécurité ;
- remplacement progressif des équipements ;
- dépendances fournisseurs ;
- gestion fine des appels d'offres ;
- et montée en charge des usages.

Une PUS n'est donc pas un investissement ponctuel, mais une infrastructure évolutive dont les coûts d'exploitation et de gouvernance deviennent rapidement structurants.

5.4.2. Limites des approches ROI simplistes

Les projets de PUS sont parfois présentés à travers des promesses rapides de retour sur investissement. Dans les espaces ouverts au public, cette approche doit être fortement nuancée.

Les bénéfices les plus importants ne se traduisent pas toujours par des économies directes immédiatement mesurables. Ils concernent souvent :
- l'amélioration de la coordination ;
- la réduction des délais de réaction ;
- la continuité de service ;
- la meilleure gestion des incidents ;
- la réduction de certaines inefficiences ;
- ou l'amélioration de la qualité opérationnelle globale.

À l'inverse, plusieurs erreurs d'analyse sont fréquentes :
- surestimation des gains liés à l'automatisation ;
- sous-évaluation des coûts d'intégration ;
- oubli des charges humaines d'exploitation ;
- dépendance croissante aux prestataires ;
- ou sous-estimation des coûts de cybersécurité et de conformité.

Le retour sur investissement dépend fortement :
- du niveau de maturité initial ;
- des cas d'usage réellement exploités ;
- de la qualité de la gouvernance ;
- et de l'appropriation opérationnelle du dispositif.

Une plateforme techniquement performante mais peu intégrée dans l'organisation produira souvent moins de valeur qu'un dispositif plus simple mais réellement exploité par les équipes opérationnelles.

5.5. J – JURIDIQUE

5.5.1. CSI, RGPD, IA Act, NIS2, CRA et gouvernance des usages

Le déploiement d'une PUS dans des espaces ouverts au public s'inscrit dans un environnement juridique particulièrement structurant. Ces dispositifs ne relèvent pas uniquement d'un projet technique : ils touchent simultanément :

- à la sécurité publique ;
- à la protection des données ;
- à la cybersécurité ;
- aux responsabilités des acteurs ;
- et, dans certains cas, à l'usage de traitements algorithmiques ou d'intelligence artificielle.

En France, le Code de la sécurité intérieure (CSI) constitue un cadre central dès lors que le dispositif mobilise des outils de vidéoprotection dans l'espace public ou dans des espaces ouverts au public. Il encadre notamment :

- les finalités autorisées ;
- les conditions d'exploitation ;
- les durées de conservation ;
- et les conditions d'accès aux images et données associées.

Le RGPD s'applique dès lors que la plateforme traite des données à caractère personnel, ce qui est fréquent dans les dispositifs d'hypervision. Il impose notamment :

- des finalités explicites ;
- une proportionnalité des traitements ;
- une gouvernance claire des accès ;
- la sécurisation des données ;
- ainsi qu'une traçabilité des usages et des consultations.

L'IA Act introduit désormais un niveau d'exigence supplémentaire pour certains traitements algorithmiques appliqués à des environnements publics, notamment lorsque les systèmes participent à l'analyse automatisée de situations, de comportements ou d'événements.

NIS2 renforce quant à lui les exigences de cybersécurité applicables à de nombreuses entités publiques, opérateurs et infrastructures essentielles. Une PUS interconnectée peut directement devenir un élément structurant de cette chaîne de résilience :

- gestion des accès ;
- maintien en condition de sécurité ;
- supervision des incidents ;
- dépendances fournisseurs ;
- continuité opérationnelle ;
- et gouvernance des risques.

Enfin, le règlement européen Cyber Resilience Act (CRA) introduit progressivement des exigences de cybersécurité applicables aux produits numériques et aux composants connectés utilisés dans ces architectures. À terme, les équipements, logiciels et solutions intégrés dans une PUS devront démontrer un niveau minimal de sécurité, de maintien en condition et de gestion des vulnérabilités sur l'ensemble de leur cycle de vie.

L'enjeu, pour les porteurs de projets, n'est donc pas de traiter ces réglementations séparément, mais de construire une gouvernance cohérente entre :

- sécurité ;
- exploitation ;
- cybersécurité ;
- protection des données ;
- et usages opérationnels.

5.5.2. Responsabilités, partage des données et zones grises

L'un des principaux enjeux juridiques d'une PUS réside dans la multiplicité des acteurs impliqués :

- collectivités ;
- exploitants ;
- opérateurs techniques ;
- intégrateurs ;
- prestataires ;
- partenaires institutionnels ;
- ou services tiers connectés à la plateforme.

Dans ces architectures interconnectées, plusieurs zones grises apparaissent rapidement :

- qui est responsable du traitement ?
- qui agit comme sous-traitant ?
- qui décide des finalités ?
- qui autorise les accès ?
- qui valide les usages automatisés ?
- qui assume les conséquences d'une mauvaise décision opérationnelle ?

Ces questions deviennent encore plus sensibles lorsque plusieurs organisations partagent une même plateforme ou lorsqu'un événement mobilise simultanément plusieurs services.

Une PUS ne peut donc pas fonctionner durablement sans :

- cartographie claire des responsabilités ;
- documentation des flux de données ;
- doctrine d'usage partagée ;
- conventions de gouvernance ;
- règles d'habilitation précises ;
- et traçabilité des accès, actions et décisions.

Dans les espaces ouverts au public, la sécurité juridique dépend autant de cette organisation de gouvernance que des solutions techniques elles-mêmes.

Une plateforme très intégrée mais juridiquement mal gouvernée peut rapidement créer :

- dilution des responsabilités ;
- opacité décisionnelle ;
- usages non maîtrisés ;
- ou conflits entre acteurs publics et privés.

L'hypervision impose donc un travail continu de clarification juridique et organisationnelle, et non une simple conformité documentaire au moment du déploiement. Le DPO/DPD du donneur d'ordre aura donc un rôle majeur dans la mise en place d'une PUS.

5.6. E – ÉTHIQUE

5.6.1. Proportionnalité, acceptabilité et contrôle des usages

Dans les espaces ouverts au public, l'éthique d'une PUS ne peut pas être réduite à une simple question de conformité réglementaire. Elle interroge directement la légitimité des usages, la proportionnalité des moyens déployés et les limites acceptables de l'interconnexion des données et des capacités d'action.
Une plateforme d'hypervision peut agréger :

- des flux de vidéoprotection ;
- des données de mobilité ;
- des remontées techniques ;
- des capteurs ;
- des systèmes d'alerte ;
- des données d'exploitation ;
- voire certains traitements algorithmiques.

Cette capacité de corrélation constitue précisément sa valeur opérationnelle. Mais elle crée également un risque de dépassement progressif des finalités initiales du dispositif.
Le principe de proportionnalité impose donc de partir des besoins opérationnels réels, et non des possibilités maximales offertes par la technologie. Une PUS ne doit pas être conçue pour "tout voir" ou "tout connecter", mais pour répondre à des objectifs clairement définis et limités.
Cette logique est directement cohérente avec plusieurs principes structurants du Code de la sécurité intérieure.

En particulier, l'article L251-2 du CSI rappelle que la vidéoprotection dans les espaces ouverts au public ne peut être mise en œuvre que pour des finalités limitativement énumérées :

- protection des bâtiments et installations publics ;
- régulation des flux de transport ;
- prévention des atteintes aux personnes et aux biens ;
- prévention d'actes de terrorisme ;
- secours aux personnes ;
- prévention des risques naturels ou technologiques ;
- constatation de certaines infractions ;
- ou sécurité de certains espaces particulièrement exposés.

Une PUS ne doit donc pas conduire à élargir implicitement ces finalités par simple effet de capacité technologique ou de centralisation des données.
De la même manière, l'article L252-1 du CSI encadre les conditions d'autorisation, de conservation et d'exploitation des images. Ces exigences prennent une importance particulière dans une architecture d'hypervision capable de croiser plusieurs sources d'information ou de diffuser des données à différents acteurs.

Plus la plateforme devient interconnectée et automatisée, plus les enjeux de traçabilité, d'habilitation, de journalisation et d'auditabilité deviennent centraux pour garantir la maîtrise des usages.
L'éthique d'une PUS repose également sur la maîtrise des mécanismes d'automatisation. Certaines fonctions peuvent améliorer significativement la réactivité opérationnelle :

- scénarios conditionnels ;
- remontées prioritaires ;
- contextualisation automatique ;
- pilotage coordonné d'équipements ;
- aide à la décision.

Mais ces mécanismes ne doivent pas conduire à effacer la responsabilité humaine de qualification, de décision ou d'intervention. Dans les espaces ouverts au public, la supervision humaine demeure indispensable, notamment lorsqu'une décision peut produire des conséquences sur les libertés individuelles ou les conditions d'accès à un espace.

5.6.2. Rôle du DPO/DPD (Délégué à la Protection des Données)

Le DPO/DPD joue ici un rôle structurant. Son intervention ne doit pas se limiter à une validation documentaire en fin de projet. Il doit être associé très en amont afin de :

- qualifier les traitements envisagés ;
- apprécier leur proportionnalité ;
- identifier les risques de dérive fonctionnelle ;
- définir les règles de conservation ;
- encadrer les accès ;
- participer aux analyses d'impact ;
- et contribuer à la gouvernance globale des usages.

Dans les projets les plus complexes, cette gouvernance suppose également une coopération continue entre :

- directions métiers ;
- sécurité/sûreté ;
- DSI ;
- cybersécurité ;
- exploitation ;
- directions juridiques ;
- DPO/DPD ;
- et autorités publiques concernées.

L'acceptabilité démocratique d'une PUS dépend largement de cette capacité à expliquer :

- pourquoi le dispositif existe ;
- quelles données sont utilisées ;
- quelles limites ont été fixées ;
- quels mécanismes de contrôle existent ;
- et comment les usages sont régulièrement réévalués.

La transparence ne signifie pas révéler tous les paramètres techniques ou fragiliser la sécurité du dispositif. Elle consiste à rendre compréhensible la logique générale de fonctionnement, les garanties offertes et les limites assumées.

Une PUS éthiquement maîtrisée n'est donc pas celle qui collecte le plus de données ou automatise le plus d'actions. C'est celle qui démontre que chaque capacité déployée répond à un besoin explicite, proportionné, gouverné et contrôlable dans le temps.

PARTIE 2 :
PUS EN ESPACES PRIVÉS ET SITES SENSIBLES

6. PUS EN ESPACES PRIVÉS ET SITES SENSIBLES

6.1. S – STRATÉGIE

Dans les espaces privés et les sites sensibles, une PUS ne constitue plus uniquement un outil de supervision ou de sûreté. Elle devient un élément structurant de la continuité d'activité, de la résilience opérationnelle et de la gestion des situations dégradées.
Les priorités diffèrent fortement des espaces ouverts au public. L'enjeu principal n'est plus seulement la coordination ou la gestion des flux, mais :

- la disponibilité opérationnelle ;
- la protection des actifs ;
- la continuité de production ;
- la maîtrise des accès ;
- la résilience cyber ;
- la limitation des impacts en cas d'incident.

Dans ces environnements, une panne technique, une erreur humaine ou une attaque cyber peuvent entraîner un arrêt d'exploitation, une rupture logistique, une indisponibilité industrielle, des pertes financières, des impacts réglementaires ou réputationnels, voire une mise en danger d'activités critiques.

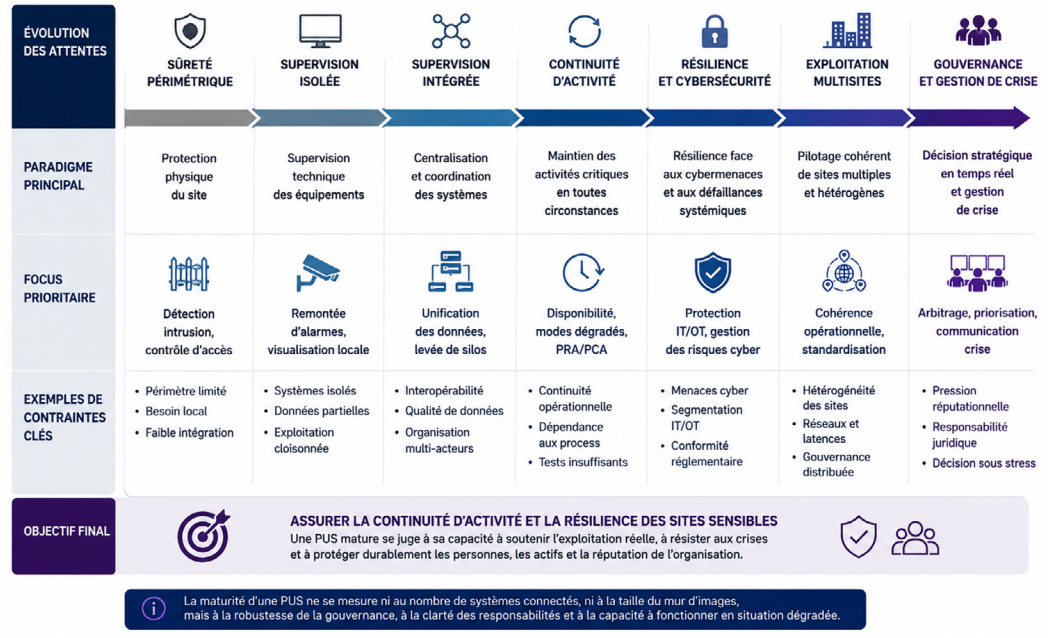
La stratégie PUS repose donc sur des arbitrages permanents entre production et sécurité, disponibilité et cybersécurité, mutualisation et perte de maîtrise, automatisation et supervision humaine, ou encore centralisation et résilience locale.

Ces arbitrages sont encore trop souvent traités tardivement. De nombreux projets restent abordés sous un angle essentiellement technologique, sans doctrine claire concernant les responsabilités, les niveaux de criticité, les modes dégradés ou les conséquences réelles d'une indisponibilité de la plateforme. Cette faiblesse de gouvernance produit fréquemment une dépendance excessive à certains intégrateurs, des plateformes difficilement maintenables, une complexité d'exploitation croissante, des scénarios obsolètes ou des architectures devenues difficiles à faire évoluer.

Dans les sites sensibles, la maturité d'une PUS ne se mesure donc ni au nombre de systèmes connectés, ni au niveau d'automatisation affiché. Elle se mesure surtout :

- à la robustesse de la gouvernance ;
- à la capacité de fonctionnement en situation dégradée ;
- à la clarté des responsabilités ;
- à la résilience opérationnelle ;
- à la capacité réelle des équipes à exploiter durablement le dispositif.

Les organisations les plus matures ne sont pas nécessairement celles qui disposent des plateformes les plus complexes, mais souvent celles qui ont défini des objectifs maîtrisés, des scénarios réellement exploitables et des chaînes de décision cohérentes avec leurs contraintes opérationnelles réelles.



Évolution des attentes liées à la PUS dans les sites sensibles

Les principaux arbitrages structurants d'une PUS peuvent être représentés de la manière suivante

Les principaux arbitrages structurants d'une PUS peuvent être représentés de la manière suivante :



L'équilibre de la PUS se construit dans la durée, par un pilotage continu et partagé

6.2. O – ORGANISATION

Dans les espaces privés et les sites sensibles, l'organisation d'une PUS devient rapidement plus complexe que dans un périmètre isolé ou monosite. Les dispositifs doivent souvent coordonner plusieurs bâtiments, plusieurs activités, plusieurs niveaux de criticité, plusieurs équipes d'exploitation et parfois plusieurs entités juridiques ou prestataires.
La difficulté ne réside donc pas uniquement dans l'intégration technique, mais dans la capacité à maintenir une gouvernance exploitable dans la durée.

Dans de nombreux projets, les responsabilités deviennent rapidement floues :

- qui pilote réellement la plateforme ?
- qui arbitre les priorités ?
- qui valide les nouveaux usages ?
- qui gère les dépendances cyber ?
- qui décide en situation dégradée ?
- qui assume l'arrêt d'un service connecté devenu critique ?

Ces ambiguïtés apparaissent fréquemment lorsque la PUS croise :

- sûreté ;
- cybersécurité ;
- exploitation industrielle ;
- maintenance ;
- production ;
- gestion technique ;
- ou direction immobilière.

Chaque métier possède ses propres contraintes, temporalités et priorités opérationnelles. Une logique de sécurité peut par exemple entrer en conflit avec les impératifs de production, les contraintes de disponibilité, les exigences de maintenance ou encore les délais d'exploitation.
Dans les environnements les plus critiques, la plateforme devient alors un espace d'arbitrage permanent entre métiers plus qu'un simple outil technique.

Cette réalité impose une gouvernance structurée dès l'amont du projet :

- maîtrise d'ouvrage clairement identifiée ;
- AMO compétente ;
- doctrine d'exploitation ;
- règles d'escalade ;
- gestion des habilitations ;
- politique de maintien en condition opérationnelle ;
- et procédures de fonctionnement en mode dégradé.

Les projets les plus fragiles sont souvent ceux où la plateforme est construite «par couches successives», au fil des demandes métiers ou des crises successives, sans gouvernance globale ni maîtrise des dépendances créées au fil du temps.

Cette dérive produit fréquemment :

- multiplication des scénarios peu utilisés ;
- accumulation d'interfaces ;
- perte de lisibilité pour les opérateurs ;
- workflows contournés ;
- dépendance excessive à certains intégrateurs ;
- ou impossibilité d'évaluer réellement les impacts d'une panne ou d'une évolution.

Dans les exploitations h24-365j/an, un autre risque apparaît progressivement : la fatigue organisationnelle.

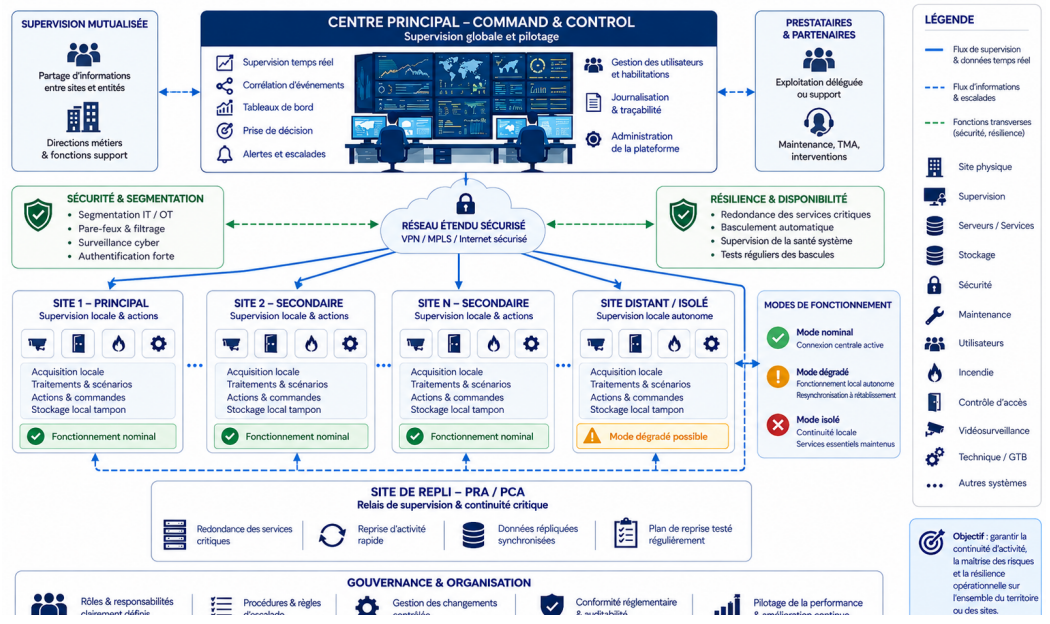
Plus la plateforme devient centrale, plus :

- les chaînes de décision se complexifient ;
- les sollicitations augmentent ;
- les opérateurs doivent traiter des flux hétérogènes ;
- et les équipes dépendent de compétences rares.

Certaines plateformes deviennent ainsi techniquement puissantes mais humainement difficiles à exploiter dans la durée.
Les organisations les plus matures cherchent donc moins à tout centraliser qu'à maintenir :

- des responsabilités lisibles ;
- des chaînes de décision courtes ;
- des scénarios réellement utilisés ;
- et des capacités locales de fonctionnement en cas de défaillance partielle.

Dans les sites sensibles, la robustesse organisationnelle devient souvent plus déterminante que la sophistication technologique elle-même.



Exemple d'architecture multisite combinant résilience locale et supervision centralisée

6.3. T – TECHNOLOGIE



Dans les espaces privés et les sites sensibles, les enjeux technologiques d'une PUS dépassent largement la simple capacité à connecter des systèmes entre eux. Les principales difficultés apparaissent rarement lors du déploiement initial, mais progressivement, au fil des évolutions, des extensions et des nouveaux usages ajoutés à la plateforme.

Avec le temps, une PUS doit continuer à fonctionner dans des environnements soumis à des contraintes fortes de disponibilité, de cybersécurité et de continuité d'activité. Elle doit pouvoir évoluer sans remettre en cause l'ensemble de l'architecture, intégrer de nouveaux équipements ou services, absorber des contraintes multisites et rester exploitable même en situation dégradée ou lors d'incidents majeurs.

Dans de nombreuses organisations, les plateformes finissent pourtant par se transformer en assemblages complexes de connecteurs, d'interfaces, de règles métiers et de systèmes historiques accumulés au fil des années. La superposition progressive des outils de cybersécurité, des fonctions de supervision technique, des équipements GTB/GTC, des systèmes de contrôle d'accès ou des dispositifs de vidéosurveillance crée alors une architecture difficile à maintenir et parfois mal comprise dans sa globalité.

Cette accumulation génère fréquemment une dette technique sous-estimée. Plus la plateforme évolue, plus certaines fragilités apparaissent : dépendances fortes à certains éditeurs, incompatibilités entre versions, scénarios devenus obsolètes, APIs modifiées sans maîtrise globale des impacts ou encore intégrations maintenues uniquement grâce à quelques compétences clés difficilement remplaçables.

Dans les environnements critiques, ces fragilités deviennent particulièrement visibles lors des mises à jour, des migrations, des changements d'intégrateur, des audits cyber, des extensions multisites ou des incidents opérationnels majeurs. Certaines organisations découvrent alors que la plateforme reste techniquement fonctionnelle, mais devient extrêmement complexe à faire évoluer, à auditer ou à restaurer rapidement en situation de crise.

La résilience technologique d'une PUS ne dépend donc pas uniquement de la robustesse initiale de l'architecture. Elle repose surtout sur sa capacité à rester maintenable, compréhensible, supervisable et gouvernable dans le temps. Une plateforme techniquement puissante mais devenue trop complexe ou insuffisamment maîtrisée finit souvent par fragiliser l'exploitation au lieu de la sécuriser.

Cette exigence impose généralement :

- des architectures segmentées ;
- des mécanismes de supervision de santé ;
- une journalisation exploitable ;
- des procédures de reprise réellement testées ;
- des politiques de gestion des versions ;
- et une maîtrise des dépendances entre composants critiques.

Dans les sites sensibles, les PRA/PCA théoriques constituent un point de faiblesse fréquent. Beaucoup de plateformes disposent de documents, de procédures, voire d'environnements de secours, sans que les mécanismes de bascule soient réellement testés dans des conditions opérationnelles réalistes.

Certaines organisations découvrent ainsi leurs dépendances critiques uniquement au moment d'un incident :

- connecteurs indispensables ;
- comptes techniques oubliés ;
- flux non documentés ;
- scénarios non transférables ;
- ou services devenus impossibles à redémarrer rapidement.

La cybersécurité complexifie encore fortement ces architectures. Les exigences de segmentation, de contrôle des accès, de supervision des flux ou de maintien des correctifs peuvent entrer en tension avec :

- les contraintes d'exploitation ;
- les impératifs de disponibilité ;
- ou les besoins temps réel de certains métiers.

Dans les environnements industriels ou multisites, cette tension devient permanente. Une politique de sécurité trop rigide peut perturber l'exploitation. À l'inverse, une logique de disponibilité absolue peut créer des vulnérabilités majeures.

Les architectures les plus matures cherchent donc généralement à limiter :

- les dépendances propriétaires ;
- les workflows non portables ;
- les couplages excessifs ;
- et les points uniques de défaillance.

Elles privilégient :

- la modularité ;
- la réversibilité ;
- l'auditabilité ;
- et la capacité de fonctionnement local en cas d'isolement partiel du système.

Enfin, la robustesse technologique d'une PUS dépend aussi fortement du facteur humain. Une plateforme techniquement performante mais :

- incomprise ;
- peu documentée ;
- difficile à maintenir ;
- ou exploitée par trop peu de compétences,

devient rapidement fragile dans la durée.

Dans les sites sensibles, la maintenabilité et la capacité d'exploitation réelle deviennent souvent plus critiques que la sophistication technologique elle-même.

6.4. A – ASPECTS FINANCIERS

6.4.1. Logiques d'investissement et d'exploitation

Pour les sites sensibles, le coût réel d'une PUS apparaît rarement lors du déploiement initial. Les principales difficultés émergent souvent plusieurs années plus tard, lorsque la plateforme devient progressivement indispensable à l'exploitation quotidienne et que chaque évolution commence à produire des impacts techniques, organisationnels et financiers de plus en plus importants.

Le sujet financier ne concerne donc pas uniquement l'investissement de départ, mais la capacité de l'organisation à maintenir durablement un niveau élevé de disponibilité, de cybersécurité et de continuité opérationnelle. Avec le temps, la plateforme doit continuer à absorber les mises à jour, les évolutions d'architecture, les PRA/PCA, les nouveaux connecteurs, les contraintes multisites et les besoins croissants en compétences spécialisées, tout en restant exploitable en continu dans des environnements h24 -365j/an.

Au fil des années, les plateformes accumulent également de nouveaux sites, de nouvelles interfaces, des exigences réglementaires supplémentaires, des couches de cybersécurité additionnelles et de nouveaux besoins métiers. Cette superposition progressive produit fréquemment une inflation des licences, une dette technique croissante, une multiplication des contrats de support, des dépendances fortes à certains éditeurs ou encore le maintien de versions historiques devenues difficiles à faire évoluer sans risque opérationnel.

Les coûts humains sont eux aussi largement sous-estimés. Une exploitation multisite permanente impose une supervision continue, des astreintes, une gestion régulière des incidents, des audits, des exercices PRA/PCA, des capacités de cybersurveillance ainsi qu'une formation constante des équipes afin de maintenir un niveau de compétence cohérent avec la complexité du dispositif.

Certaines plateformes deviennent ainsi financièrement fragiles moins à cause du coût du matériel initial que du coût réel nécessaire pour maintenir durablement la résilience, la sécurité et l'exploitabilité de l'ensemble dans le temps.

Les modèles hybrides mêlant CAPEX, SaaS, cloud ou services managés offrent davantage de souplesse budgétaire, mais créent aussi de nouvelles dépendances parfois difficiles à réverser.

Les exigences liées :

- à NIS2 ;
- aux audits cyber ;
- aux politiques de sécurité industrielle ;
- ou aux contraintes assureurs,

ajoutent désormais des coûts structurels souvent absents des évaluations initiales.

Les plateformes les plus fragiles ne sont donc pas nécessairement les moins financées, mais souvent celles dont le modèle économique ne permet plus :

- de maintenir la sécurité ;
- d'absorber l'obsolescence ;
- de conserver les compétences nécessaires ;
- ou de faire évoluer l'architecture sans rupture majeure.

6.4.2. Création de valeur mesurable

Dans les sites sensibles, la valeur d'une PUS ne se limite pas à une réduction théorique des coûts ou du nombre d'opérateurs. Les gains les plus importants concernent généralement :

- la continuité d'activité ;
- la limitation des impacts lors d'un incident ;
- la coordination multisite ;
- la rapidité de réaction ;
- la capacité à maintenir l'exploitation en situation dégradée.

La supervision distante et la mutualisation de certaines fonctions permettent parfois d'améliorer la couverture H24, d'optimiser certains PC de sécurité, de mieux répartir les ressources humaines et de réduire certaines redondances organisationnelles. L'unification des interfaces peut également réduire les besoins de formation, limiter certaines erreurs opérateurs et simplifier les procédures multisites.

Dans les environnements critiques, la valeur réelle d'une PUS apparaît surtout lorsque l'organisation doit continuer à fonctionner malgré une dégradation technique, humaine ou cyber affectant une partie du dispositif.

Mais ces gains restent fortement dépendants de la qualité réelle de l'exploitation. Une centralisation excessive ou une plateforme mal gouvernée peut produire l'effet inverse :

- surcharge cognitive ;
- multiplication des alarmes ;
- perte de maîtrise locale ;
- fatigue opérationnelle ;
- dépendances devenues trop coûteuses à maintenir.

Dans certains projets, la recherche de rationalisation aboutit paradoxalement à une augmentation durable de la complexité, des coûts de maintenance, des charges cyber et des besoins d'expertise. Une architecture pensée pour simplifier l'exploitation peut ainsi devenir, avec le temps, un facteur supplémentaire de fragilité opérationnelle.

La création de valeur d'une PUS doit donc être évaluée moins à travers un ROI immédiat qu'à travers la résilience réelle du dispositif, sa robustesse opérationnelle, la maîtrise des dépendances et sa capacité à rester exploitable dans le temps.

Une plateforme techniquement performante mais devenue trop complexe, trop coûteuse ou humainement inexploitable finit souvent par dégrader progressivement la valeur qu'elle était censée produire.

Malgré ces contraintes, les organisations qui abordent une PUS avec une gouvernance claire, une AMO compétente et une vision réaliste des enjeux d'exploitation obtiennent souvent des résultats significatifs. Une plateforme correctement structurée peut améliorer durablement :

- la continuité d'activité ;
- la coordination multisite ;
- la capacité de réaction ;
- la résilience opérationnelle ;
- et l'efficacité des équipes h24 – 365j/an ;

lorsqu'elle reste proportionnée aux besoins réels et maîtrisée dans le temps, une PUS devient moins un centre de coût qu'un véritable outil de robustesse et de performance opérationnelle.

6.5. J – JURIDIQUE

6.5.1. Responsabilité du responsable de traitement

Dans les espaces privés et les sites sensibles, le cadre juridique applicable à une PUS diffère fondamentalement de celui des espaces ouverts au public. Les dispositifs ne relèvent généralement pas du Code de la sécurité intérieure applicable à la vidéoprotection de voie publique (sauf pour les abords immédiats en périphérie du site), mais principalement :

- du RGPD ;
- du droit du travail ;
- des obligations de cybersécurité ;
- des contraintes sectorielles ;
- et des responsabilités propres à l'exploitant.

Cette différence est structurante. Elle ouvre, dans certains contextes, des possibilités fonctionnelles plus larges, y compris pour certains traitements algorithmiques avancés ou certaines formes d'analyse automatisée, dès lors que :

- les finalités sont clairement établies ;
- la proportionnalité est démontrée ;
- les personnes concernées sont correctement informées ;
- les droits applicables sont respectés ;
- et que les traitements reposent sur une base juridique valable.

Le rôle du DPO/DPD devient ici central.

Il ne constitue pas un simple valideur documentaire en fin de projet, mais l'un des acteurs structurants de la gouvernance de la plateforme.

C'est lui qui doit notamment apprécier :

- la licéité des traitements ;
- la proportionnalité des outils déployés ;
- les durées de conservation ;
- les mécanismes d'information ;
- les droits d'opposition ;
- les conditions de recours à certaines IA ;
- ou les impacts potentiels sur les libertés individuelles.

Dans les environnements privés, certains usages avancés peuvent devenir juridiquement envisageables sous conditions strictes, y compris des mécanismes d'analyse comportementale, de corrélation forte ou, dans certains cas très encadrés, des traitements biométriques ou assimilés. Ces sujets nécessitent une analyse particulièrement rigoureuse du DPO/DPD, de la direction juridique et, selon les cas, des autorités compétentes.
La difficulté ne réside donc pas uniquement dans ce que la technologie permet, mais dans la capacité de l'organisation à démontrer :

- la nécessité du dispositif ;
- sa proportionnalité ;
- son encadrement ;
- et la maîtrise réelle des usages dans le temps.

Dans les sites sensibles, les risques juridiques apparaissent souvent moins lors du déploiement initial que lors des extensions progressives :

- nouveaux usages ;
- interconnexions supplémentaires ;
- mutualisation multisites ;
- réutilisation des données ;
- ou activation de fonctionnalités initialement non prévues.

Une PUS juridiquement maîtrisée suppose donc une gouvernance continue des traitements et non une simple conformité figée au moment de la mise en service.

6.5.2. Cadre contractuel et conformité

Dans les environnements privés, les enjeux juridiques d'une PUS reposent également fortement sur les relations contractuelles entre les différents acteurs impliqués dans l'architecture et l'exploitation de la plateforme : exploitants, intégrateurs, éditeurs, hébergeurs, prestataires cyber, sociétés de maintenance ou parfois opérateurs multisites.

Dans les projets complexes, les responsabilités deviennent rapidement diffuses. Les principales zones de flou concernent notamment :

- l'hébergement ;
- la maintenance ;
- l'administration des systèmes ;
- les accès aux données ;
- le traitement des incidents ;
- la gestion des correctifs ;
- la conservation des journaux ;
- le pilotage des mécanismes d'IA ou d'automatisation.

Ces zones grises constituent une source fréquente de fragilité, notamment lors d'un incident cyber, d'une défaillance fournisseur, d'un audit, d'un changement d'intégrateur ou d'un contentieux. Les responsabilités théoriques définies au départ ne correspondent alors pas toujours aux réalités opérationnelles constatées sur le terrain.
Les contrats doivent donc encadrer précisément :

- les responsabilités ;
- les accès ;
- les niveaux de service ;
- les conditions de réversibilité ;
- les obligations de cybersécurité ;
- les mécanismes d'audit ;
- les modalités de continuité d'activité.

Dans les exploitations critiques, la conformité ne peut toutefois pas reposer uniquement sur des clauses contractuelles standardisées. Elle suppose une capacité réelle à contrôler les usages, auditer les accès, superviser les dépendances et maintenir dans le temps un niveau de sécurité cohérent avec la criticité des activités exploitées.

6.5.3. OIV, NIS2, CRA et obligations renforcées des sites sensibles

Dans les sites sensibles, les enjeux juridiques d'une PUS dépassent désormais largement le seul cadre du RGPD ou des obligations contractuelles classiques. Certaines organisations peuvent relever du statut d'OIV (Opérateur d'Importance Vitale), être considérées comme entités essentielles ou importantes au sens de NIS2, ou encore être soumises à des réglementations sectorielles spécifiques et à des exigences renforcées en matière de continuité d'activité et de cybersécurité.

Ces différents cadres imposent progressivement :

- une gouvernance cyber renforcée ;
- une gestion documentée des risques ;
- des capacités de détection et de réaction ;
- des obligations de notification d'incidents ;
- des audits réguliers ;
- une maîtrise beaucoup plus stricte des dépendances techniques et fournisseurs.

Dans ce contexte, une PUS peut devenir un composant critique de la résilience opérationnelle de l'organisation. La plateforme concentre souvent des flux temps réel, des fonctions de supervision, des capacités de commande, des mécanismes d'automatisation ainsi que des accès à des systèmes sensibles ou industriels.

Cette centralisation augmente mécaniquement les exigences :

- de segmentation ;
- de traçabilité ;
- de contrôle des accès ;
- de maintien en condition de sécurité ;
- de supervision des journaux ;
- de gestion des modes dégradés.

La plateforme ne constitue alors plus uniquement un outil d'exploitation, mais un élément structurant de la continuité opérationnelle et de la capacité globale de l'organisation à résister à des incidents techniques, cyber ou organisationnels majeurs.

NIS2 renforce particulièrement :

- les obligations de gouvernance ;
- la responsabilité des directions ;
- la gestion de la chaîne d'approvisionnement ;
- les capacités de continuité d'activité ;
- et les mécanismes de notification d'incident, avec des délais pouvant descendre à 24h pour certaines alertes.

Le Cyber Resilience Act (CRA) introduit quant à lui des exigences croissantes sur la sécurité intrinsèque des produits numériques et composants connectés intégrés dans ces architectures :

- gestion des vulnérabilités ;
- sécurité par conception ;
- mises à jour ;
- maintien en condition de sécurité ;
- et responsabilité des fabricants sur le cycle de vie des produits.

Dans certains secteurs critiques, ces obligations s'ajoutent également :

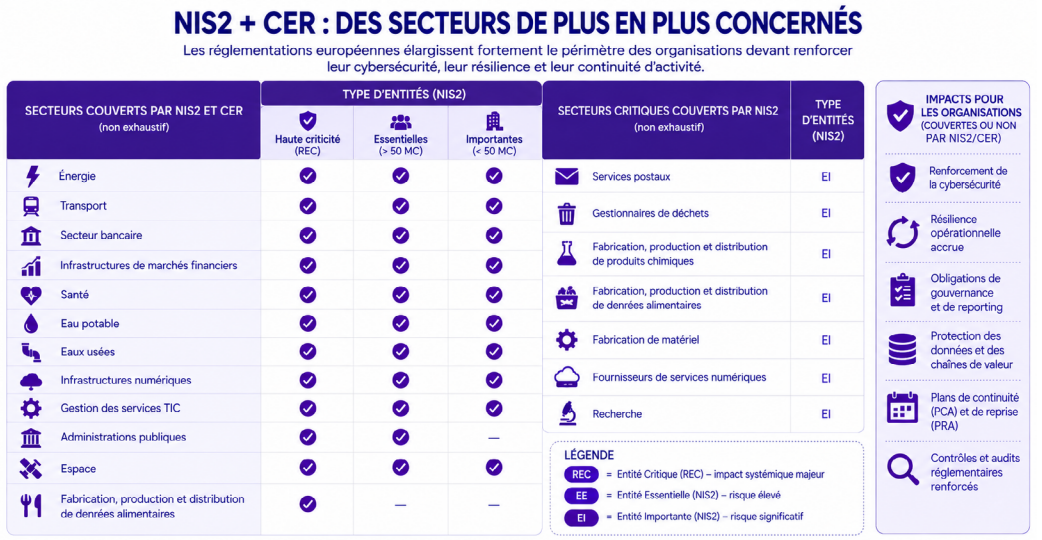
- aux contraintes OIV ;
- aux exigences de sécurité industrielle ;
- aux plans de continuité ;
- aux politiques internes de gestion de crise ;
- ou aux référentiels imposés par les assureurs et les audits clients.

Les dispositifs liés au plan Vigipirate ou aux politiques de protection des infrastructures critiques peuvent également renforcer certaines exigences de sûreté, de contrôle d'accès ou de supervision opérationnelle, notamment dans les secteurs de l'énergie, des transports, de la santé, de la logistique ou au sein de certaines infrastructures stratégiques.

Au sein des sites sensibles, la conformité juridique d'une PUS ne repose donc plus uniquement sur la légalité des traitements de données. Elle dépend désormais de la capacité globale de l'organisation à démontrer :

- sa résilience ;
- sa gouvernance ;
- sa capacité de réaction ;
- sa maîtrise des dépendances ;
- et son aptitude à maintenir durablement un niveau de sécurité cohérent avec la criticité de ses activités.

Les nouvelles réglementations européennes élargissent fortement le nombre d'organisations désormais considérées comme critiques, essentielles ou sensibles au regard des enjeux de cybersécurité et de continuité d'activité.



À RETENIR : Les exigences NIS2 et CER confirment une évolution de fond : la résilience opérationnelle, la cybersécurité et la continuité d'activité deviennent désormais **des dimensions structurantes des architectures PUS.**

SPAC ALLIANCE

6.6. E – ÉTHIQUE ET ACCEPTABILITÉ

6.6.1. Risques d'usage et dérives possibles

Dans les sites sensibles et les environnements privés, une PUS permet d'agréger de nombreuses informations et d'agir rapidement sur plusieurs systèmes ou processus opérationnels. Cette capacité constitue sa valeur, mais également sa principale zone de risque.
L'enjeu n'est pas de surveiller en permanence ou de tout analyser, mais de disposer d'outils proportionnés aux besoins réels d'exploitation, de sécurité ou de continuité d'activité.
L
es dérives apparaissent généralement lorsque :

- les usages évoluent progressivement sans gouvernance claire ;
- les fonctionnalités d'analyse sont activées sans fondement de manière permanente ;
- les données sont conservées ou réutilisées au-delà des finalités initiales ;
- ou que les capacités techniques finissent par dépasser le cadre réellement justifiable.

Exemple : généraliser des analyses vidéo avancées ou comportementales sur l'ensemble des flux disponibles, sans ciblage précis ni nécessité démontrée, peut rapidement transformer un outil opérationnel en dispositif de surveillance excessive.

Dans les environnements privés, certaines capacités techniques peuvent être juridiquement envisageables sous conditions strictes, y compris des mécanismes d'analyse avancée, voire certains traitements biométriques très encadrés. Mais la faisabilité technique ne constitue jamais, à elle seule, une justification suffisante.

Les risques d'usage apparaissent précisément lorsque :

- les finalités deviennent floues ;
- les analyses ne sont plus proportionnées ;
- les droits des personnes sont insuffisamment garantis ;
- ou que les mécanismes de contrôle deviennent purement théoriques.

Les référentiels CNIL, le RGPD et l'IA Act imposent désormais des exigences renforcées :

- proportionnalité ;
- limitation des traitements ;
- transparence ;
- auditabilité ;
- contrôle des analyses automatisées ;
- encadrement des usages à risque élevé.

Dans les sites sensibles, une dérive répétée ne constitue pas seulement un risque juridique. Elle peut rapidement devenir un risque réputationnel, un risque social, un risque contractuel, voire un facteur de perte de confiance interne.

Le DPO/DPD joue donc ici un rôle central. Il doit être intégré dès la conception du projet afin d'évaluer la légitimité des traitements, les mécanismes d'information, les conditions d'opposition, les analyses d'impact, les durées de conservation ainsi que les risques de dérive dans le temps.

Une capacité technique non gouvernée devient rapidement un risque d'usage. Et une plateforme dont les usages ne sont plus clairement maîtrisés finit souvent par fragiliser l'organisation elle-même.

6.6.2. Cadre de confiance et gouvernance

L'acceptabilité d'une PUS dans un environnement privé repose principalement sur la clarté des règles d'usage et sur la capacité de l'organisation à démontrer que les dispositifs restent maîtrisés, proportionnés et contrôlables.

Cette confiance ne dépend pas uniquement de la conformité juridique. Elle repose sur une gouvernance explicite :

- des finalités ;
- des cas d'usage autorisés ;
- des conditions d'activation ;
- des responsabilités ;
- des mécanismes de contrôle.

Dans les projets les plus matures, cette gouvernance est définie dès l'amont à travers une doctrine d'usage, des règles d'habilitation, des mécanismes de validation des fonctionnalités sensibles, des procédures d'audit, une traçabilité des actions ainsi que des dispositifs réguliers de réévaluation des usages.

L'objectif n'est pas seulement de sécuriser juridiquement la plateforme, mais d'éviter que les usages réels dérivent progressivement sous l'effet de nouvelles demandes métiers, de tensions opérationnelles, d'incidents ou de l'accumulation continue de fonctionnalités rarement remises en question dans le temps.

Une PUS doit donc être pensée comme un système gouverné et auditable dans la durée, et non comme une simple infrastructure technique. Sans cadre explicite, même une plateforme techniquement performante peut rapidement devenir contestable :

- juridiquement ;
- socialement ;
- organisationnellement.

Dans les sites sensibles, la confiance repose moins sur la sophistication technologique que sur la capacité de l'organisation à expliquer pourquoi certains outils existent, dans quelles limites ils sont utilisés, qui les contrôle et comment les usages restent durablement maîtrisés.

CONCLUSION

CONCLUSION

7. CONCLUSION

La Plateforme Unifiée Scalable ne constitue pas une évolution technologique supplémentaire dans l'écosystème de la sûreté et de la supervision. Elle marque une transformation plus profonde : celle du mode de pilotage des territoires, des infrastructures critiques et des organisations complexes.

Les équipements existent déjà. Les systèmes produisent des volumes croissants de données. Les capacités d'analyse progressent rapidement. Pourtant, dans de nombreuses organisations, la capacité réelle à comprendre une situation, à coordonner les acteurs concernés et à décider efficacement demeure insuffisante. Ce décalage ne résulte plus principalement d'un manque d'outils. Il révèle désormais une limite structurelle : fragmentation des systèmes, cloisonnement des responsabilités, multiplication des interfaces et absence de gouvernance opérationnelle cohérente.

La PUS répond précisément à cette rupture. Elle ne remplace pas les systèmes existants ; elle crée les conditions de leur cohérence opérationnelle. Son objectif n'est pas d'accumuler des technologies supplémentaires, mais de transformer des flux dispersés en capacité réelle de pilotage, de coordination et de continuité d'action.

Ce basculement est majeur. Il fait évoluer les organisations d'une logique d'équipements vers une logique de gouvernance des situations. Il transforme des dispositifs historiquement fragmentés en architectures capables de partager une compréhension commune des événements, des priorités et des décisions à prendre.

Cette évolution dépasse largement le champ technique. Elle engage directement la gouvernance des organisations, la répartition des responsabilités, les mécanismes de confiance entre acteurs publics et privés, ainsi que la capacité collective à maintenir des dispositifs exploitables dans la durée. Une PUS ne devient pertinente que si les usages sont clairement définis, les scénarios réellement maîtrisés et les chaînes de décision cohérentes avec les contraintes opérationnelles du terrain.

Les enjeux associés sont désormais stratégiques. Cybersécurité, souveraineté des données, dépendances technologiques, auditabilité des traitements, résilience opérationnelle ou conformité réglementaire ne constituent plus des sujets périphériques. Ils deviennent des conditions structurantes de la capacité des organisations à conserver la maîtrise de leurs infrastructures et de leurs décisions dans des environnements de plus en plus interconnectés et exposés.

La maturité d'une PUS ne se mesure donc ni au nombre de systèmes connectés, ni au niveau d'automatisation affiché. Elle se mesure à la capacité d'une organisation à maintenir dans le temps un équilibre entre performance opérationnelle, maîtrise des risques, gouvernance des usages et résilience des architectures déployées.

Dans les années à venir, les organisations les plus robustes ne seront pas nécessairement celles disposant des plateformes les plus complexes. Ce seront celles capables de conserver une maîtrise claire de leurs flux d'information, de leurs mécanismes de décision et de leurs dépendances techniques dans des contextes de plus en plus instables et exigeants.

La PUS ne constitue donc pas une finalité technologique. Elle devient un levier structurant de transformation opérationnelle, permettant de mieux observer, mieux comprendre, mieux décider, mieux agir et mieux capitaliser sur les événements rencontrés.
La véritable valeur d'une PUS réside dans la continuité opérationnelle qu'elle parvient à instaurer entre ces différentes dimensions.

Un flux continu au service de la décision et de l'amélioration

Une PUS connecte les systèmes, les intelligences (IA) et les humains pour transformer un événement en action coordonnée, traçable et exploitable dans le temps.

BOUCLE D'AMÉLIORATION CONTINUE

1 DÉTECTION	2 QUALIFICATION	3 CORRÉLATION	4 DÉCISION	5 ACTION	6 TRAÇABILITÉ	7 RETEX
Événement ou signal détecté par un capteur ou un système.	Analyse et qualification initiale de l'événement (filtrage, priorité, confiance).	Croisement multi-sources et contextualisation pour établir une situation fiable.	Aide à la décision pour l'opérateur ou décision automatisée selon les règles et scénarios.	Déclenchement des actions et procédures via l'orchestrateur opérationnelle.	Enregistrement horodaté des décisions, actions et échanges pour audit et conformité.	Analyse a posteriori des événements pour améliorer règles, modèles et procédures.

SYSTÈMES Capteurs, logiciels, applications métiers	Collecte des données en temps réel.	Normalisation, filtrage, enrichissement.	Agrégation, corrélation temps réel, moteur d'événements.	Moteurs de règles, scénarios, IA explicable.	Envoi d'ordres, automatisations, workflows.	Logs, journaux systèmes, chaîne d'intégrité.	Historisation, indicateurs, tableaux de bord, rapports.
IA & ANALYTIQUE Algorithmes, modèles, moteurs d'analyse	IA de détection (anomalies, objets, comportements).	IA de classification et scoring de pertinence.	IA de corrélation multi-sources et contextualisation.	IA d'aide à la décision (prévision, recommandation, priorisation).	IA d'optimisation et d'orchestration des réponses.	IA d'audit (cohérence, anomalies, conformité).	IA d'apprentissage (ajustement des modèles et des scénarios).
HUMAINS Opérateurs, experts, équipes terrain	Agents terrain, opérateurs systèmes.	Opérateur en salle, vérification et qualification.	Analystes, experts métier, validation du contexte.	Décideur / superviseur, arbitrage et validation humaine.	Opérateurs terrain, équipes d'intervention, services concernés.	Responsable conformité, auditeur, contrôleur.	Équipes métier, REX, amélioration des procédures.
ORCHESTRATION PUS	Collecte unifiée et supervision des sources.	Routage intelligent, priorisation des flux et alertes.	Moteur d'événements et bus de données temps réel.	Centre de décision unifié et gestion des scénarios.	Orchestrateur d'actions et intégration multi-systèmes.	Archivage sécurisé et traçabilité de bout en bout.	Boucle d'amélioration continue et capitalisation des connaissances.

PRINCIPES TRANSVERSES — Sécurité & cybersécurité par conception · Proportionnalité et éthique · Résilience & continuité opérationnelle · Souveraineté et maîtrise des données · Conformité réglementaire et responsabilité

Une PUS n'est pas une fin en soi, c'est un levier de performance durable au service de la sécurité, de la sûreté et de l'intérêt général.
Observer – Comprendre – Décider – Agir – Apprendre : tel est le cycle vertueux d'une PUS mature et responsable.

ANNEXES

ANNEXES

8. ANNEXES

8.1 LEXIQUE

Par ordre alphabétique, quelques acronymes utiles !

Acronyme → Définition
ACAP : Axis Camera Application Platform
AIPD : Analyse d'Impact relative à la Protection des Données
AIM : Identity and Access Management / Gestion des identités et des accès
ALPR : Automatic License Plate Recognition
AMO : Assistance à Maîtrise d'Ouvrage
AMQP : Advanced Message Queuing Protocol
AN2V : Association Nationale de la Vidéoprotection
ANPR : Automatic Number Plate Recognition
API : Application Programming Interface / Interface de programmation applicative
ABAC : Attribute Based Access Control
CAPEX : Dépenses d'investissement
CER : Critical Entities Resilience Directive
CNAPS : Conseil National des Activités Privées de Sécurité
CNIL : Commission Nationale de l'Informatique et des Libertés
CNPP : Centre National de Prévention et de Protection
CRA : Cyber Resilience Act
CSI : Code de la Sécurité Intérieure
CSD : Centre de Supervision Départemental
CSM : Centre de Supervision Mutualisé
CSU : Centre de Supervision Urbain
CSUi : Centre de Supervision Urbain Intercommunal
CSF-IS : Contrat Stratégique de Filière des Industries de Sécurité
DGS : Directeur Général des Services
DORI : Détection / Observation / Reconnaissance / Identification
DPD : Délégué à la Protection des Données
DPO : Data Protection Officer
GN : Gendarmerie Nationale
GNSS : Global Navigation Satellite System
GPS : Global Positioning System
GTB : Gestion Technique du Bâtiment
GTC : Gestion Technique Centralisée
GTI : Garantie de Temps d'Intervention
GTR : Garantie de Temps de Rétablissement
IA : Intelligence Artificielle
IA Act : Règlement européen sur l'Intelligence Artificielle
IAM : Identity and Access Management
IF/THEN : Logique conditionnelle de scénarios automatisés
IHM : Interface Homme-Machine
IoT : Internet of Things / Internet des Objets
IT : Information Technology / Technologies de l'information
K afka : Plateforme distribuée de gestion de flux et de messages temps réel
KPI : Key Performance Indicator / Indicateur clé de performance
LAN : Local Area Network
LAPI : Lecture Automatisée de Plaques d'Immatriculation
LPR : License Plate Recognition
MCI : Main Courante Informatisée
MCO : Maintien en Condition Opérationnelle
MCS : Maintien en Condition de Sécurité
MQTT : Message Queuing Telemetry Transport
NIS2 : Network and Information Security Directive 2
NTP : Network Time Protocol
OCR : Optical Character Recognition
OIV : Opérateur d'Importance Vitale
ONVIF : Open Network Video Interface Forum
OPEX : Dépenses opérationnelles
OT : Operational Technology / Technologies opérationnelles
PCA : Plan de Continuité d'Activité
POC : Proof of Concept
PRA : Plan de Reprise d'Activité
PPMS : Plan Particulier de Mise en Sûreté
PSIM : Physical Security Information Management
PTI : Protection du Travailleur Isolé
PTP : Precision Time Protocol
PTZ : Pan Tilt Zoom
PUS : Plateforme Unifiée Scalable
QoS : Quality of Service
R2A : Remontée Automatique d'Alerte
RBAC : Role Based Access Control
REST : Representational State Transfer
RGPD : Règlement Général sur la Protection des Données
REX : Retour d'Expérience
RSSI : Responsable de la Sécurité des Systèmes d'Information
SaaS : Software as a Service
SDK : Software Development Kit
SDIS : Service Départemental d'Incendie et de Secours
SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale
SI : Système d'Information
SIEMSecurity Information and Event Management
SIG : Système d'Information Géographique
SOAService-Oriented Architecture / Architecture Orientée Services
SOC : Security Operations Center
SOTAJE : Stratégie / Organisation / Technologie / Aspects financiers / Juridique / Éthique
SNR : Stratégie Nationale de Résilience
SOARSecurity Orchestration, Automation and Response
SSOS : ingle Sign-On
TMS : Troubles Musculo-Squelettiques
UTC : Coordinated Universal Time / Temps Universel Coordonné
VMS : Video Management System
VSaaS : Video Surveillance as a Service
VSA : Video Surveillance Augmentée
WAN : Wide Area Network
WDR : Wide Dynamic Range

8.2 RETOUR D'EXPERIENCE STRUCTURANT

HEURE	ACTIONS OPÉRATEUR	FONCTIONS HYPERVISEUR
22:00	• L'opérateur est à son poste d'hypervision. • Les agents d'astreinte sont à leur domicile ou en patrouille.	**L'HYPERVISEUR** donne à l'opérateur des indications globales de l'état général du site hypervisé (carrés verts par sous-système en haut de l'interface, tout va bien). En l'absence d'événement l'HYPERVISEUR exécute des rondes de surveillance générale avec la vidéo protection par exemple.
22:01	• Un appel d'urgence arrive sur le combiné téléphonique du poste d'hypervision. • L'interlocuteur indique l'adresse où vient de se produire un accident de voiture. • L'opérateur saisit l'adresse sur son interface pour localiser l'endroit sur la cartographie de son poste.	L'HYPERVISEUR gère de façon unifiée, sur un seul combiné, toutes les communications audios numérisées provenant des réseaux de téléphonie, des réseaux radio (TETRA), systèmes d'interphonie, etc.
22:02		L'HYPERVISEUR centre automatiquement le plan sur l'adresse saisie. Il localise l'événement sur la carte. Cela est possible grâce à la base de données des adresses postales associées au SIG.
22:02	En cliquant sur le plan, l'opérateur visualise automatiquement les images du lieu de l'accident (une ou plusieurs caméras couvrent la zone).	L'HYPERVISEUR utilise le superviseur vidéo pour sélectionner automatiquement la meilleure caméra vidéo, permettant une visualisation optimale de la zone. L'HYPERVISEUR la pilote automatiquement en site, azimut et zoom pour cadrer précisément le lieu de l'accident.
22:03	• L'opérateur demande à l'HYPERVISEUR d'afficher la géolocalisation des équipes d'intervention disponibles à proximité en cochant les calques des groupes désirés. • L'opérateur visualise sur la carte le véhicule d'intervention le plus proche et le contacte depuis son combiné audio, via le réseau TETRA par exemple. • Il communique à la patrouille, des informations précises : heure de l'accident, lieu géographique, et contexte de ce qu'il a visualisé et il demande l'intervention.	Les positions des intervenants sont connues grâce à des terminaux équipés de GPS transmettant leurs positions via un réseau TETRA, PMR ou 3G. L'HYPERVISEUR gère depuis son combiné audio universel différents types de terminaux audio radio.
22:08	L'opérateur passe les feux tricolores du parcours au vert pour faciliter la progression du véhicule d'intervention.	L'HYPERVISEUR visualise sur le plan les feux tricolores par l'intermédiaire du superviseur des feux de circulation et permet leur télécommande ponctuelle.
22:15	• La ville est une ville éco citoyenne. Elle est équipée d'un système d'éclairage modulable en puissance. • L'opérateur augmente l'éclairage de la rue de l'accident afin de faciliter les interventions.	L'HYPERVISEUR permet de commander les systèmes d'éclairage par l'intermédiaire du superviseur de l'éclairage public.
22:17	L'opérateur signale les perturbations sur les panneaux lumineux d'information.	L'HYPERVISEUR permet de transmettre des données à des panneaux de messages variables (PMV).
	L'opérateur complète si nécessaire la main courante : Chrono / Opérateur / Action 22:01 Jean Fera Réception Appel extérieur 22:03 Jean Fera Appel véhicule 024 22:08 Jean Fera Feu 003 commandé vert 22:15 Jean Fera Eclairage puissance 22:17 Jean Fera PMV 035 «Attention accident»	L'HYPERVISEUR enregistre au fil de l'eau les actions réalisées dans une main courante. L'HYPERVISEUR peut fournir les informations de données et d'images de façon sécurisée pour enquête.

HYPERVISION

PLATEFORME UNIFIÉE

Les outils existent. Les données aussi. Mais leur dispersion freine encore la compréhension des situations, la coordination des acteurs et la rapidité de décision. Dans les territoires comme dans les sites sensibles, la fragmentation des systèmes,plus que le manque d'équipements, est devenue la véritable limite des dispositifs de sécurité et de supervision



Porté par le Groupe de Travail PUS de l'AN2V, ce livre blanc propose une **doctrine de cadrage** pour comprendre, concevoir et gouverner l**es Plateformes Unifiées Scalable**. Ni catalogue de solutions, ni comparatif d'éditeurs, ni modèle unique, il s'adresse aux décideurs publics et privés, aux directions opérationnelles et aux experts techniques, avec une lecture à trois niveaux pour s'adapter à chaque profil.

À travers la **méthode SOTAJE** (Stratégie, Organisation, Technologie, Aspects financiers, Juridique, Éthique), déclinée pour **les espaces ouverts au public comme pour les sites sensibles**, le document éclaire les invariants fondateurs d'une PUS : interopérabilité, résilience, souveraineté des données, gouvernance des accès, conformité réglementaire (RGPD, NIS2, CRA, IA Act).

Sa thèse centrale : la PUS n'est **pas une accumulation technologique** supplémentaire, mais un levier de transformation du pilotage, celui qui fait passer les organisations d'une logique d'équipements à une logique de gouvernance des situations. Sa maturité ne se mesure ni au nombre de systèmes connectés ni au niveau d'automatisation, mais à la capacité durable de maintenir l'équilibre entre performance, maîtrise des risques et résilience.

AN2V