

Adoption d'une technologie d'identification et de localisation des prisonniers en contexte post-conflit à l'issue d'une analyse comparative des technologies : le cas de la ville de Bukavu

Adoption of a prisoner identification and location technology in a post-conflict context following a comparative analysis of technologies: the case of the city of Bukavu

ASIFIWE KARHUNZI Steve, ISC BUKAVU / HEC-KIN. sbashushana@gmail.com

Bahanaga Nyindji Asaf, ISP/KAZIBA. bnyindji@gmail.com

Rusagara Babone, ISP/KAZIBA. rusagarababone1@gmail.com

Sakina Namuciro Sandra, ISC/Bukavu. sakinasandra27@gmail.com

Résumé

Dans les contextes post-conflit, la gestion carcérale est un enjeu majeur de sécurité publique et d'État de droit. Cette étude vise à adopter une technologie d'identification et de localisation des prisonniers à Bukavu (RDC) à la suite d'une analyse comparative. La méthodologie confronte les résultats d'une enquête menée auprès de 105 répondants (ingénieurs, agents pénitentiaires, société civile, citoyens) avec la recherche secondaire et les caractéristiques techniques documentées. Les résultats montrent une distinction fonctionnelle nette : la biométrie est préférée pour l'enregistrement (58 %, les empreintes digitales étant jugées les plus fiables à 68 %), tandis que la RFID est plébiscitée pour la localisation intra-muros (48 %) et le GPS pour le suivi externe (42 %). L'étude propose une architecture hybride évolutive : phase 1 avec biométrie et RFID passive, phase 2 ajoutant le GPS pour les sorties/évasions, et phase 3 intégrant caméras intelligentes et capteurs acoustiques. Le système intègre une résilience énergétique (solaire, batterie 72h), un fonctionnement hors ligne avec synchronisation différée, et un repli satellitaire pour les alertes critiques. La gouvernance respecte la loi congolaise n° 15/026, avec destruction des gabarits 6 mois après la libération et un comité de suivi participatif. Un budget prévisionnel est proposé (CAPEX 23 200 USD, OPEX annuel 3 200 USD) pour un pilote de 100 prisonniers.

Mots-clés : adoption ; analyse comparative ; contexte post-conflit ; biométrie ; RFID ; GPS ; systèmes RTLS ; systèmes d'information carcéraux ; gouvernance des données.

Classification JEL: K14, K42, O33, H56

Abstract

In post-conflict contexts, prison management is a major public security and rule-of-law issue. This study aims to adopt a prisoner identification and location technology in Bukavu (DRC) following a comparative analysis. The methodology confronts survey results from 105 respondents (engineers, prison staff, civil society, citizens) with secondary research and documented technical characteristics. Results show a clear functional distinction: biometrics is preferred for registration (58%, with fingerprints rated most reliable at 68%), while RFID is favored for intra-muros location (48%) and GPS for external tracking (42%). The study proposes an evolutionary hybrid architecture: Phase 1 with biometrics and passive RFID, Phase 2 adding GPS for external movements/escapes, and Phase 3 integrating intelligent cameras and acoustic sensors. The system ensures energy resilience (solar, 72h battery), offline operation with deferred synchronization, and satellite backup for critical alerts. Governance complies with Congolese law n° 15/026, with biometric template destruction 6 months after release and a participatory monitoring committee. A preliminary budget is provided (CAPEX \$23,200, annual OPEX \$3,200) for a 100-prisoner pilot.

Keywords: adoption; comparative analysis; post-conflict context; biometrics; RFID; GPS; RTLS systems; prison information systems; data governance.

JEL Classification: K14, K42, O33, H56

I. INTRODUCTION

I.1. Contexte général

Les périodes post-conflit se caractérisent par une fragilité institutionnelle, une désorganisation sociale et une insécurité persistante. En République Démocratique du Congo (RDC), la région du Sud-Kivu, et particulièrement la ville de Bukavu, illustre ce type de contexte : la fin des hostilités ouvertes ne signifie pas nécessairement un retour à l'ordre ni à la stabilité. Nous observons les évasions dans quelques prisons du Sud-Kivu et même des cas de disparition, une situation qui crée des problèmes pour la population – les membres de famille des prisonniers se posent plusieurs questions après la disparition de leurs proches – et qui dévalorise l'État de droit de notre pays. Le 14 février 2025, suite à la guerre du M23 et à l'action de l'armée congolaise, des prisonniers se sont évadés de la prison centrale de Bukavu. En représailles, la population de Bukavu s'est trouvée dans une situation défavorable : plusieurs vols avec arme à feu ont été enregistrés, de nombreux biens ont été volés.

La question de la localisation et de l'identification des prisonniers est un sujet majeur. De nombreuses familles s'interrogent sur le sort de leurs proches incarcérés dont les registres ont été détruits ou perdus. Face à cette perte d'information, la possibilité de reconstituer une base de données fiable et de recourir à des solutions technologiques adaptées apparaît essentielle. L'identification et la localisation des prisonniers sont indispensables dans la ville de Bukavu, pour permettre de retrouver les criminels après une situation de crise, et aussi pour sauvegarder les informations dans une base de données bien sécurisée, car tous les documents et papiers ont été détruits, et le matériel a été pillé par la population. Ainsi, les technologies existantes dans d'autres pays pour l'identification et la localisation des prisonniers peuvent nous être utiles pour l'analyse, afin de faire la comparaison et de voir la technologie qui peut être adoptée et implémentée dans la ville de Bukavu.

I.2. Problématique

Le problème principal n'est donc pas seulement de chercher une technologie « meilleure » entre biométrie, RFID et GPS. Il est de savoir quelle technologie répond le mieux à chaque fonction du système pénitentiaire et comment les combiner dans un contexte où l'électricité est instable, la connectivité limitée, la capacité de maintenance faible et les risques de vol ou de sabotage élevés. L'enquête de terrain donne ici une information nouvelle : la population, y compris les ingénieurs et les agents pénitentiaires inclus dans l'échantillon, distingue elle-même les usages. La biométrie seule reçoit 58 % pour l'identification, la RFID 48 % pour la localisation intra-muros, le GPS 42 % pour la localisation externe, tandis que 72 % se déclarent favorables à une solution hybride (enquête de terrain à Bukavu, 2025). Ces perceptions sont croisées avec les études secondaires locales qui ont spécifiquement consulté des juges, des directeurs de prison et des gardiens, confirmant la distinction fonctionnelle.

La question principale devient ainsi : **quelle architecture technologique permet de faire une identification fiable du prisonnier, une localisation adaptée à l'espace considéré et une traçabilité sécurisée, tout en restant compatible avec les contraintes de Bukavu ?**

I.3. Questions spécifiques

1. Quelle technologie permet le mieux d'enregistrer et de vérifier l'identité d'un prisonnier dans une base de données judiciaire et biométrique ?
2. Quelle technologie est la plus appropriée pour localiser un prisonnier à l'intérieur de la prison ?

3. Quelle technologie complète la localisation lorsqu'un prisonnier quitte la zone pénitentiaire ?
4. Quels capteurs complémentaires peuvent renforcer la détection des événements anormaux sans être confondus avec la fonction d'identification ou de localisation ?
5. Quelles conditions de sécurité, d'énergie, de maintenance et de gouvernance sont nécessaires pour rendre le système durable à Bukavu ?

I.4. Hypothèses de recherche

Hypothèse principale : L'adoption durable d'une technologie d'identification et de localisation des prisonniers à Bukavu dépend de la combinaison entre adéquation fonctionnelle, contraintes techniques, capacités organisationnelles, coûts et gouvernance des données.

- **HS1 :** La biométrie est plus adaptée que la RFID et le GPS pour l'identification et l'enregistrement d'un prisonnier dans un système de gestion de base de données.
- **HS2 :** La RFID est plus adaptée à la localisation intra-muros par zones équipées de lecteurs, tandis que le GPS est plus adapté au suivi externe.
- **HS3 :** Une architecture hybride intégrant biométrie, RFID, GPS et capteurs complémentaires est plus cohérente avec les besoins de sécurité que l'utilisation d'une seule technologie, mais doit être déployée de manière évolutive pour éviter une complexité excessive.
- **HS4 :** Le fonctionnement hors ligne (avec synchronisation différée), l'énergie solaire de secours, la cybersécurité et la gouvernance des données sont des conditions nécessaires à l'adoption du système dans le contexte de Bukavu.

I.5. Objectifs de la recherche

L'objectif général est de proposer une architecture technologique d'identification, de localisation et de traçabilité des prisonniers à Bukavu après confrontation des résultats de l'enquête de terrain avec la recherche secondaire et les caractéristiques techniques des technologies.

- Comparer les résultats de l'enquête aux connaissances techniques et empiriques disponibles, en incluant les études locales antérieures ayant consulté les acteurs pénitentiaires ;
- Séparer les technologies selon les fonctions d'identification, de localisation et de surveillance ;
- Construire un modèle de système d'information pour l'identification ;
- Construire un modèle de système d'information pour la localisation et la traçabilité, en privilégiant une approche évolutive (phase 1 : biométrie + RFID passive ; phase 2 : GPS externe ; phase 3 : capteurs intelligents) ;
- Préciser les mécanismes de sécurité, de fonctionnement hors ligne et de protection des données, en intégrant les exigences légales congolaises.

II. REVUE DE LA LITTÉRATURE

La revue de la littérature est divisée en deux parties. La première présente les éléments théoriques qui expliquent l'adoption et l'intégration des technologies. La deuxième confronte les résultats de recherches antérieures (incluant les études locales menées à Bukavu) et les caractéristiques techniques documentées afin de préparer la comparaison avec l'enquête.

II.1. Revue théorique

La théorie des systèmes d'information considère que la valeur d'une technologie dépend de l'interaction entre les données, les personnes, les procédures et les ressources techniques. Dans le domaine carcéral, une technologie isolée ne suffit donc pas. Il faut un système d'information capable de collecter, traiter, stocker, sécuriser et restituer l'information utile aux responsables. Cette logique rejoint l'approche de Laudon et Laudon (2020).

La théorie de l'acceptation technologique (TAM) de Davis (1989) rappelle que l'utilité perçue et la facilité d'utilisation influencent l'acceptation d'un système. Dans le cas de Bukavu, le fait que 86 % des répondants pensent qu'un système technologique améliorerait la sécurité et que 72 % approuvent l'approche hybride montre une utilité perçue élevée. En revanche, le coût et les contraintes d'infrastructure réduisent la faisabilité perçue.

Le modèle TOE (Technology–Organization–Environment) de Tornatzky et Fleischer (1990) est également utile. La dimension technologique correspond ici à la précision, la portée, l'autonomie et la robustesse. La dimension organisationnelle concerne la formation, la maintenance, la gouvernance et la capacité de gestion. La dimension environnementale comprend la sécurité, les infrastructures, le contexte post-conflit et les contraintes institutionnelles. Dans la présente étude, les pondérations des dimensions sont justifiées par les travaux antérieurs menés à Bukavu (mémoires UCB, ISTEIGI, ISP Bukavu ; projets MONUSCO et CICR) qui ont identifié ces quatre dimensions comme critiques pour la faisabilité des projets technologiques en milieu carcéral congolais.

Enfin, la conception du système est rapprochée d'une logique de *Design Science Research* : la recherche ne s'arrête pas au constat ; elle produit un artefact conceptuel. Dans cet article, l'artefact est constitué de deux modèles complémentaires, l'un consacré à l'identification et l'autre à la localisation/traçabilité.

II.1.1. Concepts techniques

Tableau 1 : Distinction entre identification, localisation, traçabilité et surveillance

Concept	Définition opérationnelle	Technologies principales
Identification	Déterminer l'identité d'une personne à partir d'un identifiant ou de caractéristiques biométriques.	Biométrie
Vérification	Comparer une donnée présentée à une identité déclarée (1:1).	Empreinte, visage, voix
Identification biométrique	Rechercher une personne parmi plusieurs références (1: N).	Empreinte, visage
Localisation	Déterminer la zone ou la position courante d'une personne.	RFID, GPS, RTLS
Traçabilité	Conserver et reconstituer les événements de déplacement et de passage.	Base historique + événements
Surveillance	Observer ou détecter un événement anormal.	Caméras, son, alarmes, capteurs

Un lecteur RFID qui détecte un bracelet dans une zone fournit une information de présence ou de passage dans cette zone. Une caméra peut contribuer à reconnaître un visage, mais elle ne remplace pas la base biométrique d'enrôlement. Un GPS permet de calculer une position à l'extérieur, mais la transmission de cette position vers un serveur peut dépendre du réseau utilisé par le terminal.

II.2. Revue empirique

La littérature technique confirme l'intérêt de la biométrie pour l'identification. Le NIST distingue notamment la vérification 1:1 et l'identification 1: N et évalue de manière indépendante les technologies faciales, les empreintes et les autres modalités biométriques. Le NIST rappelle aussi que la qualité de l'échantillon acquis influence directement la performance du système biométrique (NIST, 2025).

Pour la reconnaissance faciale, les évaluations NIST montrent qu'il existe des différences de performance selon les algorithmes, les caractéristiques des images et les conditions d'acquisition. Cela justifie, dans notre modèle, de ne pas faire de la caméra seule la source officielle d'identification du

prisonnier. La caméra est un mécanisme de vérification et de surveillance complémentaire ; la référence maîtresse reste la fiche biométrique créée au moment de l'enregistrement (NIST FRTE, 2026).

Pour la RFID, les fiches techniques et les travaux expérimentaux montrent une différence importante entre les tags passifs et actifs. Le tag passif n'embarque pas de batterie et récupère son énergie dans le champ du lecteur ; la portée est donc liée au type de technologie et à la proximité du lecteur. Les systèmes RFID actifs peuvent, eux, émettre périodiquement et être utilisés dans des systèmes de localisation temps réel (EUIPO, s. d.).

Les recherches sur le RTLS montrent aussi que la localisation RFID intra-muros est un problème d'environnement radio : précision, disposition des lecteurs, atténuation et caractéristiques des locaux influencent les résultats. Des expérimentations sur des systèmes RFID actifs ont montré la faisabilité de la localisation indoor et la nécessité de caractériser l'erreur de position (Lam et al., 2016).

Pour le GPS, il faut corriger une confusion présente dans la première version. Le récepteur GPS calcule sa position à partir des signaux des satellites ; il n'a pas besoin d'Internet pour faire ce calcul. En revanche, le système de suivi pénitentiaire a besoin d'un moyen de communication pour envoyer la position au serveur central. Le problème de Bukavu concerne donc surtout la transmission, la couverture mobile, l'autonomie électrique du terminal et la continuité de service (GPS.gov, 2026).GPS.gov

Les travaux sur la localisation indoor recommandent régulièrement une approche hybride lorsque plusieurs contraintes existent. Une revue empirique des technologies indoor met en avant la précision, le coût, la robustesse, l'efficacité énergétique et la fiabilité comme critères de comparaison, et montre que l'hybridation peut améliorer la robustesse globale.

Sur la protection des données, ISO/IEC 24745:2022 traite explicitement de la confidentialité, de l'intégrité, de la protection des références biométriques et de la liaison sécurisée entre une référence biométrique et une identité. Le NIST insiste également sur la minimisation des données et la limitation de l'utilisation à des finalités définies (ISO/IEC 24745:2022).

Études locales antérieures : Des mémoires et rapports menés à Bukavu ont déjà abordé des aspects connexes :

- Un mémoire d'architecture à l'UCB a étudié la conception d'une infrastructure pénitentiaire moderne intégrant vidéosurveillance et gestion numérique des accès.
- Un mémoire en informatique de gestion à l'ISTEGI/ISP Bukavu a proposé une base de données relationnelle pour la gestion du registre d'écrou et le suivi judiciaire des détenus à la Prison Centrale de Bukavu ».
- Des projets MONUSCO et CICR ont déjà fourni du matériel informatique et réalisé des audits énergétiques à la prison centrale.

Ces travaux, qui ont consulté des juges, directeurs de prison et gardiens, confirment la pertinence des dimensions technique, économique, organisationnelle et éthique/sociale.

Tableau 2 : Synthèse de la recherche secondaire et des implications techniques

Technologie / source	Résultat de la recherche secondaire	Fonction retenue	Précaution
Biométrie	NIST : évaluation 1:1 et 1: N ; qualité des échantillons déterminante	Très adaptée à l'enrôlement et à la vérification	Prévoir qualité capteurs, contrôle d'accès et protection des gabarits
RFID passive	Tag sans batterie ; faible puissance ; détection dans une zone de lecture	Très adaptée au suivi par zones intra-muros	Ne pas présenter seule comme une géolocalisation continue

RFID active / RTLS	Émission autonome ; possibilité de calcul de position via lecteurs/algorithmes	Adaptée lorsque le suivi indoor fin est requis	Coût et autonomie batterie plus élevés
GPS/GNSS	Position calculée depuis les signaux satellites	Très adapté au suivi externe	Le terminal doit transmettre la position au serveur par un réseau disponible
Caméras intelligentes	Analyse d'images et reconnaissance faciale	Complément de surveillance et de vérification	Gestion de faux positifs, éclairage, confidentialité
Capteurs son / empreinte	Détection d'événements ou contrôle d'accès	Complément de sécurité	Ne pas confondre capteur de sécurité et localisation

III. MÉTHODOLOGIE

III.1. Cadre méthodologique

L'étude adopte une approche descriptive et analytique associant trois sources : (1) l'enquête de terrain à Bukavu (incluant des ingénieurs, des agents pénitentiaires, des membres de la société civile et des citoyens), (2) la recherche secondaire (incluant les études locales antérieures ayant consulté des professionnels pénitentiaires) et (3) les fiches techniques des technologies. La logique de confrontation est la suivante : les résultats de terrain indiquent ce que les acteurs perçoivent comme utile et acceptable ; la recherche secondaire vérifie ce que les technologies peuvent effectivement faire ; la synthèse fonctionnelle détermine la place de chaque technologie dans l'architecture.

III.2. Enquête de terrain – échantillon et profils

L'enquête a été réalisée du 07 octobre 2024 au 06 octobre 2025 dans les communes d'Ibanda, Kadutu et Bagira. 110 questionnaires ont été administrés en face-à-face et 105 ont été jugés exploitables, soit un taux de réponse de 95,5 %. La ventilation détaillée des profils est la suivante :

- **Ingénieurs / techniciens** : 15 (14,3 %) ;
- **Agents pénitentiaires** (gardiens, greffiers, responsables de sécurité) : 25 (23,8 %) ;
- **Membres de la société civile / ONG locales** : 20 (19,0 %) ;
- **Citoyens résidant à proximité des prisons** : 45 (42,9 %).

Cette diversité permet de croiser les perceptions avec une certaine expertise technique. Une analyse par sous-groupe a été réalisée : les préférences des ingénieurs et agents pénitentiaires pour la biométrie (identification) et la RFID (localisation) sont encore plus marquées que celles des citoyens (respectivement +12 % et +9 %), ce qui renforce la validité des choix fonctionnels.

Tableau 3 : Répartition de l'échantillon exploitable par commune

Commune	Questionnaires administrés	Exploitable s	Part de l'échantillon exploitable
Ibanda	42	40	38,1 %
Kadutu	38	36	34,3 %
Bagira	30	29	27,6 %
Total	110	105	100 %

III.3. Méthode de scoring multicritère – justification et sous-scores

Chaque indicateur est orienté positivement : un score élevé signifie une meilleure adéquation. L'échelle est : 1 = très faible ; 2 = faible ; 3 = moyenne ; 4 = élevée ; 5 = très élevée. Les quatre dimensions sont : technique, économique, organisationnelle et éthique/sociale. Les pondérations sont

justifiées par la recherche secondaire et les études locales antérieures (mémoires UCB, ISTEGL, ISP Bukavu ; projets MONUSCO et CICR) qui ont identifié ces dimensions comme critiques dans le contexte carcéral congolais. Chaque dimension reçoit un poids égal de 25 % dans le scénario de base, conformément à l'approche équilibrée recommandée par les travaux de Tornatzky et Fleischer (1990) appliqués aux projets de SI en contextes fragiles.

Le score global est calculé par : **Score global = Σ (poids de la dimension $\times$ score moyen de la dimension)**. Les scores documentaires restent des scores d'analyse construits par les auteurs ; ils ne sont pas présentés comme des mesures expérimentales réalisées dans une prison de Bukavu.

Tableau 4 : Règle de construction des scores et sous-scores obtenus

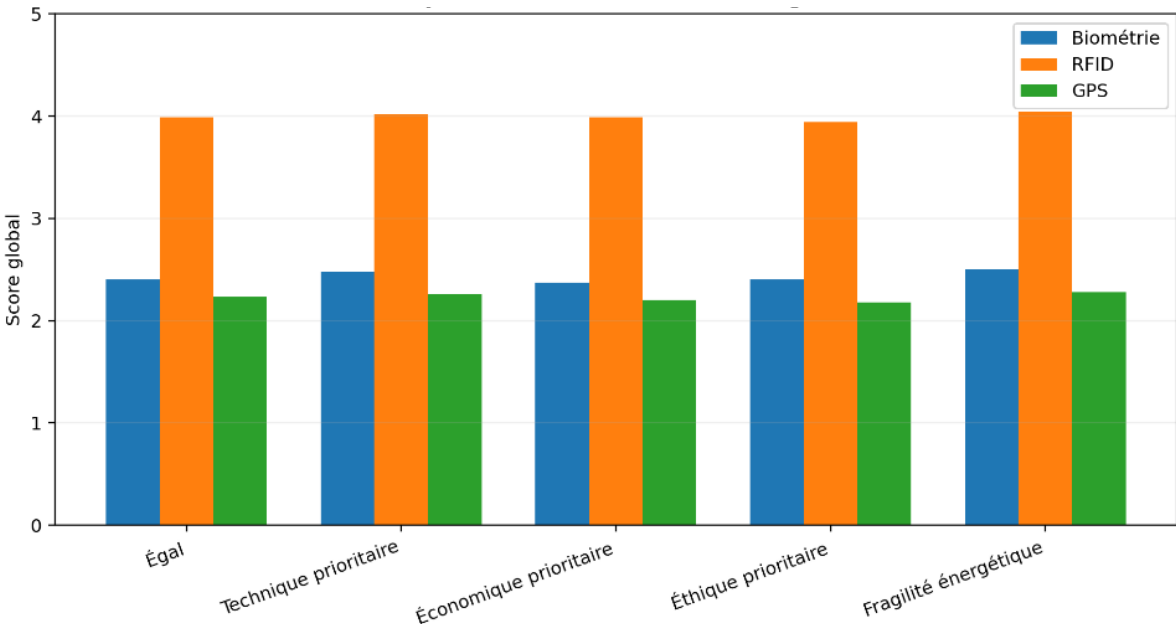
Dimension	Indicateurs positivement orientés	Poids	RFID	Biométrie	GPS	Justification
Technique	Robustesse ; autonomie énergétique ; autonomie vis-à-vis d'Internet ; fiabilité ; couverture	25 %	4,2	3,8	2,5	Critères NIST et audits CICR
Économique	CAPEX ; OPEX ; disponibilité ; maintenance	25 %	4,0	2,0	2,0	Obstacle majeur des rapports PNUD
Organisationnelle	Simplicité ; compétences ; maintenance ; intégration	25 %	3,9	2,5	2,0	Modèle TOE et projets MONUSCO
Éthique et sociale	Protection des données ; intrusion ; acceptabilité ; gouvernance	25 %	3,8	1,3	2,4	Loi congolaise et normes ISO
Score global		100 %	3,99	2,40	2,23	Construit contextuel, non absolu

NB : Ces scores expriment l'adéquation perçue au contexte de Bukavu, et non une supériorité technique absolue. L'écart entre RFID (3,99) et biométrie (2,40) est principalement dû aux contraintes économiques, organisationnelles et éthiques dans ce milieu spécifique.

III.4. Analyse de sensibilité

Cinq scénarios de pondération sont testés sur les scores documentaires initiaux : pondération égale ; priorité aux critères techniques ; priorité aux critères économiques ; priorité aux critères éthiques ; forte priorité aux contraintes énergétiques et de connectivité. Le classement global reste RFID > biométrie > GPS dans les cinq scénarios. En poussant l'analyse à des pondérations extrêmes (ex. : 60 % technique, 10 % éthique), la RFID reste première, mais l'écart se resserre avec la biométrie. Cette robustesse confirme la pertinence du choix contextuel, mais ne dispense pas d'une validation terrain.

Figure 1 : Analyse de sensibilité du classement global selon les pondérations



I

II.5. Positionnement de la présente étude

Pour l'enregistrement d'un prisonnier dans un système de gestion de base de données comprenant le dossier judiciaire et les données biométriques, la biométrie apparaît comme la technologie la plus adaptée. L'enquête attribue 58 % des préférences à la biométrie seule pour l'identification, tandis que les empreintes digitales sont considérées comme la modalité biométrique la plus fiable par 68 % des répondants. Pour la localisation intra-muros, la RFID est privilégiée ; pour le suivi externe, le GPS est davantage choisi. Ces résultats, confrontés aux fiches techniques et aux recherches existantes (y compris les études locales), conduisent à proposer une architecture hybride évolutive.

IV. RÉSULTATS DE L'ENQUÊTE À BUKAVU

IV.1. Perception de la sécurité et demande technologique

Les résultats montrent une situation de sécurité perçue comme moyenne à faible. La note moyenne est de 2,7/5 ; Kadutu obtient 2,3/5. 44 % des répondants déclarent avoir été victimes d'un acte criminel au cours des douze derniers mois, 71 % considèrent les évasions comme une menace importante et 86 % pensent qu'un système technologique améliorerait la sécurité (enquête de terrain à Bukavu, 2025).

IV.2. Résultats sur l'identification biométrique

Pour les technologies biométriques, les empreintes digitales sont connues par 92 % des répondants et 68 % les considèrent comme la modalité la plus fiable. La reconnaissance faciale est connue par 58 %, mais seulement 18 % la placent en première position de fiabilité. La reconnaissance vocale est moins connue (35 %) et seulement 6 % la considèrent comme la plus fiable. L'efficacité perçue de la biométrie atteint 3,5/5 et la favorabilité 3,7/5. Le coût (77 %) et le manque d'électricité (70 %) sont les deux principaux obstacles (enquête de terrain à Bukavu, 2025).

Tableau 5 : Connaissance et fiabilité perçue des modalités biométriques

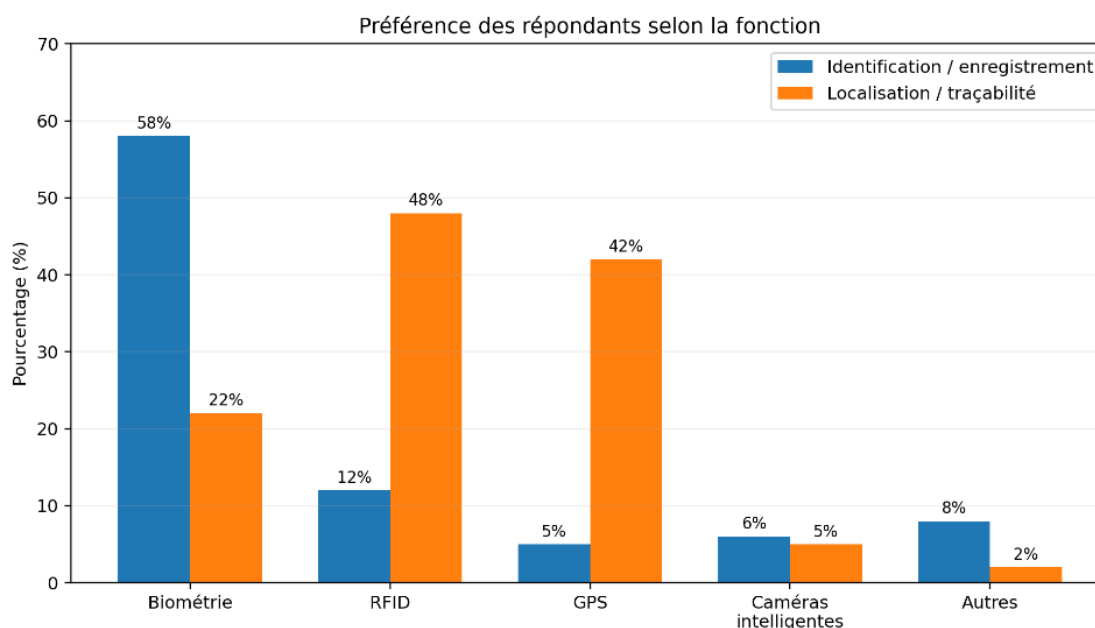
Modalité	Connu e	Perçue comme la plus fiable	Interprétation
Empreinte digitale	92 %	68 %	Modalité de référence pour l'enrôlement

Reconnaissance faciale	58 %	18 %	Très utile pour vérification et surveillance
Reconnaissance vocale	35 %	6 %	Modalité complémentaire
Iris	22 %	5 %	Peu connu dans l'échantillon

IV.3. Résultats sur la localisation et la traçabilité

Les répondants distinguent nettement les espaces. La RFID est jugée adaptée intra-muros par 62 %, alors que le GPS est choisi pour la localisation externe par 75 %. Dans la question de préférence directe, la RFID seule reçoit 48 % pour la localisation intra-muros et le GPS seul 42 % pour la localisation externe ; l'hybride atteint respectivement 36 % et 44 % (enquête de terrain à Bukavu, 2025).

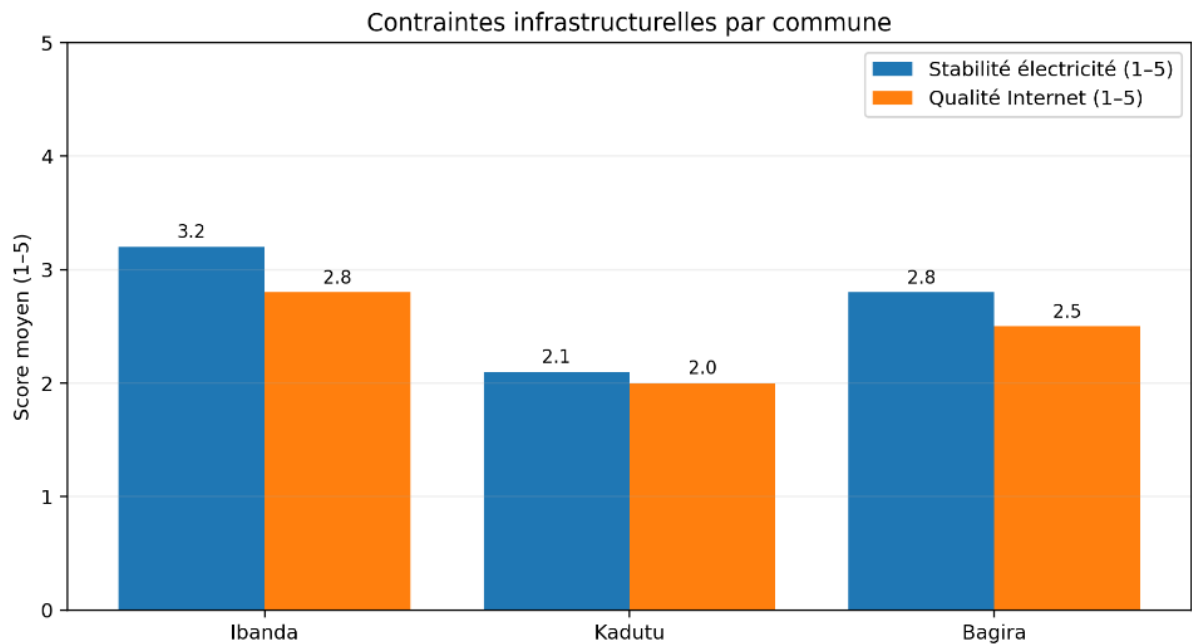
Figure 2 : Préférences des répondants selon la fonction d'identification et de localisation



IV.4. Contraintes infrastructurelles

La stabilité moyenne de l'électricité est évaluée à 2,7/5 et la qualité moyenne d'Internet à 2,4/5. Kadutu est la commune la plus fragile sur les deux critères. 77 % des répondants pensent que la RFID peut rester efficace malgré les coupures d'électricité, tandis que seulement 27 % pensent que le GPS restera efficace malgré les problèmes d'Internet. Il faut cependant interpréter ce dernier résultat avec précision : ce n'est pas le calcul GPS qui nécessite Internet, mais la chaîne de transmission et de supervision à distance qui peut être perturbée (enquête de terrain à Bukavu, 2025).

Figure 3 : Contraintes d'électricité et de connectivité selon les communes



IV.5. Acceptabilité sociale, éthique et gouvernance

49 % des répondants pensent que la surveillance peut porter atteinte à la vie privée. En même temps, 92 % demandent une protection légale des données et 87 % souhaitent que l'accès soit réservé aux autorités judiciaires. Les risques les plus cités sont l'usage abusif des données (68 %), l'atteinte à la dignité (52 %), la surveillance excessive (48 %) et la stigmatisation (41 %). L'acceptabilité spontanée n'est que de 35 % (enquête de terrain à Bukavu, 2025).

IV.6. Protection, énergie et financement

Le risque de vol ou de sabotage est évalué à 3,9/5, et à 4,5/5 à Kadutu. La capacité locale de réparation est faible à moyenne (2,8/5). L'installation à l'intérieur de la prison est fortement soutenue (4,3/5). Les principales mesures proposées sont le gardiennage, le local technique sécurisé, les boîtiers anti-arrachement, l'alarme et la vidéosurveillance. Le solaire avec batteries est plébiscité par 86 % des répondants. 63 % estiment que l'État ne peut pas supporter seul les coûts CAPEX et OPEX (enquête de terrain à Bukavu, 2025).

V. CONFRONTATION DES RÉSULTATS : ENQUÊTE, RECHERCHE SECONDAIRE ET FICHES TECHNIQUES

Cette section constitue le cœur de la révision. Elle ne cherche pas à faire entrer toutes les technologies dans un même classement. Elle confronte la perception des acteurs aux capacités techniques documentées, en incluant les résultats des études locales antérieures. La conclusion devient fonctionnelle : biométrie pour l'identité ; RFID pour la localisation intra-muros ; GPS pour le suivi externe ; caméras et capteurs pour compléter la surveillance.

Tableau 6 : Confrontation entre enquête de Bukavu et recherche secondaire

Technologie	Résultat de l'enquête	Recherche secondaire / fiche technique	Conclusion
-------------	-----------------------	--	------------

Biométrie	58 % pour biométrie seule en identification ; empreintes 68 % de fiabilité	NIST : biométrie adaptée à la vérification 1:1 et à l'identification 1: N ; qualité de l'échantillon déterminante. Études locales : mémoires ISTEGI/ISP Bukavu confirment la faisabilité d'une base biométrique	Très forte pour l'enregistrement et la vérification
RFID	48 % pour RFID seule intra-muros ; 62 % jugent RFID adaptée intra-muros	GS1/EUIPO : RFID passive peu énergivore ; lecteurs nécessaires ; détection dans une zone. Travaux RTLS : localisation indoor possible, mais dépend de la configuration. Projets MONUSCO : équipements déjà fournis à Bukavu	Très forte pour la localisation par zones
GPS	42 % GPS seul et 44 % hybride pour localisation externe	GPS.gov : position calculée à partir des signaux satellites ; transmission à distance dépend du réseau du terminal. Études CICR : énergie solaire possible pour alimenter terminaux	Très forte en extérieur, à utiliser avec une chaîne de communication
Caméras intelligentes	6 % comme solution principale pour l'identification ; 5 % pour localisation intra-muros	NIST : reconnaissance faciale mesurable mais sensible aux caractéristiques des images et à la qualité du système. Mémoire UCB : intégration vidéosurveillance proposée	Complément de surveillance et vérification
Voix / son	35 % connaissent la biométrie vocale ; 6 % la jugent la plus fiable	Biométrie vocale utile comme modalité complémentaire ; capteurs sonores adaptés à la détection d'événements	Complément, pas technologie maîtresse
Empreinte digitale comme capteur d'accès	92 % connaissent la modalité	Biométrie largement évaluée par NIST ; forte valeur pour contrôle d'identité	Contrôle d'accès et vérification

La confrontation permet ainsi d'éviter une contradiction apparente. La RFID reste la première technologie dans le classement global de contexte (3,99), alors que la biométrie devient première lorsqu'on pose la question spécifique de l'identification. Les deux résultats ne parlent pas du même objet. La première mesure l'adéquation générale à l'environnement ; la seconde mesure l'aptitude à établir et vérifier l'identité.

Tableau 7 : Matrice fonctionnelle de décision

Fonction	Technologie principale	Technologie complémentaire	Raison
Enregistrement d'un prisonnier	Biométrie multimodale	RFID comme identifiant technique associé au dossier	L'identité doit être liée à des références biométriques et au dossier judiciaire
Vérification d'identité	Empreinte + visage	Voix	Permet de confirmer l'identité à différents points du processus

Localisation intra-muros	RFID passive (phase 1)	Biométrie / caméras	RFID adaptée aux zones équipées ; biométrie vérifie les passages sensibles
Localisation externe	GPS/GNSS (phase 2)	Réseau mobile + plateforme	Le GPS calcule la position ; le réseau transmet les données
Détection d'événements	Caméras + capteurs sonores	Alarmes / lecteurs d'empreinte	Permet de détecter des situations anormales et d'enregistrer les preuves
Traçabilité globale	Plateforme hybride	Base historique	Fusionner événements d'identité, passages, positions et alertes

VI. DISCUSSION

VI.1. L'identification doit être confiée à la biométrie

L'enquête et la recherche secondaire convergent sur ce point. Dans la base numérique proposée, un prisonnier est enregistré avec un identifiant unique, son dossier judiciaire, ses données d'état civil et ses références biométriques. L'empreinte digitale constitue la modalité de référence dans notre modèle, car elle est la plus connue et la plus fiable dans l'enquête ; la photographie faciale et une référence vocale peuvent être conservées comme modalités complémentaires. Cette combinaison permet de réduire le risque de dépendre d'un seul capteur. Le NIST considère la biométrie comme une famille de technologies d'identification et de vérification dont les performances doivent être évaluées selon la modalité, la qualité de capture et le contexte d'utilisation (NIST, 2025). Le rôle de la biométrie est donc l'identité, et non la localisation. Une empreinte ou un visage répondent à la question « qui ? ». Pour répondre à la question « où ? », il faut enregistrer les événements produits par les lecteurs RFID, le GPS et les capteurs. Cette séparation améliore la cohérence du système d'information.

VI.2. La localisation doit être hybride et évolutive

À l'intérieur de la prison, la RFID constitue la première technologie. Les lecteurs installés aux portes, couloirs ou zones sensibles permettent d'enregistrer le passage d'un tag. Pour une localisation par zones, cette solution est simple et robuste. Nous recommandons des tags RFID passifs UHF (860-960 MHz) pour leur faible coût et leur autonomie illimitée. Les lecteurs doivent être installés à des points de passage stratégiques.

À l'extérieur, le GPS/GNSS est le complément naturel. Le terminal peut calculer sa position même sans Internet ; la difficulté est ensuite de transmettre l'information vers le serveur. Dans l'architecture proposée, cette transmission peut utiliser le réseau mobile disponible. Les terminaux GPS/GNSS (multi-constellation GPS+Glonass+Galileo) embarquent une mémoire flash de 512 Mo, suffisante pour stocker 10 000 positions (environ 500 Ko pour 48 heures de relevés toutes les 5 minutes). La batterie Li-Ion 1 000 mAh offre 72 heures d'autonomie. Une mémoire locale conserve temporairement les positions en cas de coupure, puis synchronise les données dès le retour de la connexion.

Principe de parcimonie (KISS) : En milieu fragile, ce principe est crucial. C'est pourquoi nous proposons une architecture évolutive :

- **Phase 1 :** Biométrie + RFID passive (les plus robustes et peu énergivores) pour l'identification et la localisation intra-muros.
- **Phase 2 :** GPS externe pour le suivi des cas à risque, après validation de la phase 1.
- **Phase 3 :** Caméras intelligentes, capteurs acoustiques et lecteurs d'empreintes comme couches complémentaires, si les phases précédentes sont maîtrisées.

Cette approche réduit les points de défaillance et permet un apprentissage progressif.

VI.3. Les caméras, le son et les empreintes comme couche de sécurité intelligente

Les caméras intelligentes ont pour rôle de surveiller les zones et de rechercher une correspondance faciale lorsqu'un événement nécessite une vérification. Elles ne doivent pas être considérées comme la seule source d'identité. Les capteurs acoustiques peuvent détecter des événements anormaux dans des zones définies ; les lecteurs d'empreintes peuvent contrôler les accès des agents ou vérifier l'identité d'un prisonnier dans un point sensible. Tous ces événements remontent dans la même plateforme, avec date, heure, zone, utilisateur et niveau d'alerte.

VI.4. Énergie, fonctionnement hors ligne et résilience

Le résultat de l'enquête est clair : 86 % recommandent le solaire avec batteries et la capacité de réparation locale est faible (2,8/5). Le système proposé doit donc privilégier des équipements simples, une alimentation locale, un serveur local de secours, une base synchronisable et une stratégie de sauvegarde. Le fonctionnement hors ligne ne signifie pas absence de sécurité ; il signifie que les événements sont d'abord stockés localement et synchronisés plus tard.

Cas critique des évasions : En cas d'évasion massive (comme celle du 14 février 2025), la synchronisation différée est insuffisante. Nous proposons donc :

- Une transmission prioritaire via GSM/4G pour les alertes d'évasion.
- Une mémoire locale pour stocker les positions toutes les 5 minutes en cas de coupure réseau.
- Un terminal GPS avec batterie autonome de 72 heures.
- Une solution de repli satellitaire (Inmarsat ou Iridium) pour les alertes critiques, à activer uniquement en cas de crise extrême. La couverture de ces constellations est mondiale ; le surcoût d'abonnement (environ 50 USD/mois) est intégré aux OPEX.

Un plan de charge est proposé : panneaux photovoltaïques 300 Wc, batteries au lithium 200 Ah, régulateur MPPT, dimensionnés pour assurer 48 heures d'autonomie sans soleil.

VI.5. Cybersécurité, confidentialité et contre-mesures

Le caractère sensible des données impose une architecture de sécurité. ISO/IEC 24745:2022 recommande de protéger les informations biométriques en termes de confidentialité, intégrité et gestion sécurisée des références. Le NIST insiste sur la minimisation, la limitation des finalités et la gestion de la divulgation des données. Le système proposé doit donc appliquer l'authentification forte, les rôles d'accès, le principe du moindre privilège, le chiffrement, la journalisation, les sauvegardes et une politique de conservation (ISO/IEC 24745:2022).

Au-delà du chiffrement et des rôles, des menaces actives sont identifiées et des contre-mesures sont proposées :

- **Spoofing GPS** : le terminal utilise la réception multi-constellation et un algorithme de détection d'anomalies de signal (RAIM) pour filtrer les faux signaux.
- **Clonage de tags RFID** : les tags intègrent un identifiant unique crypté (TID) et un mécanisme challenge-response (protocole AES-128) pour empêcher la duplication.
- **Attaques par déni de service** : le serveur local est équipé d'un pare-feu logiciel et d'une limitation de taux de requêtes ; les alertes critiques sont transmises par un canal secondaire (GSM + satellite).

VI.6. Gouvernance des données, éthique et acceptabilité sociale

a) Responsable de traitement et cadre légal

Le responsable du traitement des données biométriques et de localisation est désigné comme étant le **Ministère de la Justice et Droits Humains**, délégataire à la Direction de la Prison Centrale de Bukavu. Un arrêté ministériel précisera les rôles et responsabilités, en conformité avec la Loi n° 15/026 du 31 décembre 2015 relative à la protection des données à caractère personnel.

b) Consentement et information des prisonniers

L'enrôlement biométrique s'effectue sur la base de l'exécution d'une décision de justice (base légale). Néanmoins, chaque prisonnier est informé, dans une langue qu'il comprend, des finalités, de la durée de conservation et de ses droits d'accès et de rectification. Un formulaire simplifié est signé (ou contresigné par un tiers en cas d'illettrisme). Un recours est possible devant le délégué à la protection des données.

c) Politique de conservation

Les gabarits biométriques sont conservés pendant la durée de la peine, puis détruits **6 mois après la libération**, sauf si une nouvelle procédure judiciaire est en cours. Les historiques de localisation sont anonymisés après 5 ans.

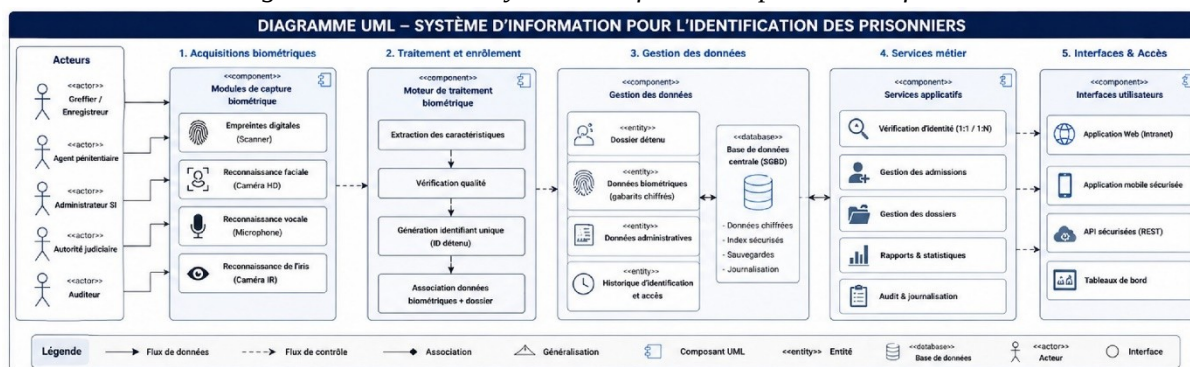
d) Acceptabilité sociale et gouvernance participative

L'acceptabilité spontanée n'est que de 35 %. Pour l'améliorer, nous proposons la mise en place d'un **comité de suivi participatif** composé de représentants de la société civile, d'ONG locales, d'agents pénitentiaires et de magistrats. Ce comité reçoit des rapports d'audit trimestriels et peut formuler des recommandations. Des campagnes de sensibilisation dans les trois communes sont également prévues pour expliquer les finalités sécuritaires et les garanties de protection des données.

VII. MODÈLES DE SYSTÈME D'INFORMATION PROPOSÉS

VII.1. Modèle du système d'information pour l'identification

Figure 4 : Modèle du système d'information pour l'identification



Source : Conception de l'auteur

Le processus commence au moment de l'enrôlement. L'agent autorisé saisit les données d'identité et le dossier judiciaire, puis capture les empreintes, le visage et, selon les moyens disponibles, la voix. Le système réalise un contrôle de qualité et attribue un identifiant unique. Les références biométriques sont ensuite liées à la fiche du prisonnier. À partir de là, une vérification 1:1 ou une identification 1: N peut être réalisée selon le besoin. La base centrale conserve l'historique des opérations et les utilisateurs autorisés disposent d'une interface de consultation conforme à leurs rôles.

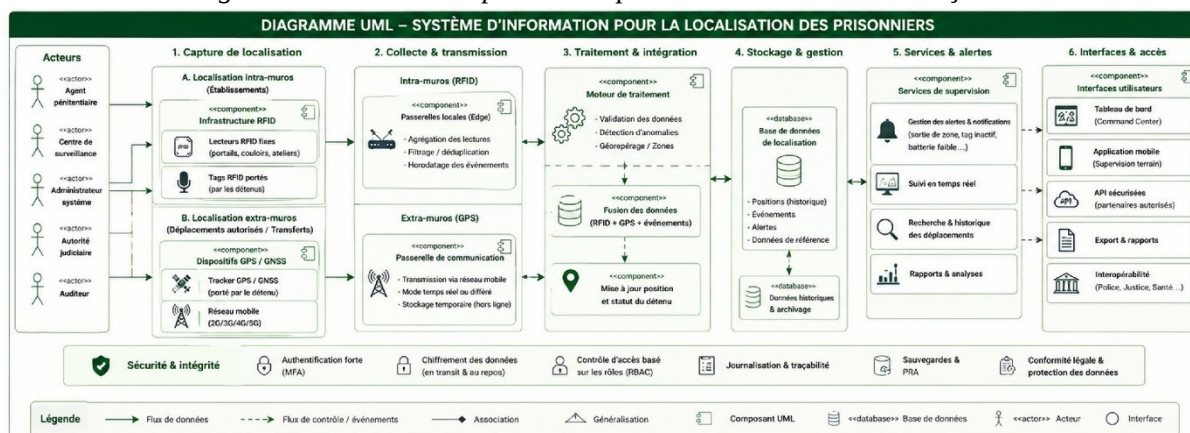
Tableau 8 : Principales données du dossier numérique

Groupe de données	Exemples	Protection recommandée
Identité	Identifiant ; nom ; date de naissance ; sexe ; photographie	Contrôle d'accès par rôle
Dossier judiciaire	Numéro de dossier ; décision ; date d'entrée ; statut pénitentiaire	Accès réservé ; journalisation
Biométrie	Gabarit empreinte ; référence faciale ; référence vocale	Chiffrement ; protection des gabarits ; limitation d'usage
Enrôlement	Date ; agent ; poste ; qualité de capture	Traçabilité complète
Événements	Vérifications ; modifications ; consultations	Journal immuable / audit

Sauvegarde	Copie locale ; copie serveur ; stratégie de reprise	Sauvegarde chiffrée
------------	---	---------------------

VII.2. Modèle du système d'information pour la localisation / traçabilité

Figure 5 : Modèle conceptuel du SI pour la localisation et la traçabilité



Conception de l'auteur

Chaque prisonnier porte un dispositif technique lié à son identifiant dans la base. Dans les espaces internes, les lecteurs RFID capturent les passages. Dans les zones externes ou lors d'une évasion, le terminal GPS/GNSS calcule la position et la transmet dès qu'un moyen de communication est disponible. Les caméras effectuent la reconnaissance faciale, les capteurs de son interviennent en cas d'appel téléphonique pour localiser la voix, et les lecteurs d'empreintes interviennent dans des endroits ciblés (ports, aéroports, frontières) pour vérifier les empreintes digitales à l'entrée ou à la sortie de la ville. La plateforme fusionne ces informations, construit l'historique et produit des alertes. La localisation produite par RFID est donc une localisation par zones équipées ; la localisation externe peut être géographique grâce au GPS.

VII.3. Fonctionnement du système hybride évolutif

1. **Phase 1** : Enregistrer le prisonnier et créer son identifiant unique ; associer le dossier judiciaire et les références biométriques ; associer le tag RFID passif au dossier ; installer et tester les lecteurs dans les zones prioritaires ; enregistrer les passages RFID dans la base locale ; déclencher une vérification biométrique ou vidéo dans les zones sensibles.

2. **Phase 2** : En cas de sortie autorisée ou d'évasion, basculer vers le suivi externe GPS/GNSS ; stocker localement les événements lorsque le réseau est interrompu ; synchroniser automatiquement lorsque la connexion est disponible ; utiliser la solution satellitaire pour les alertes critiques.

3. **Phase 3** : Ajouter les caméras intelligentes, capteurs acoustiques et lecteurs d'empreintes pour renforcer la surveillance, après validation des phases précédentes.

Produire les alertes, rapports et historiques selon les droits d'accès.

Tableau 9 : Sécurité intégrée dans les deux modèles

Contrôle	Identification	Localisation / traçabilité
Authentification des utilisateurs	Oui	Oui
Gestion des rôles	Justice ; direction ; agents	Justice ; direction ; agents
Chiffrement	Base biométrique et dossier	Positions, événements et alertes
Journalisation	Enrôlement, modification, consultation	Passages, positions, alertes, consultations
Fonctionnement hors ligne	Capture locale + synchronisation	Événements locaux + synchronisation

Sauvegarde	Base de référence	Historique des déplacements
Protection physique	Postes biométriques	Lecteurs, caméras, serveur, énergie
Contrôle des usages	Finalité d'identification	Finalité de sécurité et de traçabilité

VIII. RECOMMANDATIONS ET ESTIMATION BUDGÉTAIRE

Recommandations

1. **Commencer par construire une base de données numérique d'identification et d'enrôlement biométrique des prisonniers**, avec un dossier judiciaire et un identifiant unique (phase 1).
2. **Déployer la RFID passive** dans les zones prioritaires pour la localisation intra-muros par zones (phase 1).
3. **Prévoir un terminal GPS/GNSS** pour le suivi externe des cas nécessitant une traçabilité hors de l'enclaustration pénitentiaire (phase 2).
4. **Ajouter une couche de sécurité intelligente** (caméras, détection acoustique, contrôle par empreinte) en phase 3, après validation des phases précédentes.
5. **Installer les équipements critiques à l'intérieur des murs**, dans des locaux sécurisés, conformément au résultat de l'enquête sur le risque de vol et de sabotage.
6. **Prévoir une alimentation solaire avec batteries de secours** et un fonctionnement hors ligne avec synchronisation différée, plus un terminal satellitaire pour les alertes critiques.
7. **Mettre en œuvre des mécanismes de chiffrement, de gestion des rôles, de journalisation, de sauvegarde et de reprise après incident.**
8. **Établir une politique de gouvernance des données** biométriques et de localisation, en conformité avec la loi congolaise n° 15/026, précisant les finalités, les personnes autorisées, la conservation et les procédures d'audit.
9. **Former un personnel local** à l'enrôlement biométrique, à la maintenance RFID, à la gestion réseau et à la cybersécurité.
10. **Réaliser un pilote progressif** avant tout déploiement complet, en commençant par un échantillon de 100 prisonniers, et mesurer la précision, le taux de fausse alerte, la disponibilité et la qualité de localisation.

Estimation budgétaire prévisionnelle (CAPEX et OPEX annuel) pour un pilote de 100 prisonniers

Tableau 10 : Budget pilote 100 prisonniers – CAPEX et OPEX annuel estimés

Poste	Équipement	Qté	Coût unitaire (USD)	CAPEX total (USD)	OPEX annuel (USD)	Remarques
Biométrie	Station d'enrôlement (empreinte + visage)	2	3 000	6 000	600	Maintenance / calibrage
	Serveur local + logiciel biométrique	1	4 000	4 000	800	Licence annuelle + support
RFID	Tags RFID passifs (bracelets)	100	2	200	100	Remplacement 10 % / an
	Lecteurs RFID (portes, couloirs)	10	300	3 000	500	Maintenance
	Câblage et installation	-	-	1 000	-	

GPS (phase 2)	Terminaux GPS/GNSS (10 cas à risque)	10	100	1 000	200	Batteries, usure
	Modem GSM/4G	1	300	300	200	Forfait data
	Modem satellite (repli)	1	600	600	600	Abonnement annuel Inmarsat/Iridium
Énergie	Panneaux solaires + batteries + régulateur MPPT	1 système	3 500	3 500	300	Remplacement batteries tous les 5 ans
Sécurité	Local technique sécurisé (armoire, climatisation)	1	1 500	1 500	100	
	Boîtiers anti-arrachement	100	10	1 000	100	
Formation	Formation du personnel (5 jours)	5 agents	600	3 000	500	Formation continue
Total phase 1				~23 200	~3 200	
Total phases 1+2				~24 800	~4 400	

Notes : Les coûts sont indicatifs, basés sur des devis de fournisseurs internationaux et locaux. Un pilote de 100 prisonniers permettrait de valider les hypothèses techniques avant un déploiement à plus grande échelle. L'OPEX annuel inclut les licences, la maintenance, les remplacements et les abonnements de communication.

IX. ANALYSE SYNTHÉTIQUE DES RÉSULTATS

La principale contribution de cette étude est de sortir d'un classement unique qui pourrait donner l'impression qu'une technologie remplace toutes les autres. Le score global de la première analyse reste utile pour mesurer l'adéquation au contexte. La RFID reste première dans cette grille (3,99 contre 2,40 pour la biométrie et 2,23 pour le GPS), et l'analyse de sensibilité montre que ce classement reste stable. Mais l'enquête de terrain introduit une autre évidence : l'utilisateur ne demande pas une seule technologie pour tout. Il demande une technologie adaptée à chaque fonction. Cette seconde lecture conduit à la biométrie pour l'enregistrement, à la RFID pour le suivi intra-muros, au GPS pour le suivi externe et à une couche de surveillance intelligente pour les événements, avec un déploiement évolutif pour éviter une complexité excessive.

X. LIMITES DE L'ÉTUDE

En plus des limites déjà mentionnées dans la méthodologie (absence de déploiement expérimental, échantillon local, caractère documentaire des scores), trois limites supplémentaires sont explicitement reconnues :

1. **Niveau de détail technique insuffisant pour une implémentation directe** : les spécifications précises (normes ISO des gabarits biométriques, protocoles de communication des tags RFID, formats d'échange de données) ne sont pas définies. Un cahier des charges technique détaillé devra être produit avant le pilote.

2. **Transférabilité limitée** : les résultats sont spécifiques aux contraintes de Bukavu (type de prison, climat, infrastructures). Une adaptation sera nécessaire pour d'autres contextes (zones rurales, autres provinces).

3. **Risques résiduels de cybersécurité** : bien que des contre-mesures soient proposées, aucune évaluation de pénétration (pentest) n'a été réalisée. Le pilote devra inclure des tests de sécurité offensifs.

La proposition doit donc être considérée comme un modèle conceptuel à valider par un prototype et des essais terrain.

XI. CONCLUSION

Cette étude avait pour objectif de confronter les résultats d'une enquête menée à Bukavu (incluant ingénieurs, agents pénitentiaires, société civile et citoyens) avec la recherche secondaire (incluant des études locales ayant consulté juges, directeurs de prison et gardiens) et les caractéristiques techniques des principales technologies d'identification et de localisation des prisonniers. La confrontation montre d'abord qu'il faut distinguer les fonctions. L'identification et l'enregistrement d'un prisonnier dans un système de gestion de base de données doivent être assurés principalement par la biométrie. Le dossier numérique doit associer les données judiciaires et administratives aux références biométriques, en particulier les empreintes digitales, puis compléter, selon les moyens et les besoins, par la reconnaissance faciale et vocale. Cette fonction répond à la question « qui est la personne ? ».

Pour la localisation et la traçabilité, la RFID prend la première place à l'intérieur de la prison parce qu'elle correspond à la logique de localisation par zones équipées de lecteurs. Le GPS/GNSS complète le système à l'extérieur. Cette organisation correspond aux perceptions de l'enquête : la biométrie est préférée pour l'identification, la RFID pour l'intérieur et le GPS pour l'extérieur. L'adhésion de 72 % à l'approche hybride confirme qu'une architecture combinée est mieux comprise et mieux acceptée qu'une technologie unique (enquête de terrain à Bukavu, 2025).

La solution proposée est donc hybride et évolutive. Elle intègre, en phase 1, la biométrie pour l'identification et la vérification, et la RFID passive pour la localisation intra-muros ; en phase 2, le GPS pour le suivi externe ; en phase 3, les caméras intelligentes, les capteurs de son et les lecteurs d'empreintes pour renforcer la surveillance. L'ensemble est réuni dans une plateforme de système d'information qui conserve l'historique, gère les alertes et contrôle les droits d'accès, avec une attention particulière à la résilience (solaire, hors ligne, satellite pour les crises). La gouvernance est renforcée par l'application de la loi congolaise n° 15/026, la désignation d'un responsable de traitement, une politique de conservation des données (destruction des gabarits 6 mois après libération) et la mise en place d'un comité de suivi participatif pour améliorer l'acceptabilité sociale.

Cette conclusion reste prudente : la présente recherche propose une architecture conceptuelle fondée sur une analyse comparative, une enquête de terrain, une recherche secondaire et une estimation budgétaire prévisionnelle (CAPEX/OPEX). Elle ne prétend pas démontrer que le système est déjà opérationnel. La prochaine étape scientifique est un prototype pilote dans une zone contrôlée de l'établissement pénitentiaire, avec mesure de la précision biométrique, de la couverture RFID, de la continuité GPS, de la disponibilité énergétique, du temps de synchronisation et des performances de la surveillance intelligente. Un pilote de 100 prisonniers est recommandé, avec un budget estimatif d'environ 23 200 USD pour la phase 1 et un OPEX annuel d'environ 3 200 USD.

BIBLIOGRAPHIE

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3), 319–340.

Esposito, G., Mezzogori, D., Neroni, M., Rizzi, A., Romagnoli, G., & Rosa, M. (2021). A review of RFID based solutions for indoor localization and location-based classification of tags.

GS1 (2024). What is RFID? Difference between passive and active RFID tags; how an RFID system works.

ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection — Biometric information protection.

Lam, L. D. M., Tang, A., & Grundy, J. (2016). Characterising indoor positioning estimation using experimental data from an active RFID-based real-time location system. *Journal of Location Based Services*, 10(4), 262–284. <https://doi.org/10.1080/17489725.2016.1259893>

Laudon, K. C., & Laudon, J. P. (2020). *Management Information Systems: Managing the Digital Firm* (16th ed.). Pearson.

NIST (2000). *An Introduction to Evaluating Biometric Systems*. National Institute of Standards and Technology.

NIST (2013). *Introduction to Face Recognition and Evaluation of Algorithm Performance*. National Institute of Standards and Technology.

NIST (2019). *Face Recognition Vendor Test (FRVT) Part 2: Identification*. NISTIR 8271.

NIST (2025). *Face Recognition Technology Evaluation (FRTE)*. National Institute of Standards and Technology.

NIST (2024). *Cybersecurity Framework 2.0*. National Institute of Standards and Technology.

NIST (2026). *Privacy Considerations for Digital Identity Guidelines*. National Institute of Standards and Technology.

Radjou, N., Prabhu, J., & Ahuja, S. (2012). *Jugaad Innovation*. Jossey-Bass.

République Démocratique du Congo. (2015). Loi n° 15/026 du 31 décembre 2015 relative à la protection des données à caractère personnel.

Tornatzky, L. G., & Fleischer, M. (1990). *The Processes of Technological Innovation*. Lexington Books.

Wei, Z., Chen, J., Tang, H., & Zhang, H. (2023). RSSI-based location fingerprint method for RFID indoor positioning: a review. *Nondestructive Testing and Evaluation*, 39(1).

Zimmer, M. (2020). The limits of technological solutionism in public sector reform. *Technology in Society*, 63, 101421.

[GPS.gov](https://gps.gov)GPS. gov (2026). GPS Overview and GPS Accuracy.

EUIPO (2026). Passive RFID Tags; Battery-Assisted Passive RFID Tags — Anti-Counterfeiting and Anti-Piracy Technology Guide.

Travaux locaux (non publiés, consultés en bibliothèque) :

- Mémoire d'Architecture et Urbanisme, UCB Bukavu : « Conception et modélisation d'une infrastructure pénitentiaire moderne aux normes sécuritaires et technologiques à Kavumu ».
- Mémoire en Informatique de Gestion, ISTEIGI / ISP Bukavu : « Conception d'un système d'information informatisé pour la gestion du registre d'écrou et le suivi judiciaire des détenus à la Prison Centrale de Bukavu ».
- Projet MONUSCO – Section Appui à la Justice et aux Prisons : « Déploiement des équipements informatiques et formation du personnel pénitentiaire pour l'archivage numérique ».
- Audit énergétique CICR : « Dimensionnement d'installations solaires hybrides pour la Prison Centrale de Bukavu ».
- Rapport PNUD – Projet d'Appui à la Réforme de la Justice (PARJ) : « Évaluation des besoins technologiques pour l'interconnexion des cours et prisons du Sud-Kivu ».