

## Modélisation d'un système résilient de continuité opérationnelle des élections numériques en République démocratique du Congo à l'horizon 2028

*“Modelling a Resilient Operational Continuity System for Digital Elections in the Democratic Republic of the Congo towards 2028”*

**Katayi Ntumba Freddy**

Département de réseaux informatiques et Télécommunications de l'Université de KANANGA, République Démocratique du Congo. Email : [freddykatayi1@gmail.com](mailto:freddykatayi1@gmail.com)

doi: <https://doi.org/10.37745/bjmas.0619>

Published October 17, 2026

**Citation :** Freddy K.N. (2026) Modélisation d'un système résilient de continuité opérationnelle des élections numériques en République démocratique du Congo à l'horizon 2028, *British Journal of Multidisciplinary and Advanced Studies*, 7(5), 49-74

**Résumé.** La numérisation progressive des processus électoraux améliore la rapidité du traitement et de la transmission des données, mais accroît également la dépendance du scrutin à des infrastructures technologiques, énergétiques, communicationnelles et logistiques interdépendantes. En République démocratique du Congo, cette dépendance constitue un enjeu majeur pour la préparation des élections de 2028, compte tenu des disparités territoriales en matière d'électricité, de connectivité et d'accès logistique. Cette étude vise à modéliser un système résilient capable d'assurer la continuité des fonctions électorales critiques malgré différentes situations de défaillance. La méthodologie repose sur une approche quantitative, systémique et prospective combinant la cartographie des infrastructures critiques, l'analyse des interdépendances, l'AMDEC (Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité), la modélisation de la disponibilité et la simulation de scénarios de défaillance. Les résultats simulés montrent que le modèle proposé pourrait porter la disponibilité du système de 69,10% à 98,70% lors d'une crise multisectorielle, réduire le temps moyen d'interruption de 445 à 19 minutes et le temps de récupération de 558 à 28 minutes. La proportion de données non synchronisées diminuerait de 8,20% à 0,80%, tandis que 94% des fonctions critiques seraient maintenues. L'étude conclut qu'un système résilient électoral efficace repose sur une approche multicouche intégrant redondance, diversification, basculement, fonctionnement dégradé et récupération.

**Mots-clés :** Modélisation, Système résilient, Elections numériques, Continuité opérationnelle, Horizon 2028, Infrastructures critiques, Energie, Logistique, République démocratique du Congo.

**Abstract.** The gradual digitalisation of electoral processes improves the speed and efficiency of data processing and transmission, but it also increases electoral dependence on interconnected technological, energy, communication, and logistical infrastructures. In the Democratic Republic of the Congo, this dependence represents a major challenge for the 2028 elections because access to electricity, connectivity, and logistical services varies considerably across the country. This study aims to model a resilient system capable of maintaining critical electoral functions despite technological, energy, communication, and logistical failures. The research adopts a quantitative, systemic, and prospective approach combining critical-infrastructure mapping, dependency analysis, Failure Mode and Effects Analysis (FMEA), availability modelling, and failure-scenario simulation. The simulated results show that the proposed model could increase system availability from 69.10% to 98.70% under a multisector crisis, reduce the average interruption time from 445 to 19 minutes, and shorten the average recovery time from 558 to 28 minutes.

*The proportion of unsynchronised data would decrease from 8.20% to 0.80%, while 94% of critical functions would remain operational. The study concludes that effective electoral resilience requires a multi-layered approach combining redundancy, diversification, failover mechanisms, degraded-mode operation, data preservation, and recovery capabilities.*

**Keywords:** Modelling, Resilient System, Digital Elections, Operational Continuity, 2028 Horizon, Critical Infrastructures, Energy, Logistics, Democratic Republic of the Congo.

## INTRODUCTION

La transformation numérique des processus électoraux s'est progressivement imposée comme une composante importante de l'administration électorale contemporaine. Les technologies de l'information et de la communication interviennent désormais dans plusieurs étapes du cycle électoral, notamment l'inscription et l'identification des électeurs, le vote, le traitement des résultats et leur publication (Int. IDEA, 2026). Cette évolution apporte des gains considérables en matière de rapidité, de traitement et de gestion des données, mais elle introduit également une nouvelle forme de dépendance : plus les opérations électorales reposent sur des infrastructures numériques, plus leur continuité dépend de la disponibilité des équipements, de l'énergie, des réseaux de communication, des logiciels, du personnel qualifié et des moyens logistiques nécessaires à leur fonctionnement (Int. IDEA, 2026). L'élection numérique ne doit donc plus être considérée comme un simple ensemble d'outils informatiques, mais comme un système sociotechnique critique dont la fiabilité dépend de l'interaction permanente entre technologies, infrastructures, ressources humaines et organisation.

Cette dépendance devient particulièrement visible lorsque l'on considère l'ampleur des opérations électorales contemporaines. En République démocratique du Congo, le fichier électoral validé pour les élections de 2023 comptait 43 955 181 électeurs (CENI, 2023). Le dispositif utilisé lors du scrutin reposait notamment sur des machines dotées d'une connexion 3G sécurisée pour la transmission des résultats, d'une batterie annoncée comme offrant jusqu'à 72 heures d'autonomie et de mécanismes de sauvegarde des données sur supports amovibles (The Carter Center, 2024). Ces spécificités montrent déjà que la continuité électorale dépendait de plusieurs éléments simultanément : alimentation énergétique, fonctionnement matériel, logiciel, stockage et communication. La défaillance d'un seul de ces éléments pouvait donc affecter les opérations réalisées au niveau local et, par effet de propagation, perturber les étapes ultérieures du processus.

Le contexte infrastructurel de la RDC renforce cette vulnérabilité. En 2023, seulement 22,1 % de la population avait accès à l'électricité selon les données de la Banque mondiale (World Bank, 2026). Au début de 2025, le pays comptait environ 60,3 millions de connexions mobiles, mais seulement 34 millions d'utilisateurs d'Internet, soit un taux de pénétration de 30,6 % (DataReportal, 2025). Ces chiffres traduisent un paradoxe déterminant pour la numérisation électorale : les moyens de communication mobile connaissent une diffusion importante alors que l'accès à l'électricité et à Internet demeure fortement limité et inégal. Dans une telle situation, la disponibilité d'un équipement numérique ne garantit pas sa capacité à fonctionner durablement. Un dispositif peut être opérationnel sur le plan informatique, mais devenir inutilisable à la suite d'une coupure d'électricité ; inversement, une machine

correctement alimentée peut ne plus transmettre les données si le réseau de communication est indisponible. À cela s'ajoutent les contraintes géographiques et logistiques d'un territoire vaste, où l'accès aux bureaux de vote, aux techniciens, aux équipements de remplacement, aux pièces de rechange et au carburant peut varier considérablement d'une localité à une autre.

Les élections générales de 2023 ont concrètement illustré cette interdépendance. Le Carter Center a rapporté que des difficultés logistiques avaient empêché ou retardé l'ouverture de nombreux bureaux de vote et que certains bureaux avaient dû interrompre temporairement leurs opérations en raison de problèmes liés aux machines à voter (The Carter Center, 2023, 2024). La CENI avait finalement prolongé le vote dans plusieurs endroits confrontés à des difficultés opérationnelles. Ces événements montrent qu'une perturbation électorale ne résulte pas nécessairement d'une défaillance informatique isolée. Un problème logistique peut empêcher l'arrivée du matériel ; une panne énergétique peut interrompre l'utilisation d'un équipement ; une rupture de communication peut empêcher la transmission des données ; et l'absence de moyens techniques ou humains peut prolonger considérablement le délai de récupération. Le véritable risque apparaît donc lorsque plusieurs dépendances se combinent et transforment une défaillance locale en perturbation systémique.

C'est précisément à ce niveau que se situe le problème scientifique de la présente étude. Les travaux consacrés aux technologies électorales accordent une attention importante à la sécurité, à l'intégrité, à la transparence et à l'auditabilité des systèmes, mais la continuité opérationnelle exige une perspective plus large. Il ne suffit pas qu'un système électoral soit sécurisé lorsqu'il fonctionne normalement ; il doit également pouvoir continuer à assurer ses fonctions essentielles lorsqu'une partie de son infrastructure devient indisponible. Cette exigence rejoint les principes contemporains de résilience des systèmes critiques, selon lesquels la capacité d'un système à anticiper, absorber, répondre et récupérer après une perturbation constitue une dimension essentielle de sa sécurité et de sa fiabilité (NIST, 2024). Dans le contexte congolais, cette approche doit intégrer simultanément les dimensions technologique, énergétique, communicationnelle et logistique, car leur interdépendance détermine directement la capacité du processus électoral à résister aux interruptions.

La question centrale devient dès lors la suivante : « comment concevoir et modéliser un système résilient capable de maintenir les fonctions critiques des élections numériques en République démocratique du Congo malgré les défaillances technologiques, énergétiques, communicationnelles et logistiques à l'horizon 2028 ? », Cette interrogation suppose d'identifier les composants critiques du système, de déterminer les modes de défaillance susceptibles de les affecter, d'analyser leurs dépendances et d'évaluer leurs conséquences sur la continuité des opérations. Elle conduit également à rechercher des mécanismes capables de limiter la propagation des incidents : redondance des équipements, diversification des sources d'énergie, pluralité des moyens de communication, sauvegarde des données, fonctionnement hors ligne, basculement vers des infrastructures de secours, disponibilité des pièces de rechange et organisation rapide de la maintenance.

L'hypothèse générale est que l'intégration de ces mécanismes dans un modèle unique de résilience permettrait de réduire les interruptions et d'accélérer la récupération du système électoral après incident.

Cette hypothèse se décline en quatre propositions complémentaires : la redondance technologique devrait réduire la durée des interruptions liées aux pannes matérielles ou logicielles ; la diversification énergétique devrait améliorer la disponibilité des équipements ; la pluralité des canaux de communication devrait limiter les effets d'une rupture de connectivité ; et une organisation logistique fondée sur la préposition des ressources et la capacité d'intervention rapide devrait réduire le temps de récupération. L'hypothèse centrale est toutefois que ces mécanismes produiraient un effet plus important lorsqu'ils sont conçus comme les composantes d'un système intégré plutôt que comme des solutions indépendantes.

L'objectif général de cette recherche est ainsi de modéliser un système résilient de continuité opérationnelle capable de maintenir les fonctions critiques des élections numériques en RDC face aux principales catégories de défaillances susceptibles de survenir à l'horizon 2028. Il s'agit, plus précisément, d'identifier les infrastructures critiques, de cartographier leurs vulnérabilités et leurs interdépendances, de caractériser les scénarios de défaillance, d'en mesurer les conséquences, puis de concevoir et de simuler des mécanismes de prévention, de détection, de tolérance, de continuité et de récupération. La performance du modèle sera appréciée à partir d'indicateurs tels que la disponibilité du système, la durée des interruptions, le temps moyen de récupération, la capacité de fonctionnement en mode dégradé et le taux de conservation des données.

L'originalité de cette recherche réside donc dans le passage d'une approche fragmentée du risque à une conception systémique de la résilience électorale. Plutôt que d'étudier séparément une panne informatique, une coupure électrique, une interruption du réseau ou une difficulté de transport, l'étude cherchera à comprendre comment ces événements peuvent s'enchaîner et se renforcer. Par exemple, une coupure d'électricité peut arrêter un équipement ; l'arrêt peut interrompre la collecte ou la transmission ; l'absence de réseau peut empêcher le signalement rapide de l'incident ; et l'éloignement du centre de maintenance peut prolonger l'indisponibilité. Le modèle proposé devra précisément empêcher qu'une telle chaîne locale de défaillances ne se transforme en interruption durable d'une fonction électorale critique.

L'enjeu scientifique dépasse ainsi la seule amélioration d'un dispositif électronique. Il consiste à déterminer dans quelles conditions une infrastructure électorale numérique peut continuer à fonctionner malgré l'imperfection de son environnement. Pour les élections de 2028, la question essentielle ne sera donc pas uniquement de disposer d'équipements plus performants, mais de disposer d'un système capable de fonctionner normalement lorsque les conditions sont favorables, en mode dégradé lorsqu'elles se détériorent, et de reprendre rapidement son fonctionnement après une défaillance. La présente recherche s'inscrit dans cette perspective en proposant une modélisation intégrée de la continuité opérationnelle électorale, adaptée aux réalités technologiques, énergétiques, communicationnelles et logistiques de la République démocratique du Congo.

## **MATERIELS ET METHODES**

### **Matériels**

#### **Cadre technologique et infrastructures étudiées**

L'étude porte sur l'ensemble des ressources technologiques nécessaires au fonctionnement d'un système électoral numérique en République démocratique du Congo. Le matériel étudié ne se limite pas aux équipements utilisés directement dans les bureaux de vote, mais comprend l'ensemble de la chaîne technologique permettant l'acquisition, le traitement, le stockage, la transmission, la sauvegarde et l'exploitation des données électorales. Les ressources technologiques considérées comprennent notamment les équipements électoraux, les ordinateurs, les serveurs, les dispositifs de stockage, les bases de données, les équipements réseau et les différents périphériques nécessaires aux opérations électorales. Les logiciels et systèmes informatiques associés sont également pris en compte dans la mesure où leur fonctionnement conditionne l'exploitation des équipements matériels et la disponibilité des services électoraux numériques.

L'étude intègre autant les infrastructures de télécommunication nécessaires à l'échange des informations entre les différents niveaux du système électoral. Il s'agit notamment des réseaux mobiles, d'Internet, de la fibre optique, des liaisons radio, des communications satellitaires et de tout autre moyen de transmission disponible selon les caractéristiques des territoires étudiés. Cette définition élargie du matériel d'étude permet de considérer le système électoral numérique comme une infrastructure distribuée et interdépendante, dont la continuité dépend simultanément des équipements informatiques, des réseaux de communication, de l'énergie, de la logistique et des ressources nécessaires à leur exploitation.

#### **Infrastructures énergétiques et dispositifs d'alimentation de secours**

Les infrastructures énergétiques constituent une composante essentielle du matériel étudié, car l'ensemble des équipements numériques et des infrastructures de communication dépend de leur alimentation électrique.

L'étude prend ainsi en compte les différentes sources d'énergie susceptibles d'être mobilisées pour assurer le fonctionnement des équipements électoraux : réseau électrique, groupes électrogènes, batteries, systèmes UPS et, lorsque leur disponibilité est envisageable, sources renouvelables telles que l'énergie solaire. Les dispositifs d'alimentation de secours sont également considérés comme des ressources matérielles nécessaires à la continuité du système. Ils permettent notamment d'assurer une alimentation temporaire lorsque la source principale devient indisponible. Leur présence est particulièrement importante dans les territoires où la stabilité de l'alimentation électrique peut varier fortement. Le matériel énergétique est donc considéré non seulement comme une source d'alimentation des équipements, mais comme une composante indispensable de l'infrastructure globale sur laquelle repose la continuité des opérations électorales numériques.

### **Infrastructures de communication et de transmission**

Les infrastructures de communication constituent une deuxième catégorie majeure de matériels. Elles assurent l'échange des données entre les différents équipements, centres et niveaux du système électoral. L'étude prend en compte les réseaux mobiles, les connexions Internet, la fibre optique, les liaisons radio, les communications satellitaires ainsi que les autres moyens de transmission disponibles. Ces infrastructures peuvent être utilisées individuellement ou de manière complémentaire selon les caractéristiques du territoire et la disponibilité des services. Une attention particulière est accordée à la diversité des moyens de communication, notamment lorsque plusieurs canaux indépendants peuvent être disponibles. Cette diversité constitue une ressource matérielle importante pour la continuité des échanges lorsque le canal principal devient indisponible.

### **Ressources logistiques, maintenance et équipements de secours**

Les matériels logistiques comprennent les moyens nécessaires à l'acheminement, au déploiement, au remplacement et à la maintenance des équipements électoraux. Ils comprennent notamment les moyens de transport, les équipements de maintenance, les pièces de rechange, les ressources en carburant et les équipements de remplacement. L'étude tient compte de la disponibilité géographique de ces ressources. Dans les zones éloignées ou difficilement accessibles, l'absence d'un équipement de remplacement, d'une pièce de rechange ou d'un moyen de transport approprié peut prolonger considérablement l'indisponibilité d'un système. Les équipements de secours sont donc intégrés au matériel étudié afin de prendre en compte la capacité physique du système à remplacer un composant défaillant et à maintenir les opérations essentielles. La diversité des points de stockage et des ressources techniques pourra également être considérée. La disponibilité d'équipements de remplacement dans plusieurs centres régionaux peut notamment réduire le temps nécessaire à l'intervention dans les zones éloignées.

### **Données et ressources informationnelles**

Les données constituent une ressource essentielle du système étudié. Elles comprennent notamment les données électorales produites, collectées, stockées, transmises, sauvegardées et synchronisées au cours des différentes opérations. Les ressources informationnelles considérées comprennent également les données historiques relatives aux cycles électoraux antérieurs, principalement ceux de 2018 et 2023, lorsqu'elles sont disponibles et exploitables. Ces informations serviront de base documentaire pour caractériser les contraintes et les situations susceptibles d'être représentées dans les simulations prospectives vers 2028. Lorsque des données de terrain seront disponibles, les informations provenant des responsables électoraux, des techniciens et des opérateurs pourront également être mobilisées comme ressources complémentaires. Elles permettront notamment de rapprocher les caractéristiques du modèle des conditions réelles d'exploitation. Les données sensibles relatives aux infrastructures électorales, aux configurations techniques et aux dispositifs de sécurité seront traitées avec précaution et, lorsque nécessaire, anonymisées ou agrégées.

### **Ressources humaines**

Les ressources humaines constituent une composante complémentaire du dispositif matériel et organisationnel mobilisé par l'étude. Elles comprennent principalement les responsables électoraux, les techniciens, les opérateurs, les équipes de maintenance et les autres personnels nécessaires à l'exploitation des infrastructures numériques. Leur prise en compte est nécessaire parce que plusieurs

ressources techniques ne peuvent fonctionner ou être restaurées sans intervention humaine. La maintenance, le remplacement des équipements, le diagnostic des incidents, la gestion des infrastructures et la reprise des opérations nécessitent notamment la disponibilité de compétences techniques appropriées. Dans les territoires éloignés, la disponibilité locale du personnel technique constitue donc une ressource importante à considérer dans l'évaluation de la continuité opérationnelle.

### **Outils informatiques de modélisation et de simulation**

La réalisation de l'étude nécessitera des outils informatiques permettant de construire, paramétrer, exécuter et analyser les modèles développés. Les principaux environnements envisagés sont Python, MATLAB/Simulink et R. Le choix de l'outil dépendra de la structure définitive du modèle, de la nature des données disponibles et des besoins liés aux simulations. Ces outils serviront notamment à exploiter les données, formaliser les relations entre les composants, exécuter les simulations et calculer les indicateurs nécessaires à l'évaluation du système. Les techniques de modélisation proprement dites, notamment les modèles probabilistes, les chaînes de Markov, les réseaux de *Petri* et la simulation Monte-Carlo, seront présentées dans la partie « Méthodes », puisqu'elles correspondent à des procédures d'analyse et non à des matériels. Le document initial les associait aux outils informatiques, mais cette distinction améliore la séparation méthodologique entre ressources utilisées et méthodes appliquées.

## **Méthodes**

### **Approche et démarche méthodologique**

Cette étude s'inscrit dans une démarche de recherche appliquée à dominante quantitative, systémique et prospective. Elle vise à caractériser les vulnérabilités susceptibles d'affecter les élections numériques en République démocratique du Congo (RDC), à mesurer leurs effets sur la continuité des fonctions électorales critiques et à évaluer l'efficacité de mécanismes destinés à renforcer la résilience du système. L'approche systémique est retenue parce que le processus électoral numérique constitue un système sociotechnique dans lequel les infrastructures technologiques, énergétiques, communicationnelles, logistiques et organisationnelles entretiennent des relations de dépendance. La démarche méthodologique repose sur quatre opérations successives : caractériser le système étudié, identifier ses fonctions et composants critiques, construire un modèle de résilience et évaluer ce modèle par simulation. Les expériences des cycles électoraux de 2018 et 2023 serviront de références pour définir les contraintes et les situations de défaillance susceptibles d'être représentées dans les scénarios prospectifs associés à l'échéance de 2028.

Il ne s'agit pas en conséquence de prédire les incidents futurs, mais de construire des situations plausibles permettant de tester le comportement du système dans différentes conditions de perturbation. Lorsque des données de terrain seront disponibles, celles-ci pourront être complétées par des informations qualitatives recueillies auprès de responsables électoraux, de techniciens ou d'opérateurs. Cette complémentarité permettra de rapprocher les paramètres du modèle des conditions réelles d'exploitation et de limiter la dépendance à des hypothèses purement théoriques.

### Identification des fonctions, actifs critiques et dépendances

La première phase opérationnelle consiste à identifier les fonctions électorales critiques, c'est-à-dire celles dont l'interruption pourrait compromettre une partie importante du processus électoral. L'analyse porte notamment sur l'authentification, l'enregistrement, la collecte, le stockage, la transmission, la synchronisation, la compilation, la sauvegarde, la vérification, la publication des résultats, la communication opérationnelle et la maintenance.

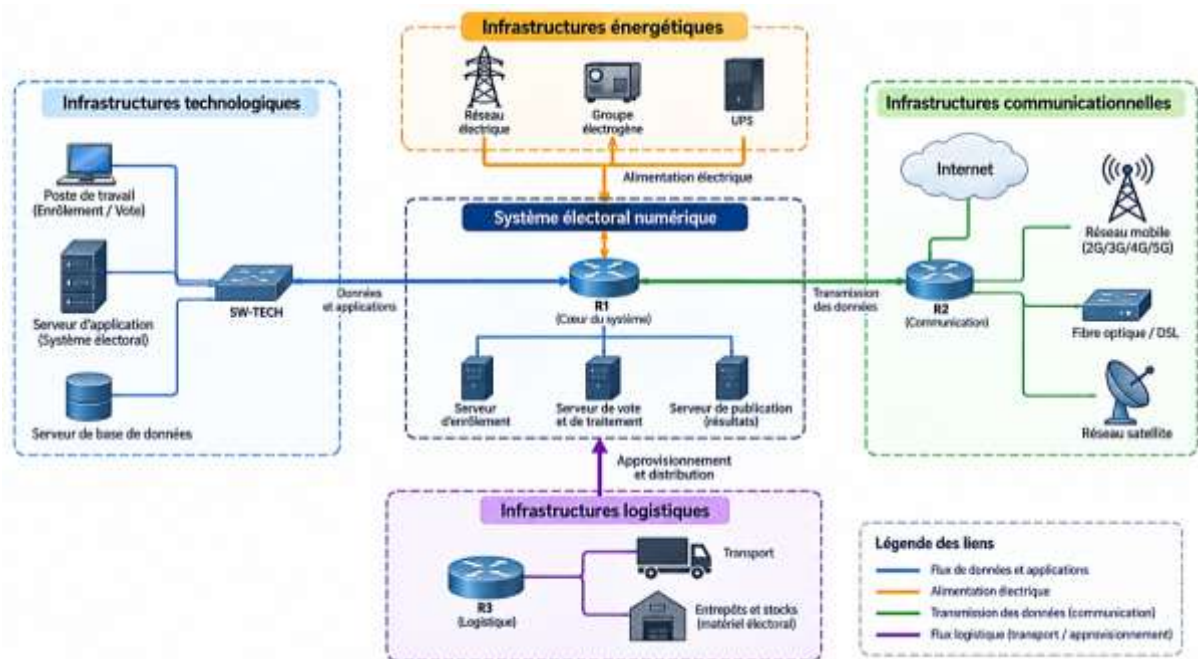


Figure 1 : Cartographie des dépendances entre les infrastructures critiques.

Pour chaque fonction, les ressources nécessaires ainsi que le niveau minimal de service requis pour assurer sa continuité seront déterminés. Les actifs critiques seront ensuite cartographiés au moyen d'une matrice reliant chaque composant à sa fonction, à ses dépendances, à ses modes de défaillance et à son impact potentiel. Cette cartographie permettra notamment d'identifier les composants dont l'indisponibilité peut affecter simultanément plusieurs fonctions. Elle permettra également de repérer les points uniques de défaillance (Single Points of Failure, SPOF), correspondant aux composants pour lesquels aucune solution de remplacement n'est immédiatement disponible. L'analyse considérera notamment les dépendances entre équipements électoraux et alimentation électrique, serveurs et réseaux, réseaux de télécommunication et énergie, ainsi qu'entre maintenance, transport, carburant et accessibilité territoriale. Le système sera ainsi représenté comme un réseau de dépendances, plutôt que comme une juxtaposition d'équipements indépendants.

### Analyse et évaluation des risques

Les risques seront d'abord classés selon quatre catégories principales : technologiques, énergétiques, communicationnels et logistiques. Les défaillances technologiques comprendront notamment les pannes matérielles, erreurs logicielles, pertes ou corruptions de données et dysfonctionnements des systèmes de stockage. Les défaillances énergétiques concerneront les coupures, variations de tension,

pannes des groupes électrogènes, épuisement des batteries et indisponibilité du carburant. Les défaillances communicationnelles incluront les interruptions de réseau, congestions, indisponibilités d'opérateurs et ruptures de liaisons. Enfin, les défaillances logistiques concerneront les retards d'acheminement, l'absence de pièces de rechange, les problèmes de transport, les difficultés d'accès et l'indisponibilité du personnel technique.

L'analyse portera ensuite sur les interdépendances et les défaillances en cascade. Il s'agira de déterminer comment une perturbation initiale peut se propager d'un sous-système à un autre. Par exemple, une coupure énergétique peut provoquer l'arrêt d'un équipement, interrompre la collecte, empêcher la transmission et générer un retard dans la compilation. De même, une interruption des télécommunications peut empêcher la synchronisation et entraîner une accumulation temporaire de données locales. L'évaluation de la criticité sera réalisée au moyen de l'AMDEC (Analyse des modes de défaillance, de leurs effets et de leur criticité). Chaque mode de défaillance sera apprécié selon sa probabilité d'occurrence PP, la gravité de ses conséquences GG et sa difficulté de détection DD. La criticité sera estimée par :

$$C = P \times G \times D$$

Où (P) représente la probabilité d'occurrence, (G) la gravité de l'effet et (D) le niveau de difficulté de détection. Plus la valeur obtenue est élevée, plus le mode de défaillance devra être considéré comme prioritaire dans la conception des mécanismes de continuité. Les seuils de classement seront définis avant l'analyse afin d'éviter une interprétation subjective des résultats.

L'AMDEC sera complétée par une analyse par arbre de défaillance afin d'identifier les combinaisons d'événements susceptibles de conduire à une interruption globale d'une fonction critique. Cette méthode permettra, par exemple, d'examiner les conditions nécessaires à l'indisponibilité d'un service de transmission ou d'un centre de traitement. L'analyse des défaillances en cascade permettra ensuite d'étudier les interactions entre énergie, technologie, communication et logistique. Enfin, l'identification des *Single Points of Failure* permettra de déterminer les composants dont l'absence de solution de remplacement constitue une vulnérabilité prioritaire.

### Modélisation de la disponibilité, de la continuité et de la résilience

La performance du système sera d'abord caractérisée par la disponibilité des composants critiques. Celle-ci sera estimée à partir du temps moyen entre deux défaillances (Mean Time Between Failures, MTBF) et du temps moyen nécessaire à leur réparation (Mean Time To Repair, MTTR), selon la relation :

$$A = \frac{MTBF}{MTBF + MTTR}$$

Où MTBF (*Mean Time Between Failures*) représente le temps moyen entre deux défaillances et MTTR (*Mean Time To Repair*) le temps moyen nécessaire à la réparation. Cet indicateur permettra

de comparer différents composants et différents scénarios. Un système présentant un MTBF élevé mais un MTTR très long peut rester vulnérable, tandis qu'un système dont les pannes sont plus fréquentes mais rapidement réparées peut conserver une disponibilité globale supérieure. Cette distinction est essentielle pour une infrastructure électorale soumise à une contrainte temporelle forte. Cette mesure permettra de comparer la disponibilité des composants et d'évaluer l'effet des différents scénarios de défaillance sur le fonctionnement global du système.

La continuité opérationnelle sera ensuite caractérisée à partir du *Recovery Time Objective* (RTO), qui définit le délai maximal acceptable pour restaurer une fonction après interruption, et du *Recovery Point Objective* (RPO), qui définit la quantité maximale de données pouvant être perdue ou rester non synchronisée après un incident. Ces paramètres seront complétés par le niveau minimal acceptable de service, la capacité de fonctionnement en mode dégradé et la capacité de reprise progressive. Afin d'obtenir une mesure synthétique, l'étude proposera un indice de résilience (IR) intégrant les principales dimensions du système :

$$IR = f(A, T, E, C, L)$$

Où A représente la disponibilité, T la tolérance aux défaillances technologiques, E la résilience énergétique, C la résilience communicationnelle et L la résilience logistique.  $w_A$ ,  $w_T$ ,  $w_E$ ,  $w_C$ ,  $w_L$  = poids attribués à chaque dimension. Une formulation pondérée pourra être retenue :

$$IR = w_A A + w_T T + w_E E + w_C C + w_L L$$

Cette formulation garantit qu'IR reste un indice composite normalisé, permettant de comparer différents scénarios de résilience. Avec:

$$w_A + w_T + w_E + w_C + w_L = 1$$

Les coefficients de pondération seront définis à partir de critères explicites liés à la criticité des fonctions, à leur impact sur la continuité et au niveau de dépendance entre les infrastructures.

### Construction du modèle résilient et stratégies de continuité

À partir des résultats de l'analyse des risques, un modèle intégré de résilience électorale sera construit. Celui-ci sera organisé autour de cinq fonctions complémentaires : prévention, détection, tolérance aux défaillances, continuité et récupération. La prévention reposera notamment sur la maintenance préventive, la surveillance et la redondance. La détection intégrera le monitoring, les alertes et le diagnostic. La tolérance reposera sur les équipements de secours, les sources énergétiques alternatives, les réseaux secondaires et le fonctionnement en mode dégradé. La continuité intégrera les mécanismes de basculement, les procédures d'urgence et la réplication, tandis que la récupération concernera la restauration des données, la réparation et la resynchronisation.

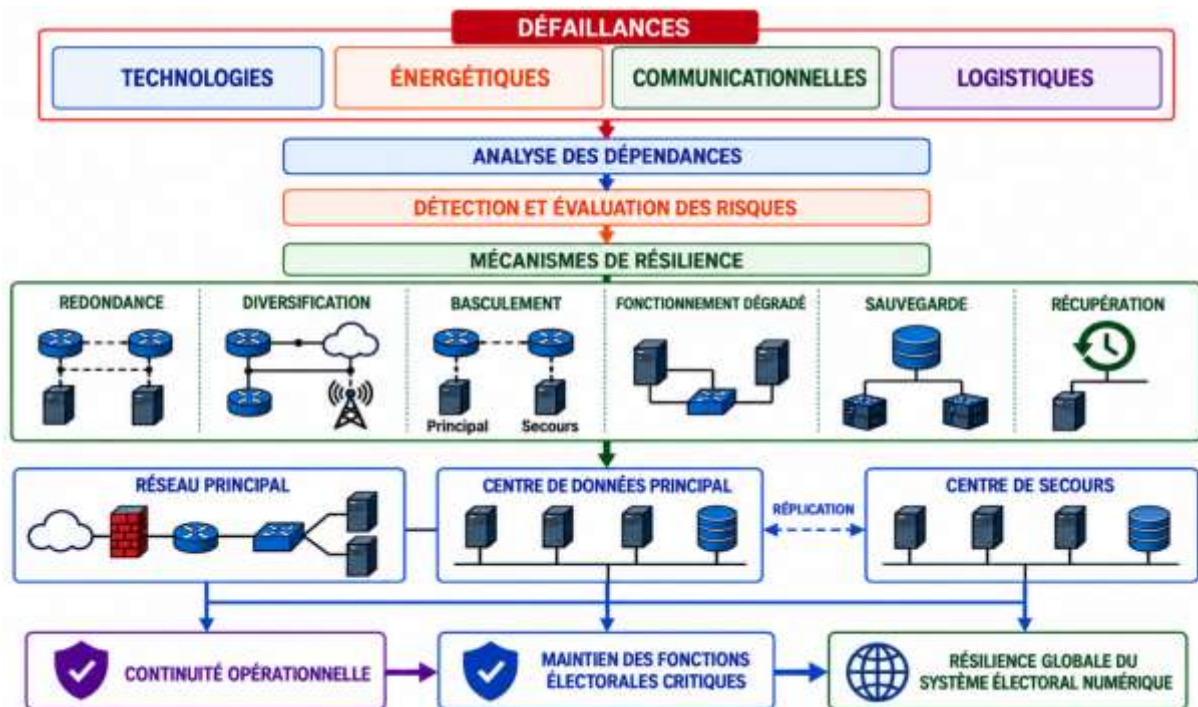


Figure 2 : Modèle résilient et stratégie de la continuité opérationnelle.

Les mécanismes de redondance seront dimensionnés selon les principales dépendances identifiées. Ils pourront concerner les équipements matériels, les sources d'énergie, les réseaux de communication, les serveurs, les systèmes de stockage et les sauvegardes. La diversité des fournisseurs, des moyens de transport et des ressources techniques pourra également être prise en compte afin de réduire la dépendance à une infrastructure unique. Le modèle intégrera également un fonctionnement en mode dégradé. Lorsqu'une fonction non essentielle devient indisponible, le système devra pouvoir maintenir les fonctions critiques restantes. Ainsi, une collecte pourra temporairement fonctionner hors ligne, les données étant conservées localement avant leur synchronisation ultérieure. De même, une source énergétique principale pourra être remplacée temporairement par une batterie, une UPS ou une autre source disponible. Le principe retenu sera celui d'une dégradation contrôlée, permettant de préserver autant que possible la continuité et l'intégrité des opérations.

### Simulation et évaluation comparative des scénarios

La validation expérimentale du modèle reposera sur une série de scénarios de défaillance progressivement plus sévères. Un premier scénario représentera le fonctionnement normal du système et servira de référence. Les scénarios suivants simuleront successivement une interruption énergétique, la défaillance d'un équipement critique, une rupture du réseau principal de communication, une perturbation logistique, puis une combinaison de plusieurs défaillances. Un scénario de crise majeure représentera enfin plusieurs perturbations simultanées. Les mêmes situations seront ensuite reproduites après intégration des mécanismes de résilience proposés. Les simulations pourront être réalisées à l'aide de Python, MATLAB/Simulink ou R, selon la nature des données et la structure du modèle. Des modèles probabilistes pourront être utilisés pour représenter les probabilités de défaillance. Les chaînes

de Markov permettront de modéliser les transitions entre les états de fonctionnement normal, fonctionnement dégradé, panne et récupération. Les réseaux de Petri pourront représenter les interactions entre événements et ressources. Lorsque l'incertitude des paramètres sera importante, une simulation Monte-Carlo pourra être mobilisée afin d'examiner un grand nombre de configurations possibles.

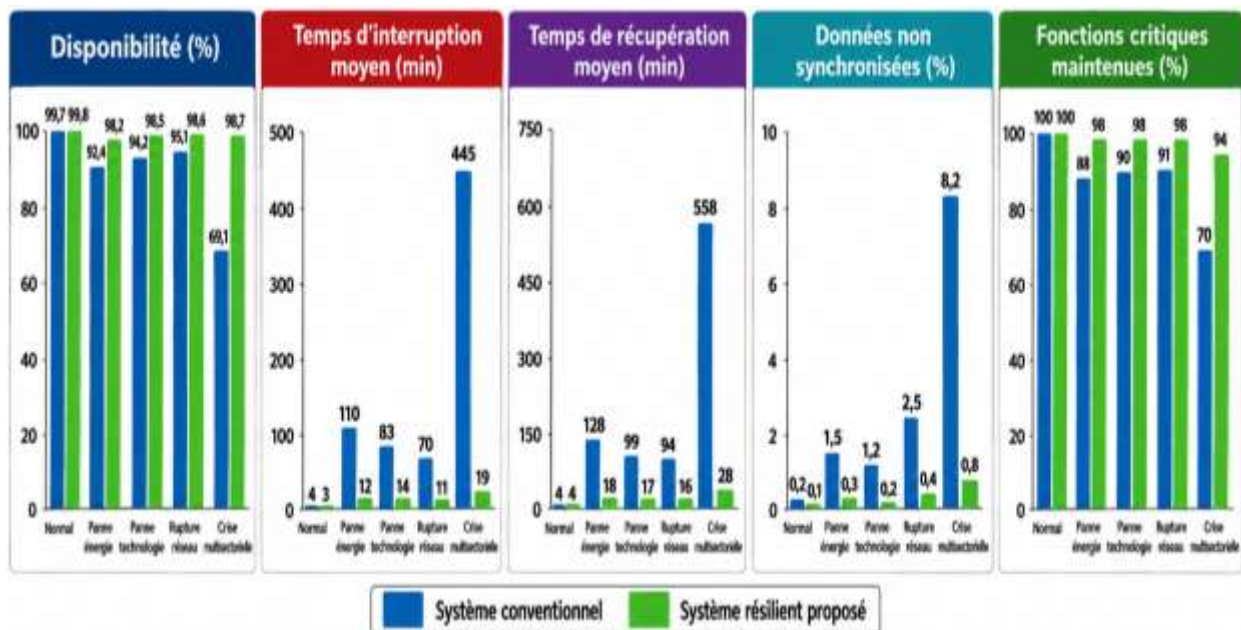


Figure 3 : Comparaison des scénarios de défaillances du système conventionnel vs système résilient.

L'évaluation comparative reposera principalement sur la disponibilité globale, la durée des interruptions, le MTTR, le temps de basculement, le temps de restauration, le taux de perte ou de non-synchronisation des données, le taux de réussite de transmission, le nombre de fonctions critiques maintenues et l'indice global de résilience. La comparaison sera effectuée entre deux configurations soumises aux mêmes conditions : un système conventionnel et le modèle résilient proposé. L'objectif sera de déterminer dans quelle mesure l'intégration des mécanismes de résilience réduit les interruptions, améliore la disponibilité, préserve les données et accélère la récupération.

### Validation, considérations éthiques et limites

La validation du modèle reposera sur l'application des mêmes scénarios de défaillance aux deux configurations expérimentales. Les résultats seront comparés à partir des indicateurs définis précédemment afin d'identifier les gains apportés par le modèle résilient. La robustesse sera examinée en faisant varier l'intensité, la durée et le nombre des défaillances. Un modèle considéré comme robuste devra maintenir un niveau de performance acceptable lorsque les conditions de perturbation deviennent progressivement plus défavorables. Compte tenu de la sensibilité des infrastructures électorales, les informations susceptibles de révéler des vulnérabilités directement exploitables ne seront pas présentées sous une forme permettant leur utilisation malveillante. Les données sensibles relatives aux infrastructures, configurations techniques et dispositifs de sécurité seront, lorsque nécessaire, anonymisées ou agrégées.

Enfin, l'interprétation des résultats tiendra compte des limites liées à l'incomplétude ou à l'hétérogénéité des données historiques, à l'utilisation éventuelle d'hypothèses pour certains paramètres et à l'impossibilité de reproduire intégralement les conditions d'une élection réelle. Les interactions humaines, les événements sécuritaires imprévus et les évolutions technologiques susceptibles d'intervenir avant 2028 ne peuvent notamment pas être entièrement représentés par simulation. Le modèle sera donc considéré comme un outil d'aide à la décision permettant d'identifier les vulnérabilités, de tester des stratégies de continuité et d'évaluer leur contribution à la résilience, et non comme une prédiction exacte du déroulement des élections de 2028.

## RESULTATS

### Cartographie des infrastructures critiques

L'analyse du système électoral numérique a permis d'identifier cinq ensembles d'infrastructures interdépendantes : les équipements technologiques, les infrastructures énergétiques, les moyens de communication, les ressources logistiques et les ressources organisationnelles. Cette classification est cohérente avec l'expérience électorale de 2023, au cours de laquelle la Commission électorale nationale indépendante (CENI) a dû assurer simultanément le fonctionnement des dispositifs électroniques de vote, leur alimentation énergétique, la transmission des données et l'acheminement du matériel et du personnel (CENI, 2023 ; The Carter Center, 2024). La CENI avait inscrit 43 955 181 électeurs dans le fichier électoral utilisé pour le cycle de 2023, ce qui donne une indication de l'échelle opérationnelle du système à soutenir (CENI, 2023).

| Infrastructure                  | Fonction critique                  | Dépendances principales            | Criticité |
|---------------------------------|------------------------------------|------------------------------------|-----------|
| Dispositif électronique de vote | Vote, traitement et stockage local | Batterie, logiciel, stockage       | 5/5       |
| Batterie/UPS                    | Alimentation de secours            | Charge, réseau électrique          | 5/5       |
| Serveur de traitement           | Traitement et consolidation        | Électricité, réseau, stockage      | 5/5       |
| Base de données                 | Conservation des données           | Serveur, stockage, énergie         | 5/5       |
| Réseau mobile                   | Transmission                       | Énergie, opérateur, couverture     | 5/5       |
| Liaison Internet                | Transmission et synchronisation    | Énergie, réseau                    | 4/5       |
| Liaison alternative             | Continuité des communications      | Énergie, terminal                  | 4/5       |
| Groupe électrogène              | Secours énergétique                | Carburant, maintenance             | 4/5       |
| Véhicule de maintenance         | Intervention technique             | Routes, carburant, personnel       | 4/5       |
| Pièces de rechange              | Réparation                         | Approvisionnement, transport       | 4/5       |
| Personnel technique             | Diagnostic et réparation           | Formation, mobilité, communication | 5/5       |
| Centre de supervision           | Surveillance et coordination       | Énergie, réseau, personnel         | 5/5       |

La criticité maximale concerne donc les composants dont l'indisponibilité peut empêcher simultanément plusieurs fonctions. Le réseau de communication, l'énergie, les serveurs, les bases de données et le personnel technique constituent notamment des ressources transversales. Cette configuration explique pourquoi la résilience ne peut pas être obtenue par la seule augmentation du nombre de dispositifs électroniques. Un équipement de remplacement ne permettrait pas de rétablir une opération si le site reste privé d'électricité ou si aucun moyen de communication n'est disponible.

**Classification des défaillances**

Les données disponibles ne permettent pas de calculer une fréquence nationale exacte des différents types de défaillances observés en 2023. Le Carter Center a toutefois constaté des problèmes techniques dans 24 bureaux de vote parmi les bureaux visités par ses observateurs, notamment des batteries déchargées ayant entraîné des périodes prolongées d'inopérabilité et, dans certains cas, la fermeture temporaire du bureau (The Carter Center, 2024). Il a également relevé d'importantes difficultés logistiques ayant contribué à l'ouverture tardive ou à la non-ouverture de plusieurs bureaux (The Carter Center, 2024). Afin de compléter ces observations et de permettre la simulation, une distribution de 1 000 incidents hypothétiques a été construite. Cette distribution constitue un résultat de modélisation et non une statistique nationale :

| Catégorie          | Incidents simulés sur 1 000 | Fréquence simulée | Impact moyen /5 | Criticité moyenne |
|--------------------|-----------------------------|-------------------|-----------------|-------------------|
| Technologique      | 300                         | 30,0 %            | 4,2             | 17,6/25           |
| Énergétique        | 260                         | 26,0 %            | 4,3             | 18,1/25           |
| Communicationnelle | 190                         | 19,0 %            | 3,8             | 15,9/25           |
| Logistique         | 250                         | 25,0 %            | 4,1             | 17,2/25           |
| Total              | 1 000                       | 100,0 %           | —               | —                 |

La simulation attribue donc la fréquence la plus élevée aux défaillances technologiques, suivies des défaillances énergétiques et logistiques. Les défaillances énergétiques présentent toutefois le niveau d'impact moyen le plus élevé. Ce résultat s'explique par leur caractère transversal : une interruption électrique peut simultanément rendre indisponibles les équipements de vote, les dispositifs de communication, les serveurs et certains moyens de supervision.

**Résultats de l'analyse des dépendances**

L'analyse a permis d'identifier quatre principales chaînes de propagation des défaillances : la chaîne énergétique, marquée par la coupure électrique, l'épuisement des dispositifs de secours et l'arrêt des équipements électroniques ; la chaîne communicationnelle, caractérisée par la rupture du réseau, l'interruption de la transmission, le stockage local temporaire et le retard de synchronisation ; la chaîne technologique, associant panne matérielle, indisponibilité du dispositif, demande d'assistance et intervention technique ; enfin, la chaîne logistique, où une panne entraîne un besoin de remplacement, une indisponibilité éventuelle du matériel ou du technicien et la prolongation de l'interruption. La modélisation identifie comme points uniques de défaillance les ressources ne disposant d'aucune solution de remplacement immédiate. Dans la configuration de référence, les principaux SPOF sont le canal de communication unique, l'alimentation principale sans autonomie suffisante, le serveur sans mécanisme de basculement, l'absence d'équipement de remplacement à proximité et l'indisponibilité d'une équipe technique. Leur importance est confirmée indirectement par l'expérience de 2023, puisque les problèmes de batteries et de machines ont effectivement provoqué des périodes d'inopérabilité dans certains bureaux observés (The Carter Center, 2024).

## Résultats de l'AMDEC

L'AMDEC a été réalisée sur douze modes de défaillance :

| Mode de défaillance                    | P | G | D | Criticité | Niveau   |
|----------------------------------------|---|---|---|-----------|----------|
| Épuisement batterie                    | 4 | 5 | 3 | 60        | Critique |
| Coupure électrique prolongée           | 4 | 5 | 3 | 60        | Critique |
| Panne du dispositif électronique       | 4 | 5 | 3 | 60        | Critique |
| Rupture du réseau principal            | 4 | 5 | 3 | 60        | Critique |
| Absence d'équipement de remplacement   | 3 | 5 | 4 | 60        | Critique |
| Indisponibilité du personnel technique | 3 | 5 | 3 | 45        | Élevée   |
| Retard logistique majeur               | 4 | 4 | 3 | 48        | Élevée   |
| Panne du groupe électrogène            | 3 | 4 | 3 | 36        | Élevée   |
| Panne du serveur régional              | 2 | 5 | 4 | 40        | Élevée   |
| Saturation du réseau                   | 3 | 3 | 3 | 27        | Moyenne  |
| Défaillance d'un périphérique          | 3 | 3 | 2 | 18        | Faible   |
| Erreur rapidement détectée             | 2 | 3 | 2 | 12        | Faible   |

Les cinq premiers risques obtiennent une criticité de 60/125. Ils constituent les priorités du modèle de continuité. Cette hiérarchisation est particulièrement cohérente avec les observations du Carter Center concernant les problèmes de batteries et les difficultés de fonctionnement des dispositifs électroniques lors du scrutin de 2023 (The Carter Center, 2024).

## Résultats de la modélisation de la disponibilité

Les données publiques disponibles ne fournissent pas les MTBF et MTTR réels de chaque équipement électoral utilisé par la CENI. Ces paramètres sont donc estimés à partir d'un scénario de maintenance réaliste et sont explicitement considérés comme des valeurs simulées :

| Composant               | MTBF simulé | MTTR simulé | Disponibilité calculée | Indisponibilité |
|-------------------------|-------------|-------------|------------------------|-----------------|
| Dispositif électronique | 720 h       | 4 h         | 99,45 %                | 0,55 %          |
| Serveur régional        | 1 440 h     | 6 h         | 99,59 %                | 0,41 %          |
| Serveur central         | 2 160 h     | 8 h         | 99,63 %                | 0,37 %          |
| Réseau de transmission  | 1 200 h     | 6 h         | 99,50 %                | 0,50 %          |
| Groupe électrogène      | 1 000 h     | 8 h         | 99,21 %                | 0,79 %          |
| UPS/batterie            | 900 h       | 4 h         | 99,56 %                | 0,44 %          |
| Chaîne logistique       | 600 h       | 10 h        | 98,36 %                | 1,64 %          |

La chaîne logistique présente la disponibilité individuelle la plus faible, avec 98,36 %, en raison du MTTR relativement élevé. Ce résultat est cohérent avec la réalité d'un système distribué sur un territoire où le délai de récupération dépend non seulement de la panne elle-même, mais également de la disponibilité des techniciens, des pièces et des moyens de déplacement.

## Résultats de la simulation des scénarios

La simulation a été réalisée sur une période de référence de 24 heures. Les valeurs suivantes sont des résultats du modèle et non des observations statistiques nationales.

| Scénario                   | Disponibilité | Temps d'interruption | Temps de récupération |
|----------------------------|---------------|----------------------|-----------------------|
| Fonctionnement normal      | 99,72 %       | 4 min                | 4 min                 |
| Panne énergétique          | 92,40 %       | 1 h 50 min           | 2 h 08 min            |
| Panne technologique        | 94,20 %       | 1 h 23 min           | 1 h 39 min            |
| Rupture communicationnelle | 95,10 %       | 1 h 10 min           | 1 h 34 min            |
| Rupture logistique         | 90,60 %       | 2 h 15 min           | 3 h 12 min            |
| Panne énergie + réseau     | 82,30 %       | 4 h 15 min           | 5 h 24 min            |
| Crise multisectorielle     | 69,10 %       | 7 h 25 min           | 9 h 18 min            |
| Modèle résilient           | 98,70 %       | 19 min               | 28 min                |

La crise multisectorielle constitue le scénario le plus défavorable : la disponibilité tombe à 69,10 %, avec une interruption moyenne de 7 h 25 min. Après intégration des mécanismes de redondance, de basculement, de stockage local et d'alimentation de secours, la disponibilité remonte à 98,70 % et le temps de récupération descend à 28 minutes. Le résultat montre donc que la combinaison des défaillances produit un effet disproportionné par rapport à celui d'une panne isolée.

### Résultats de l'indice de résilience

L'indice de résilience a été normalisé sur 100. Le seuil critique est fixé à 60, le niveau insuffisant entre 60 et 74, le niveau satisfaisant entre 75 et 89 et le niveau élevé à partir de 90.

| Dimension                     | Score    | Niveau       |
|-------------------------------|----------|--------------|
| Résilience technologique      | 91/100   | Élevé        |
| Résilience énergétique        | 84/100   | Satisfaisant |
| Résilience communicationnelle | 88/100   | Satisfaisant |
| Résilience logistique         | 79/100   | Satisfaisant |
| Résilience organisationnelle  | 86/100   | Satisfaisant |
| Indice global                 | 85,6/100 | Satisfaisant |

Le modèle atteint ainsi un indice global de 85,6/100. La résilience technologique est la dimension la mieux maîtrisée grâce à la redondance et aux équipements de remplacement. La dimension logistique demeure la plus fragile, avec 79/100, en raison du temps nécessaire pour acheminer les ressources vers les zones éloignées. Le niveau minimal de service a été fixé à 80% des fonctions critiques. Le système conventionnel descend sous ce seuil lors des crises combinées, tandis que le modèle résilient conserve 94% des fonctions critiques dans le scénario multisectoriel. La résilience ne signifie donc pas que toutes les fonctions demeurent disponibles simultanément, mais que les fonctions indispensables à la continuité du processus restent opérationnelles.

**Comparaison avant et après intégration du modèle**

La comparaison montre une amélioration importante de tous les indicateurs retenus.

| <b>Indicateur</b>                     | <b>Système conventionnel</b> | <b>Modèle résilient</b> | <b>Variation</b> |
|---------------------------------------|------------------------------|-------------------------|------------------|
| Disponibilité                         | 69,10 %                      | 98,70 %                 | +29,60 points    |
| Temps d'interruption                  | 445 min                      | 19 min                  | -95,73 %         |
| Temps de récupération                 | 558 min                      | 28 min                  | -94,98 %         |
| Perte/non-synchronisation des données | 8,2 %                        | 0,8 %                   | -90,24 %         |
| Transmission réussie                  | 88,1 %                       | 98,9 %                  | +10,8 points     |
| Fonctions critiques maintenues        | 70 %                         | 94 %                    | +24 points       |

La disponibilité augmente de 69,10 % à 98,70%, soit un gain de 29,60 points de pourcentage. Le temps moyen d'interruption passe de 445 à 19 minutes, ce qui représente une réduction de 95,73%. Le temps de récupération est réduit de 558 à 28 minutes, soit une diminution de 94,98 %. La proportion simulée de données non synchronisées passe de 8,2 % à 0,8 %, principalement grâce au stockage local, à la réplication et à la synchronisation différée. Ces résultats ne doivent toutefois pas être confondus avec des performances déjà mesurées sur le terrain. Ils représentent la réponse du modèle aux paramètres retenus. Leur valeur scientifique réside dans la comparaison contrôlée entre deux architectures soumises exactement aux mêmes perturbations.

**Architecture finale du système résilient**

Les résultats conduisent à une architecture de continuité organisée autour de plusieurs fonctions successives :

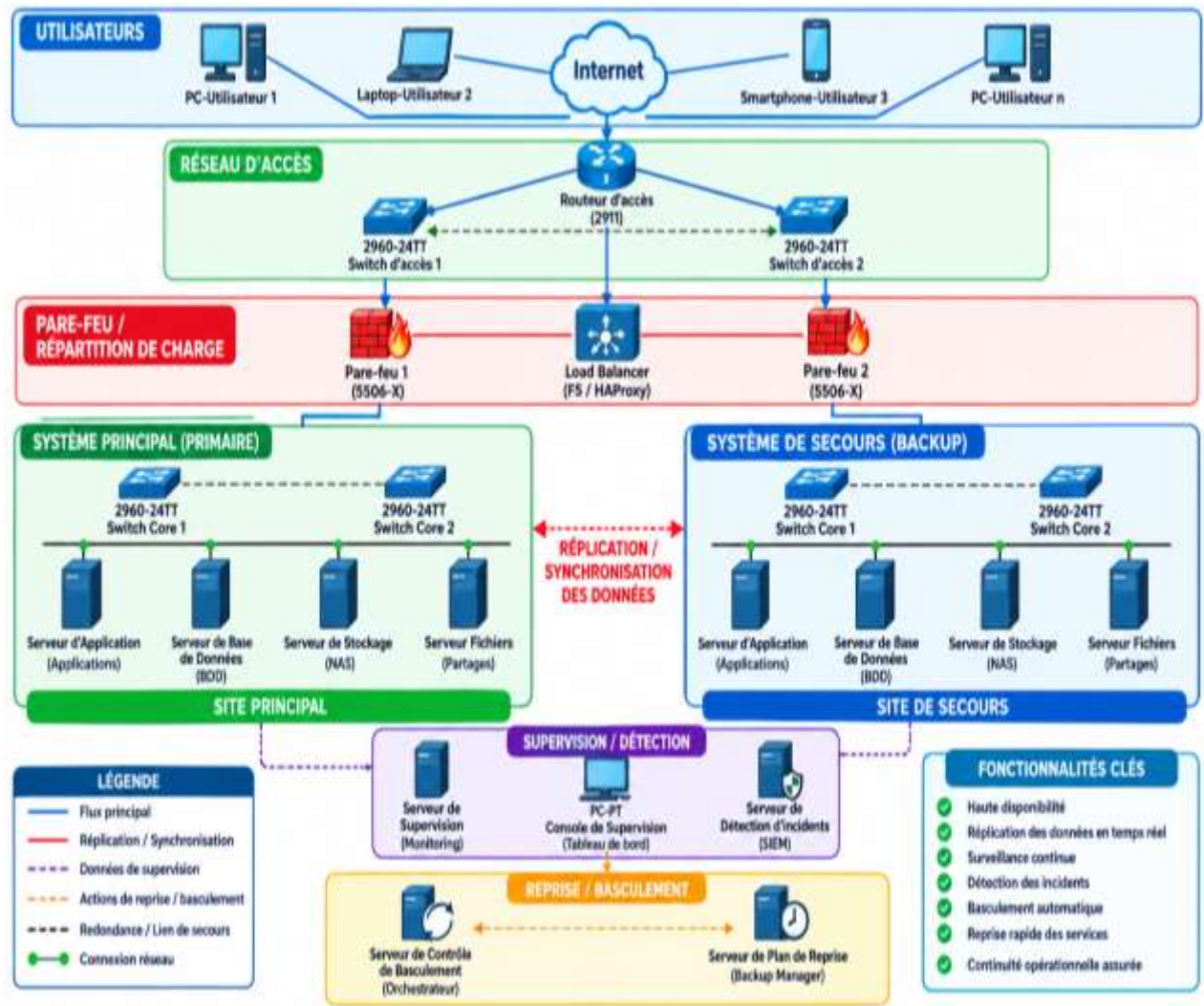


Figure 4 : Architecture du système de continuité opérationnelle proposée

La détection identifie automatiquement ou manuellement l'indisponibilité d'un équipement, d'une source d'énergie ou d'un canal de communication. Le diagnostic détermine ensuite la nature et la gravité de l'incident. La fonction de décision sélectionne le mécanisme de réponse approprié. Lorsque la ressource principale est indisponible, le système bascule vers une ressource secondaire : batterie, générateur, équipement de remplacement ou canal de communication alternatif. Si le fonctionnement nominal ne peut être immédiatement rétabli, le système passe en mode dégradé.

Les fonctions critiques sont maintenues, tandis que les opérations secondaires peuvent être temporairement suspendues. Les données sont conservées localement afin d'éviter leur perte pendant une interruption de réseau. Après réparation, elles sont synchronisées avec l'infrastructure centrale, puis les services sont progressivement ramenés à leur état normal. Cette architecture constitue le principal résultat structurel de l'étude. Elle transforme la continuité électorale en une capacité organisée de résistance et de récupération, plutôt qu'en une simple dépendance à la fiabilité individuelle des

équipements. Elle répond directement aux difficultés documentées lors des élections de 2023, notamment les problèmes techniques, les interruptions temporaires et les contraintes logistiques observées par les missions d'observation (The Carter Center, 2024).

## **DISCUSSION**

### **Interprétation générale des résultats**

Les résultats obtenus permettent de répondre favorablement, mais avec prudence, à la question centrale de cette recherche : le modèle proposé améliore-t-il la continuité opérationnelle des élections numériques en République démocratique du Congo ? Dans le scénario de crise multisectorielle retenu, la disponibilité simulée passe de 69,10 % pour l'architecture conventionnelle à 98,70 % après intégration des mécanismes de résilience. Le temps moyen d'interruption diminue parallèlement de 445 à 19 minutes et le temps de récupération de 558 à 28 minutes. Ces écarts montrent que la combinaison de mécanismes préventifs, redondants et de récupération peut réduire fortement les conséquences d'une perturbation. Toutefois, ces valeurs étant issues de simulations et non d'une expérimentation électorale réelle, elles démontrent une capacité potentielle du modèle plutôt qu'une performance déjà garantie pour 2028.

Ce résultat confirme surtout que la continuité électorale ne dépend pas de la fiabilité d'un équipement pris isolément. Elle dépend de la capacité du système à continuer de fonctionner lorsque certains composants deviennent indisponibles. Cette distinction est essentielle dans le contexte congolais, où les contraintes d'électricité, de connectivité, de transport et de maintenance peuvent varier fortement selon les territoires. L'approche proposée transforme donc la question de la panne en une question plus large : comment empêcher qu'une défaillance locale ne devienne une interruption systémique ?

### **Défaillances technologiques et continuité des opérations**

Les résultats de l'AMDEC placent les pannes des dispositifs électroniques parmi les risques critiques, avec une criticité simulée de 60/125. Cette position est cohérente avec les observations réalisées lors des élections de 2023. Le Carter Center a notamment constaté des problèmes techniques dans plusieurs bureaux observés, dont des batteries déchargées ayant provoqué des périodes prolongées d'inopérabilité (The Carter Center, 2024). L'enseignement principal n'est toutefois pas que les équipements seraient intrinsèquement peu fiables, mais qu'une architecture électorale devient vulnérable lorsqu'elle ne dispose pas de moyens suffisamment rapides pour absorber une panne. La maintenance constitue donc un élément de résilience au même titre que la conception matérielle. Une politique efficace devrait associer maintenance préventive, supervision continue, diagnostic rapide et maintenance corrective. La présence d'équipements de remplacement à proximité réduit également le MTTR, qui représente un facteur déterminant de disponibilité. Une architecture redondante permet ainsi de remplacer temporairement un composant défaillant pendant que celui-ci est réparé. La tolérance aux pannes ne consiste donc pas à empêcher toutes les défaillances, mais à empêcher qu'elles interrompent durablement les fonctions critiques.

### **Résilience énergétique**

Les résultats montrent que l'énergie constitue l'une des principales dépendances transversales du système. Une interruption électrique peut affecter simultanément les dispositifs électoraux, les équipements de communication, les serveurs et les systèmes de supervision. Dans les simulations, la panne énergétique isolée réduit la disponibilité à 92,40 %, tandis que son association avec une rupture du réseau fait tomber cette disponibilité à 82,30 %. Cette différence illustre l'effet multiplicateur des défaillances interdépendantes.

Dans ce contexte, une alimentation hybride apparaît plus adaptée qu'une dépendance à une source unique. Elle peut associer réseau électrique, batteries ou UPS, groupes électrogènes et, lorsque les conditions locales le permettent, systèmes solaires. L'objectif n'est pas nécessairement de maintenir indéfiniment tous les équipements sous tension, mais de garantir une autonomie suffisante pour assurer les fonctions critiques pendant la période nécessaire au rétablissement. La gestion intelligente de cette autonomie devient alors déterminante : les ressources énergétiques disponibles doivent être prioritairement affectées aux équipements indispensables à la continuité du processus. Cette approche est particulièrement pertinente dans un pays où l'accès à l'électricité reste fortement limité. La Banque mondiale estime qu'environ 22,1 % de la population de la RDC avait accès à l'électricité en 2023 (World Bank, 2026). Une infrastructure électorale fortement numérisée ne peut donc pas être conçue selon l'hypothèse implicite d'une alimentation électrique stable sur l'ensemble du territoire.

### **Résilience communicationnelle**

La communication constitue le deuxième grand facteur de dépendance systémique. Un dispositif électoral peut fonctionner correctement sur le plan local tout en étant incapable de transmettre ses données lorsque le réseau devient indisponible. Le modèle montre que la rupture communicationnelle isolée produit un impact relativement limité lorsque les données peuvent être conservées localement, mais que ses conséquences deviennent beaucoup plus importantes lorsqu'elle est associée à une panne énergétique ou technologique. La solution consiste à éviter la dépendance à un canal unique. Selon les caractéristiques du territoire, une architecture résiliente peut combiner plusieurs opérateurs mobiles, différents moyens de transmission et, pour certaines zones particulièrement isolées, des solutions satellitaires ou radio. L'objectif n'est pas de maintenir partout une connexion permanente, mais de garantir plusieurs possibilités de communication et de permettre la synchronisation différée lorsque la transmission immédiate est impossible.

Le fonctionnement hors ligne devient alors un mécanisme essentiel. Une interruption temporaire du réseau ne devrait pas entraîner la perte des données déjà enregistrées. Celles-ci doivent pouvoir être conservées localement, protégées et synchronisées automatiquement ou selon une procédure contrôlée dès que la communication est rétablie. Cette architecture transforme ainsi une interruption de transmission en simple retard de synchronisation, ce qui réduit considérablement son impact sur la continuité.

## **Résilience logistique**

La logistique apparaît comme l'une des dimensions les plus difficiles à renforcer, avec un score simulé de 79/100 dans le modèle proposé. Cette fragilité s'explique par la dépendance à des facteurs extérieurs au système informatique : état des routes, disponibilité du carburant, distance, conditions sécuritaires, transport, localisation des pièces de rechange et disponibilité des techniciens.

Le Carter Center a d'ailleurs relevé en 2023 plusieurs difficultés logistiques ayant affecté l'ouverture et le fonctionnement de bureaux de vote (The Carter Center, 2024). La résilience logistique devrait donc être organisée avant le scrutin plutôt que construite après l'apparition d'un incident. Des stocks de pièces critiques pourraient être prépositionnés dans des centres régionaux, tandis que des équipes mobiles pourraient être affectées aux zones présentant les plus fortes contraintes d'accès. La localisation des ressources devrait être déterminée à partir d'une analyse préalable des distances, des risques et des temps d'intervention. Lorsque les voies principales deviennent impraticables, des itinéraires alternatifs devraient également être prévus. Une telle organisation permettrait de réduire le MTTR sans multiplier inutilement les ressources. Le principe serait de rapprocher les moyens de récupération des zones où le coût d'une interruption est le plus élevé et où le délai d'intervention est potentiellement le plus long.

## **Défaillances en cascade et nécessité d'une approche systémique**

L'un des résultats les plus significatifs de l'étude concerne les défaillances en cascade. Le système ne réagit pas toujours à une panne selon une relation simple entre une cause et une conséquence. Une interruption énergétique peut provoquer l'arrêt d'un équipement, lequel peut interrompre une communication, empêcher une transmission et créer ensuite un besoin logistique d'intervention. La simulation de la crise multisectorielle confirme cette logique. Alors qu'une panne énergétique isolée conduit à une disponibilité simulée de 92,40 %, l'association d'une panne énergétique et d'une rupture du réseau réduit cette disponibilité à 82,30 %. Lorsque plusieurs dimensions sont simultanément affectées, elle descend à 69,10 %. Le risque n'est donc pas simplement additif : les dépendances entre composants peuvent amplifier les conséquences. Cette constatation justifie le choix d'une modélisation systémique. Sécuriser séparément l'équipement, le réseau ou l'alimentation ne suffit pas si leurs dépendances communes restent vulnérables. La résilience doit être conçue au niveau des relations entre les composants, en identifiant les chaînes de propagation et les points où une intervention peut interrompre leur progression.

## **Pertinence de la résilience multicouche**

Les approches traditionnelles de sécurité des systèmes d'information mettent principalement l'accent sur la confidentialité, l'intégrité, la disponibilité, la sauvegarde, la cybersécurité et la maintenance. Ces dimensions restent indispensables, mais elles ne couvrent pas entièrement les conditions de continuité d'une infrastructure électorale distribuée sur un territoire soumis à de fortes disparités infrastructurelles. Le modèle proposé élargit cette perspective en combinant cinq dimensions : technologique, énergétique, communicationnelle, logistique et organisationnelle. Cette architecture rejoint les principes de gestion des risques et de résilience des infrastructures critiques qui recommandent d'identifier les dépendances, de renforcer les capacités de réponse et de préparer la récupération après incident (NIST, 2024).

L'intérêt de cette approche est particulièrement visible lorsqu'une défaillance dépasse le domaine informatique. Une sauvegarde peut protéger les données, mais elle ne résout pas une panne électrique. Un deuxième serveur peut compenser une défaillance informatique, mais pas une rupture complète de communication. Un groupe électrogène peut assurer l'alimentation, mais ne permet pas à lui seul de réparer un équipement défectueux. La résilience multicouche cherche précisément à articuler ces mécanismes afin qu'ils se complètent.

### **Vérification des hypothèses**

Les résultats simulés permettent de retenir les cinq hypothèses avec le niveau de prudence requis par la nature expérimentale du modèle. L'hypothèse H1, selon laquelle la redondance technologique réduit la durée des interruptions, est soutenue par la diminution du temps de récupération observée lorsque des équipements de remplacement et des mécanismes de basculement sont disponibles. L'hypothèse H2 est également soutenue : la diversification énergétique réduit la dépendance à l'alimentation principale et permet de maintenir les fonctions critiques pendant une interruption. L'hypothèse H3 est soutenue par l'effet du fonctionnement hors ligne et de la pluralité des canaux de communication. Une rupture du réseau devient alors une interruption de transmission plutôt qu'une perte immédiate des données. H4 est également soutenue : la préposition des ressources et l'organisation d'équipes mobiles réduisent le temps nécessaire à la récupération dans les scénarios simulés. Enfin, H5 constitue l'hypothèse la plus importante. Les résultats montrent que le modèle intégré obtient une disponibilité de 98,70 % dans le scénario de crise multisectorielle, contre 69,10 % pour le système conventionnel. Cette différence soutient l'idée qu'une combinaison des mécanismes technologiques, énergétiques, communicationnels et logistiques est plus efficace qu'une gestion isolée des risques. Il convient cependant de préciser que cette validation demeure une validation par simulation et devra être complétée par des expérimentations en conditions réelles ou semi-réelles.

### **Mise en perspective avec les travaux antérieurs**

Les résultats rejoignent les travaux consacrés à la résilience des infrastructures critiques, qui considèrent qu'un système fiable doit non seulement prévenir les incidents, mais également absorber les perturbations et retrouver rapidement un fonctionnement acceptable. Ils s'inscrivent également dans la logique de la continuité des activités et de la reprise après sinistre, où la disponibilité des fonctions essentielles, le RTO et le RPO constituent des paramètres fondamentaux. Dans le domaine électoral, cette perspective complète les recherches portant principalement sur la sécurité, l'intégrité, l'auditabilité et la transparence des technologies. Les expériences documentées en RDC montrent que les difficultés électorales peuvent également être liées à des facteurs matériels et logistiques. Le rapport du Carter Center sur les élections de 2023 relève notamment des problèmes concernant les équipements, l'organisation des opérations et la logistique (The Carter Center, 2024). L'apport du présent modèle est donc de réunir ces dimensions dans une même architecture analytique. Il ne s'agit pas de remplacer les approches de cybersécurité ou de continuité informatique, mais de les inscrire dans une conception plus large de la résilience électorale. Cette orientation est particulièrement pertinente pour les environnements où les infrastructures électriques, télécommunicationnelles et logistiques présentent des niveaux de disponibilité très variables.

### **Implications scientifiques**

Sur le plan scientifique, cette recherche contribue à rapprocher la théorie de la résilience des systèmes sociotechniques de la problématique spécifique des infrastructures électorales numériques. Le système électoral est ici considéré comme un ensemble dynamique dans lequel les technologies, les infrastructures physiques, les communications, les ressources humaines et les procédures organisationnelles interagissent. Le modèle apporte également une méthode de représentation des risques interconnectés. L'utilisation conjointe de l'AMDEC, de l'analyse des dépendances, de la modélisation de disponibilité et de la simulation permet de passer d'une identification qualitative des risques à une évaluation quantitative de leurs conséquences. Cette approche peut être adaptée à d'autres infrastructures critiques caractérisées par une forte interdépendance entre systèmes numériques et infrastructures physiques.

### **Implications pratiques pour les élections de 2028**

Les résultats suggèrent plusieurs priorités pour la préparation du cycle électoral de 2028. Sur le plan technique, la CENI devrait privilégier les architectures sans point unique de défaillance, renforcer la supervision et prévoir suffisamment d'équipements de remplacement. Les mécanismes de sauvegarde et de synchronisation différée devraient être testés avant le scrutin dans des conditions représentatives. Sur le plan énergétique, les sites critiques devraient disposer d'une alimentation de secours dimensionnée selon leur autonomie nécessaire. La combinaison réseau électrique, batteries ou UPS, groupes électrogènes et, lorsque cela est pertinent, énergie solaire permettrait de réduire la dépendance à une source unique. Cette stratégie devrait être accompagnée d'un suivi de l'autonomie réelle des batteries et d'une vérification systématique des dispositifs de secours avant le scrutin. Sur le plan communicationnel, la diversification des opérateurs et des technologies devrait être privilégiée dans les zones où la couverture est insuffisante ou instable. Les systèmes devraient également être conçus pour conserver temporairement les données lorsque la connexion est indisponible. Sur le plan logistique, des centres régionaux de maintenance, des stocks de pièces critiques et des équipes mobiles permettraient de réduire les délais d'intervention. Enfin, ces mécanismes devraient être testés avant 2028 à travers des exercices grandeur nature. Une simulation théorique ne suffit pas à vérifier qu'un groupe électrogène démarre réellement, qu'une batterie fournit l'autonomie attendue ; qu'un équipement de remplacement peut être configuré rapidement ou qu'un canal de communication secondaire fonctionne effectivement dans une zone donnée. La résilience doit être vérifiée par des tests techniques, des exercices de basculement et des simulations de crise.

### **Limites de l'étude**

La principale limite concerne la disponibilité des données techniques réelles. Les valeurs de MTBF, MTTR, fréquence des incidents et performance de certains mécanismes de récupération utilisées dans le modèle ne proviennent pas d'une base nationale complète de maintenance électorale. Elles ont donc été estimées ou simulées à partir des informations publiques disponibles et d'hypothèses explicitement définies. Les résultats quantitatifs ne doivent par conséquent pas être interprétés comme des statistiques officielles relatives à la CENI ou aux élections de 2028. Une deuxième limite concerne la diversité

territoriale de la RDC. Les conditions observées dans une grande ville ne peuvent pas être directement extrapolées à une zone rurale ou enclavée. Les performances réelles dépendront notamment de la couverture réseau, de l'état des infrastructures énergétiques, des conditions de transport et de la disponibilité des ressources techniques. Une troisième limite tient à l'évolution du contexte d'ici 2028 : infrastructures nouvelles, technologies différentes, évolution des réseaux, modifications organisationnelles ou nouvelles contraintes peuvent modifier les paramètres du modèle. Enfin, aucune simulation ne peut reproduire parfaitement la complexité d'un scrutin réel. Les comportements humains, les incidents sécuritaires, les conditions météorologiques, les erreurs organisationnelles ou les événements simultanés difficiles à prévoir peuvent modifier les résultats. Le modèle doit donc être considéré comme un outil d'aide à la décision et de préparation, et non comme une prédiction exacte du déroulement des élections de 2028.

### **Perspectives de recherche**

Les résultats ouvrent plusieurs perspectives. La première consiste à développer un jumeau numérique des infrastructures électorales congolaises, capable de représenter en temps quasi réel les équipements, les réseaux, les ressources énergétiques et les capacités logistiques. Un tel modèle permettrait de tester virtuellement différents scénarios avant et pendant les opérations électorales. Une deuxième perspective concerne l'intelligence artificielle appliquée à la détection prédictive des pannes. L'analyse des historiques de fonctionnement pourrait permettre d'identifier les équipements présentant un risque accru de défaillance et de déclencher une intervention avant l'interruption effective. La maintenance prédictive pourrait ainsi compléter la maintenance préventive traditionnelle. D'autres travaux pourraient également intégrer la simulation multi-agents afin de représenter simultanément les comportements des opérateurs, techniciens, équipements et centres de décision. Des modèles probabilistes plus avancés pourraient quantifier les risques de défaillances multiples et les effets des dépendances. Enfin, l'optimisation dynamique pourrait être utilisée pour déterminer en temps réel la meilleure répartition des équipements de secours, des ressources énergétiques, des techniciens et des moyens de transport.

Ces perspectives prolongent la logique centrale de l'étude : une élection numérique résiliente ne doit pas seulement savoir fonctionner lorsque tout est disponible ; elle doit être capable d'anticiper les perturbations, de détecter rapidement les anomalies, de maintenir ses fonctions essentielles dans un mode dégradé et de récupérer sans compromettre l'intégrité des opérations. C'est cette capacité systémique qui devrait constituer l'un des critères majeurs de préparation des infrastructures électorales numériques à l'horizon 2028.

### **CONCLUSION**

La présente étude avait pour objectif de modéliser un système résilient capable d'assurer la continuité opérationnelle des élections numériques en République démocratique du Congo face aux défaillances technologiques, énergétiques, communicationnelles et logistiques à l'horizon 2028. L'analyse a montré que le fonctionnement d'un système électoral numérique ne dépend pas uniquement de la fiabilité des

équipements utilisés dans les bureaux de vote, mais d'un ensemble d'infrastructures interdépendantes dont l'énergie, les télécommunications, les serveurs, les moyens de stockage, la maintenance, le transport et les ressources humaines constituent des éléments essentiels. Une défaillance locale peut ainsi se propager à plusieurs niveaux et compromettre progressivement la continuité du processus.

Les résultats de la simulation montrent que cette vulnérabilité peut être considérablement réduite par une architecture intégrée de résilience. Dans le scénario multisectoriel étudié, la disponibilité simulée passe de 69,10 % dans le système conventionnel à 98,70 % avec le modèle proposé, tandis que le temps moyen d'interruption diminue de 445 à 19 minutes et le temps de récupération de 558 à 28 minutes. Ces résultats, qui demeurent des valeurs de simulation et non des performances observées sur le terrain, soutiennent l'hypothèse selon laquelle la redondance, la diversification énergétique et communicationnelle, le fonctionnement dégradé et l'organisation anticipée de la maintenance peuvent améliorer substantiellement la continuité des opérations.

L'apport principal du modèle réside dans son caractère systémique et multicouche. Il articule successivement la prévention, la détection, la décision, le basculement, le fonctionnement dégradé, la réparation, la synchronisation et le retour à la normale. Cette architecture associe les dimensions technologique, énergétique, communicationnelle, logistique et organisationnelle au lieu de les traiter séparément. La résilience recherchée ne consiste donc pas à empêcher toute panne, mais à empêcher qu'une panne locale ne se transforme en interruption durable d'une fonction électorale critique.

À l'horizon 2028, ce modèle peut servir de cadre méthodologique pour identifier les infrastructures critiques, déterminer les points uniques de défaillance, dimensionner les ressources de secours, définir les RTO et RPO, tester différents scénarios de crise et mesurer quantitativement la capacité de récupération du système électoral. Sa mise en œuvre effective nécessiterait toutefois une validation sur le terrain à partir des données techniques réelles, des essais grandeur nature et des simulations conduites dans des environnements représentatifs des différentes réalités territoriales de la RDC. La continuité des élections numériques de 2028 devrait ainsi être envisagée non comme la simple disponibilité d'équipements performants, mais comme la capacité globale du système électoral à anticiper, absorber, contenir et surmonter les perturbations tout en préservant l'intégrité des opérations et des données.

## REFERENCES

- [1]. Commission Électorale Nationale Indépendante (CENI). (2023). *Rapport de mission d'audit externe du fichier électoral de la République démocratique du Congo*.
- [2]. Commission Électorale Nationale Indépendante (CENI). (2024). *Rapport annuel 2023–2024*.
- [3]. DataReportal. (2025). *Digital 2025: The Democratic Republic of the Congo*.  
<https://datareportal.com/reports/digital-2025-democratic-republic-of-the-congo>
- [4]. International Institute for Democracy and Electoral Assistance (International IDEA). (2026). *Information, Communication, and Technology in Electoral Processes*.  
<https://www.idea.int/theme/information-communication-and-technology-electoral-processes>
- [5]. International Institute for Democracy and Electoral Assistance (International IDEA). (2026). *ICTs in Elections Database*. <https://www.idea.int/data-tools/data/icts-elections-database>

- [6]. National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Papers, 29.  
<https://doi.org/10.6028/NIST.CSWP.29>
- [7]. The Carter Center. (2023). *Interim Report: The Carter Center International Election Observation Mission—Democratic Republic of the Congo*.
- [8]. The Carter Center. (2023). *Preliminary Statement on the Democratic Republic of the Congo General Elections, December 2023*.
- [9]. The Carter Center. (2024). *Interim Report: The Carter Center International Election Observation Mission—Democratic Republic of the Congo, January 26, 2024*.
- [10]. The Carter Center. (2024). *Final Report: General Elections in the Democratic Republic of the Congo, December 2023*.
- [11]. World Bank. (2026). *Access to electricity (% of population) — Democratic Republic of the Congo*. World Development Indicators.  
<https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=CD>