**Scénarios et tactiques de disponibilité**

[Transfert d’un compte à un autre compte](#_30j0zll)

[Tactique : Ping/Echo](#_1fob9te)

[Utilisation générale du GAB](#_3znysh7)

[Tactique : Monitor (self-test)](#_2et92p0)

[Impossiblité d’obtention du solde](#_tyjcwt)

[Tactique : Passive Redundancy Active redundancy](#_3dy6vkm)

[Guichet Système inopérable](#_1t3h5sf)

[Tactique : Escalating Restart](#_4d34og8)

[Disponibilité pour les retraits de fonds](#_17dp8vu)

[Tactique : Mise hors d’usage (pour retrait seulement)](#_3rdcrjn)

[Disponibilité des informations bancaire des clients](#_26in1rg)

[Tactique : Redondance passive](#_lnxbz9)

[Un client ne peut pas faire de retrait à cause d’un problème de communication avec le serveur](#_35nkun2)

[Tactique : Ping/echo](#_1ksv4uv)

[Tactique : Exception handling](#_44sinio)

[Tactique : Removal From Service](#_2jxsxqh)

[Le lecteur de carte est défectueux](#_z337ya)

[Tactique : Dégradation](#_3j2qqm3)

[Tactique : Retry](#_1y810tw)

[Tactique : Removal from service](#_4i7ojhp)

[Le guichet automatique n’a plus de fond pour effectuer des retraits. Le système informe l’usager et procède aux autres fonctionnalités](#_szzstar9m6vs)

[Tactique : Prevent faults](#_1ci93xb)

[Le système du guichet automatique redémarre suite à une panne électrique](#_3whwml4)

[Tactique : recover from faults / reintroduction](#_2bn6wsx)

[Disponibilité – Fonction authentification](#_qsh70q)

[Tactique : Détection de fautes – Moniteur](#_3as4poj)

[Tactique : Détection de fautes – Autotest](#_1pxezwc)

[Tactique : Prévention des fautes : Maintenance préventive](#_49x2ik5)

[Tactique : Removal from service](#_2p2csry)

[Disponibilité – Fonction Dépôt](#_147n2zr)

[Tactique : Détection de fautes – Moniteur](#_3o7alnk)

[Tactique : Détection de fautes – Autotest](#_23ckvvd)

[Tactique : Prévention des fautes : Maintenance préventive](#_ihv636)

[Un client veut effectuer une opération .](#_32hioqz)

[Tactique : Monitor](#_1hmsyys)

[Le client souhaite utiliser une carte MasterCard](#_41mghml)

[Tactique : Software Upgrade](#_2grqrue)

| **Scénario** | Transfert d’un compte à un autre compte |
| --- | --- |
| **objectifs d'affaires** | Fournir un service de transfer instantané et disponible à 99.99% |
| **Source** | Équipement interne du guichet (Ports), Infrastructure physique (câble de connexion) |
| **Stimulus** | Connexion indisponible entre le guichet et la/les banque(s). |
| **Artéfact** | Canaux de communication. |
| **Environnement** | Opération normale |
| **Réponse** | * Garder une trace du problème. * Rendre le service indisponible le temps de réparer le problème. |
| **Mesure de la réponse** | * Temps nécessaire¸ pour réparer le problème. * Pourcentage de disponibilité. |
| **Questions** | 1. Comment vérifier la disponibilité de la connexion ? 2. Combien de fois on teste la disponibilité par minute ? |

### Tactique : Ping/Echo

**Description**: envoi de messages asynchrone (Requête/Réponse) à partir du GAB vers le/les serveurs de la banque.

**Justification**: il faut tester l’accessibilité aux serveurs de la banque et temps réel ou en une très courte période de temps (espace de quelque dizaine de secondes) afin de garantir le bon fonctionnement du GAB ainsi que permettre la détection de défaillance dans la connexion et pouvoir agir en conséquence dans les plus brefs délais.

| **Scénario** | Utilisation générale du GAB |
| --- | --- |
| **objectifs d'affaires** | Fournir une disponibilité de 99.99% du GAB ainsi que l’accès à tous ses services. |
| **Source** | Équipement interne du guichet (Clavier, lecteur de cartes, imprimante de reçus) |
| **Stimulus** | Réponse incorrecte |
| **Artéfact** | Clavier |
| **Environnement** | Opération normale |
| **Réponse** | * Garder une trace de l’erreur. * Notifier l’équipe de maintenance. * Rendre le système temporairement indisponible. |
| **Mesure de la réponse** | * Le temps nécessaire pour rendre le système disponible. * Temps nécessaire pour réparer le clavier. |
| **Questions** | 1. Comment suivre le bon fonctionnement des composants du GAB ? 2. Quels sont périphériques essentiel pour fournir le minimum d’accessibilité au GAB ? |

### Tactique : Monitor (self-test)

**Description**: le Monitoring est la tactique utilisé pour surveiller le bon fonctionnement et la bonne santé des composants physiques et logiques d’un système donné.

**Justification**: le clavier est un périphérique d’entrée et fait parties des composants les plus importants au fonctionnement correct du GAB. Surveiller ce périphérique sera d’une grande utilité si on veut garder le GAB accessible et fonctionnel car cela permettrai aux équipes de maintenance de réparer le clavier ou la changer dès la détection du disfonctionnement.

| **Scénario** | Impossiblité d’obtention du solde |
| --- | --- |
| **Objectifs d'affaires** | Satisfaction du client |
| **Source** | Logiciel interne |
| **Stimulus** | Réponse incorrect ou trop longue |
| **Artéfact** | Canaux de communications |
| **Environnement** | Opération normal |
| **Réponse** | Logging des requêtes qui ne fonctionnent pas  Dégradation des fonctionnalités sans l’information du solde |
| **Mesure de la réponse** | Le système peut fonctionner x h en mode dégradé  Maintien de xx% des fonctionnalités du système en mode dégradé |
| **Questions** | 1. Combien de temps le système prend pour tomber en mode dégradé? 2. Quelles sont les fonctionnalités fonctionnelles en mode dégradé? 3. Ou seront stocké les informations des transactions? |

### Tactique : Passive Redundancy

**Description**: Permet d’avoir plusieurs copies des informations si jamais la charge devient trop grande ou qu’un serveur tombe en panne.

**Justification**: En utilisant la redondance passive, on pourrait avoir plusieurs serveurs qui contiennent chacun une copie du solde actuel. Ainsi si l’un des serveurs tombent en panne, un autre est en place pour obtenir le solde.

| **Scénario** | Système inopérable |
| --- | --- |
| **objectifs d'affaires** | Satisfaction du client |
| **Source** | Logiciel interne |
| **Stimulus** | Crash |
| **Artéfact** | Processus |
| **Environnement** | Environnement normal |
| **Réponse** | Afficher un message indiquant que le guichet est inopérable.  Logging des erreurs  Notifier les administrateurs aux administrateurs. |
| **Mesure de la réponse** | Réparation du crash en moins de x heures.. |
| **Questions** | 1. Quelles sont les opérations possibles à distance pour réparer le crash? 2. Es-ce que le nombre d’heures pour la réparation varie en fonction du moment? Jour vs Nuit? |

### Tactique : Escalating Restart

**Description**: Permet de redémarrer les services automatiquement avec un minimum d’impact sur les autres services.

**Justification**: Puisque le guichet redémarre les services automatiquement lorsqu’ils tombent en panne, le guichet à une possibilité de pouvoir récupérer de ses propres problèmes. Si le crash n’est pas majeur, le guichet pourrait récupérer sans l’intervention physique d’un technicien.

| **Scénario** | Disponibilité pour les retraits de fonds |
| --- | --- |
| **objectifs d'affaires** | La banque souhaite que les clients puissent effectuer des retraits de 500$ dans 99,9% des cas |
| **Source** | Interne et externe |
| **Stimulus** | Omission |
| **Artéfact** | Processus système |
| **Environnement** | Condition normale et dégradée |
| **Réponse** | Aviser les intervenants appropriés du manque de fond |
| **Mesure de la réponse** | Le système doit poursuivre les opérations possibles. |
| **Questions** | 1. Quel est le temps requis pour recharger le distributeur de billet? 2. Combien de temps le système va mettre pour se mettre hors d’usage pour la fonctionnalité retrait? |

### Tactique : Mise hors d’usage (pour retrait seulement)

**Description** : En cas de manque de fond dans le guichet automatique, la fonctionnalité permettant d’effectuer des retraits doit se retrouver inactive.

**Justification** : Étant donné que le distributeur n’est plus en mesure de fournir de l’argent comptant à ces clients, la fonctionnalité de retrait ne doit plus demeurer active. Les autres opérations pouvant être effectuées avec le guichet ne sont pas affectées et peuvent être utilisées.

| **Scénario** | Disponibilité des informations bancaire des clients |
| --- | --- |
| **objectifs d'affaires** | La banque souhaite que ces clients puissent consulter et imprimer les informations de leurs comptes dans 99.99% du temps |
| **Source** | Interne ou externe |
| **Stimulus** | Message erreur |
| **Artéfact** | Processus système |
| **Environnement** | Conditions normales d’exécution |
| **Réponse** | Afficher un message d’erreur permettant d’informer l’utilisateur du dysfonctionnement et le système doit revenir à son état initial |
| **Mesure de la réponse** | Le système ne doit pas s'arrêter, il doit poursuivre son exécution |
| **Questions** | 1. Combien de temps le système va mettre pour basculer vers le nouveau canal de communication? |

### Tactique : Redondance passive

**Description** : Mettre en place deux liens permettant la consultation des informations de compte. Mettre en place un lien primaire et un lien de secours

**Justification** : Afin de permettre aux clients de pouvoir consulter leurs informations bancaires en tout temps, la redondance va permettre d’assurer un lien de communication de secours dans le cas ou le canal primaire viendrait à tomber.

| **Scénario** | Un client ne peut pas faire de retrait à cause d’un problème de communication avec le serveur |
| --- | --- |
| **objectifs d'affaires** | Je veux qu’un client soit capable de faire un retrait avec 95% du temps. Justification de pertinence : Réputation de la banque, perte d’argent, perte de clients |
| **Source** | Serveur |
| **Stimulus** | Ne répond pas |
| **Artéfact** | Processus de communication du guichet automatique |
| **Environnement** | Opération normale |
| **Réponse** | Message d’indisponibilité au client et au responsable du guichet, log de la faute |
| **Mesure de la réponse** | Le temps de réparation, le temps de disponibilité |
| **Questions** | 1. Comment est-ce que le responsable du guichet est avisé du problème? 2. Est-ce qu’il y a un système de backup pour le serveur ? 3. Est-ce qu’il y d’autres processus qui sont affectés ? 4. Est-ce que le réseau au complet est affecté ? |

### Tactique : Ping/echo

**Description**: Le guichet essaye de recontacter le serveur afin de faire le retrait d’argent.

**Justification**: Il se peut que le problème se règle de lui même (le réseau était peut-être congestionné).

### Tactique : Exception handling

**Description**: Le guichet affiche un message d’erreur et éjecte la carte du client.

**Justification**: Le client ne désire pas s’éterniser au guichet. Il veut simplement faire une transaction. S’il ne peut pas la faire on présume qu’il veut quitter le guichet.

### Tactique : Removal From Service

**Description**: Le guichet essaye de contacter le serveur dès que le client insère sa carte afin de ne pas faire perdre de temps au client inutilement en lui faisant faire une transaction qui risque d’échouer.

**Justification**: La frustration ressentie par une personne est généralement proportionnel au temps qu’elle a investi lorsqu’elle rencontre un problème (ex: perdre un travail parce que Word décide de planter). Il faut donc s’assurer que le guichet fonctionne bien avant d’offrir des services au client.

| **Scénario** | Le lecteur de carte est défectueux |
| --- | --- |
| **objectifs d'affaires** | La carte doit être lu à 99% du temps qu’elle est insérée dans le lecteur de carte. |
| **Source** | Le lecteur de carte |
| **Stimulus** | Est défectueux |
| **Artéfact** | Impossibilité de lire les données à l’intérieur de la puce de la carte |
| **Environnement** | Opération normale |
| **Réponse** | Message d’erreur envoyé au responsable de la machine et log de la faute |
| **Mesure de la réponse** | Le temps de réparation, le temps de disponibilité |
| **Questions** | 1. Comment est notifié le responsable de la machine ? 2. Est-ce que le guichet peut utiliser une méthode de lecture alternatif pour lire la carte, ex : bande magnétique ? 3. Est-ce que la carte est endommagée après l’utilisation du lecteur de carte défectueux ? |

### Tactique : Dégradation

**Description**: Le lecteur de carte essaie de lire les données de la bande magnétique.

**Justification**: Si la carte est munie d’une bande magnétique, le guichet peut essayer cette méthode, bien qu’elle soit plus ancienne et moins recommandé.

### Tactique : Retry

**Description**: Le lecteur de carte essaie de lire les données de la puce une deuxième fois.

**Justification**: C’est une option peu coûteuse en temps et en ressources et il se peut que la seconde tentative fonctionne sans problème.

### Tactique : Removal from service

**Description**: Le guichet éjecte la carte et indique au client actuel et aux futures clients qu’il est défectueux.

**Justification**: Le guichet ne peut pas remplir ses fonctions il doit donc aviser les utilisateurs qu’ils devront utiliser un autre guichet.

| **Scénario** | Le guichet automatique n’a plus de fond pour effectuer des retraits. Le système informe l’usager et procède aux autres fonctionnalités |
| --- | --- |
| **Objectifs d'affaires** |  |
| **Source** | Interne/externe : usagers, hardware, software, physical environnement |
| **Stimulus** | Fault : ommission. A component fails to respond to an input |
| **Artéfact** | Storage, communication channel, processor, process |
| **Environnement** | Normal operation, degraded operation |
| **Réponse** | Detect the fault :   * Log the fault * Notify appropriate entities   Recover from the fault :   * Disable source of events causing the fault * Be temporarily unavalaible while repair is being affected * Operate in a degraded mode |
| **Mesure de la réponse** | Time or time interval when the system must be available  Availability percentage 99.99%  Time or time interval when the system can be in degraded mode 99.00% |

### Tactique : Prevent faults

**Description**: Predictive model

**Justification :** Vérifie l’état du system régulièrement pour assurer l’exécution du système en mode normal et prévenir les fautes. Dans notre cas, cela permet de vérifier le solde courant des fonds disponibles pour les retraits.

| **Scénario** | Le système du guichet automatique redémarre suite à une panne électrique |
| --- | --- |
| **Objectifs d'affaires** |  |
| **Source** | Interne/externe : usagers, hardware, software, physical environnement |
| **Stimulus** | Fault : ommission, crash |
| **Artéfact** | Storage, communication channel, processor, process |
| **Environnement** | Shutdown, repair mode |
| **Réponse** | Detect the fault :   * Log the fault * Notify appropriate entities   Recover from the fault :   * Notify selected users or others systems * Take actions to limit the damage caused by the fault * Be temporarily unavalaible while repair is being affected * Operate in a degraded mode |
| **Mesure de la réponse** | Time or time interval when the system must be available  Availability percentage 99.99%  Time or time interval when the system can be in degraded mode 99.00% |

### Tactique : recover from faults / reintroduction

**Description**: Escalating restart

**Justification :** Redémarrage automatique suite au problème.

| **Scénario** | Disponibilité – Fonction authentification |
| --- | --- |
| **objectifs d'affaires** | Assurer une disponibilité satisfaisante de toutes les fonctionnalités post authentification au client |
| **Source** | Logiciel interne – Interne au système |
| **Stimulus** | Pas de réponse ou réponse incorrecte : Le guichet automatique est incapable de valider le PIN du client. |
| **Artéfact** | Communication : connexion au serveur de base de données comptes |
| **Environnement** | Opération normale en mode (ID confirmation) |
| **Réponse** | **Détection de fautes :**   * Détection au niveau logiciel et de réseautique. * Noter l’exception survenue, date et heure lors de l’interruption de service dans le but de créer un rapport pour de la maintenance préventive. * Envoyer les rapports et les enregistrements de traces à une équipe de techniciens.   **Prévention de fautes**   * Effectuer une maintenance préventive sur le serveur de données et les guichets reliés pour s’assurer d’un bon fonctionnement en tout temps.   **Rétablir le service :**   * Réinitialiser le fonctionnement normal de la machine lors de la récupération de la connexion sur le réseau. |
| **Mesure de la réponse** | 99,9% de disponibilité  Temps pour détection de la faute : Immédiat  Temps pour réparer la faute : Maximum 8 heures |

### Tactique : Détection de fautes – Moniteur

**Description**: Cette tactique utilise un élément d’observation afin de valider l’état et le bon fonctionnement de composants clés du système.

**Justification**: Tel que mentionné dans le scénario ci-dessus, il est impératif de détecter les fautes le plus tôt possible afin de limiter les temps d’arrêt du système. Cette tactique nous permet de faire exactement cela.

### Tactique : Détection de fautes – Autotest

**Description**: Les composantes elles-mêmes peuvent utiliser des procédures pré identifiées de tests afin d’assurer leurs bons fonctionnements.

**Justification**: Dans notre cas, nous utilisons cette tactique en parallèle avec la tactique du ***moniteur*** afin de tester les composantes de manières périodiques pour les mêmes raisons que notre utilisation de la tactique du ***moniteur***.

### Tactique : Prévention des fautes : Maintenance préventive

**Description**: Cette tactique permet de limiter les erreurs en temps d’opération normal en prenant soin de réparer certaines composantes d’un système avant que celles-ci ne flanchent complément et causent un arrêt de service.

**Justification**: Dans notre cas, cette tactique est utilisée en parallèle de nos tactiques ***moniteur et autotest***. À chaque fois, qu’un événement non attendu est enregistré, un rapport est produit et ces rapports nous aident à planifier nos efforts de maintenance préventive.

### Tactique : Removal from service

**Description**: Réduire les services offerts (ou que l’on peut offrir) à l’usager lors d’une perte de connexion.

**Justification**: Lorsque la machine est incapable de communiquer avec la base de données pour récupérer le certificat d’accès de l’utilisateur, on réduit ou on coupe les fonctionnalités à offrir à l’usager.

| **Scénario** | Disponibilité – Fonction Dépôt |
| --- | --- |
| **objectifs d'affaires** | Assurer une disponibilité satisfaisante de la fonction de dépôt au client |
| **Source** | Externe au système logiciel, mais interne au guichet (matériel) |
| **Stimulus** | Échec |
| **Artéfact** | (Hardware) du système GAB – tiroir à billet est en défaut. |
| **Environnement** | Opération normale en mode (ouverture du tiroir à billet) |
| **Réponse** | **Détection de fautes :**   * Détection au niveau matériel jumelé à une alarme en cas de faute du mécanisme pour appeler l’équipe de réparation. * Noter l’exception survenue, date et heure lors de l’interruption de service dans le but de créer un rapport pour de la maintenance préventive. * En mode (attente) du guichet, effectuer des tests périodiques sur les composantes clés matérielles pour détecter des fautes potentielles.   **Prévention de fautes**   * Effectuer une maintenance préventive sur les composantes les plus à risques du système en utilisant les données recueillies lors des rapports d’interruption de service.   **Rétablir le service :**   * Transaction annulée, carte redonnée au client et redémarrage de la machine afin de réinitialiser le système et ses composants physiques. * Équipe dépêchée lors de la détection de faute. |
| **Mesure de la réponse** | 99,9% de disponibilité  Temps pour détection de la faute : Immédiat  Temps pour réparer la faute : Maximum 8 heures |

### Tactique : Détection de fautes – Moniteur

**Description**: Cette tactique utilise un élément d’observation afin de valider l’état et le bon fonctionnement de composants clés du système.

**Justification**: Tel que mentionné dans le scénario ci-dessus, il est impératif de détecter les fautes le plus tôt possible afin de limiter les temps d’arrêt du système. Cette tactique nous permet de faire exactement cela.

### Tactique : Détection de fautes – Autotest

**Description**: Les composantes elles-mêmes peuvent utiliser des procédures pré identifiées de tests afin d’assurer leurs bons fonctionnements.

**Justification**: Dans notre cas, nous utilisons cette tactique en parallèle avec la tactique du ***moniteur*** afin de tester les composantes de manières périodiques pour les mêmes raisons que notre utilisation de la tactique du ***moniteur***.

### Tactique : Prévention des fautes : Maintenance préventive

**Description**: Cette tactique permet de limiter les erreurs en temps d’opération normal en prenant soin de réparer certaines composantes d’un système avant que celles-ci ne flanchent complément et causent un arrêt de service.

**Justification**: Dans notre cas, cette tactique est utilisée en parallèle de nos tactiques ***moniteur et autotest***. À chaque fois, qu’un événement non attendu est enregistré, un rapport est produit et ces rapports nous aident à planifier nos efforts de maintenance préventive.

CONCLUSION

Notre analyse permet de mettre la lumière sur plusieurs tactiques afin d’atteindre les objectifs visés pour l’attribut de qualité de la disponibilité du système GAB. En appliquant ces stratégies, nous sommes sûrs d’atteindre le seuil visé de 99.9% de disponibilité pour notre système. Veuillez noter que notre analyse s’est limitée sur des tactiques propres à la facette logicielle du système. Pour atteindre des objectifs plus stricts de disponibilité, une autre tactique à envisager serait la redondance des guichets automatiques.

| **Scénario** | Un client veut effectuer une opération . |
| --- | --- |
| **objectifs d'affaires** | Garantir une disponibilité de 99,99% (optimisation du processus de maintenance et réparation des GAB). |
| **Source** | Composant du GAB (lecteur de carte, distributeur de billets ..etc). |
| **Stimulus** | Réponse incorrecte |
| **Artéfact** | Périphériques /logiciel du GAB |
| **Environnement** | Normal |
| **Réponse** | Mettre le GAB en mode dégradé, enregistrer (logger) l’erreur et envoyer un message au service de maintenance et réparation. |
| **Mesure de la réponse** | Temps de réparation du composant |
| **Questions** | 1. Quels sont les interfaces des périphériques du GAB? 2. Quels sont les contraintes liées à ces interfaces ?(moyen de communication ,API utilisé ...etc). 3. Quel service est responsable de la maintenance/réparation des périphériques du GAB ? 4. Où doit-on envoyer un message d’alerte ?et sous quel forme? 5. Quels périphériques sont essentiels au fonctionnement minimum d’un GAB? |

### Tactique : Monitor

**Description**: Il faut une supervision des périphériques, afin de détecter dans les plus brefs délais les périphériques défectueux.

Une fois un matériel est signalé défectueu, selon le type du matériel le gab prend le statut normal/dégradé/hors service; et un message est envoyé à l’équipe concernée de la maintenance et réparation des GAB.

**Justification:** la détérioration des composantes peuvent affecter la continuité de service, par exemple un lecteur de carte défectueux ne vas pas pouvoir lire les carte insérée , et peut renvoyé au client un faux message tel que : carte non acceptés .

L’ajout d’un composant de monitoring qui contiendra la logique d’initialisation des self-test des périphériques du GAB optimisera le processus de détection , le temps d'indisponibilité équivaudra au temps de l’intervention de l’équipe de maintenance et réparation.

| **Scénario** | Le client souhaite utiliser une carte MasterCard |
| --- | --- |
| **objectifs d'affaires** | Fournir un service au client munie de cartes de divers compagnies |
| **Source** | Insertion de carte |
| **Stimulus** | L’appareil ne répond pas lors de l’insertion de la carte MasterCard |
| **Artéfact** | Réseaux bancaire |
| **Environnement** | Normal |
| **Réponse** | Le système éjecte la carte et demande a l’utilisateur d'insérer sa carte |
| **Mesure de la réponse** | Temps entre la détection de l’erreur et la mise en place de la mise à jour du logiciel |
| **Questions** | 1. Quel est le protocole de communication et la forme des messages ? 2. Quel est l’estimation du temps de réponse ?(GAB to BANK to GAB) 3. Quel sont les composantes logiciels a modifier ? quel impacte aura ce changement ? |

### Tactique : Software Upgrade

**Description**: On doit permettre au logiciel du GAB de communiquer avec les nouveaux réseaux bancaire et éventuellement de reconnaître les nouveaux types de cartes bancaires.

**Justification**: Il s’agit de modifier les composantes logicielles pour permettre au GAB de communiquer avec les nouveaux réseaux bancaires, les protocoles de communication ,la forme des messages, les erreurs ainsi que les exceptions peuvent différés des traitements avant la MAJ