

Conception par approche UP/SysML d'un système de contrôle d'accès basé sur le QR-Code, cas du campus de l'Université Protestante de Lubumbashi (UPL)

Design of a QR-Code-Based Access Control System Using the UP/SysML Approach: Case Study of the Université Protestante de Lubumbashi (UPL) Campus

TSHIANGALA KASANJI Mardochée

Enseignant chercheur
Université Protestante de Lubumbashi
Faculté des sciences informatiques
République Démocratique du Congo
0009-0000-4026-261X

KIBWIKI MUSA Jason

Enseignant chercheur
Université Protestante de Lubumbashi
Faculté des sciences informatiques
République Démocratique du Congo
0009-0004-4422-6797

Date de soumission : 08/05/2026

Date d'acceptation : 12/08/2026

Pour citer cet article :

TSHIANGALA KASANJI. M. & KIBWIKI MUSA. J. (2026) «Conception par approche UP/SysML d'un système de contrôle d'accès basé sur le QR-Code, cas du campus de l'Université Protestante de Lubumbashi (UPL)», Revue Internationale du chercheur « Volume 7 : Numéro 3 » pp : 587-610

Résumé

La gestion sécurisée des accès constitue un enjeu majeur dans les campus universitaires, où les méthodes traditionnelles présentent des limites en termes de sécurité, de traçabilité et d'efficacité. Cet article propose la conception d'un système de contrôle d'accès basé sur le QR-Code, appliquée au campus de l'Université Protestante de Lubumbashi (UPL).

La démarche adoptée repose sur la méthode UP (Unified Process) pour structurer les phases d'analyse des besoins et de conception, et sur le langage SysML pour la modélisation des exigences, des fonctionnalités et de l'architecture du système. Cette contribution propose un modèle de conception intégré permettant de formaliser simultanément les exigences fonctionnelles, structurelles et comportementales d'un système de contrôle d'accès universitaire, dans un contexte congolais où ce type de démarche reste peu documenté. L'étude se limite à la conception du système et présente les principaux modèles SysML, notamment les diagrammes de contexte, d'exigences, de cas d'utilisation, de séquence, de blocs et de déploiement.

Cette démarche méthodologique permet de concevoir un système de contrôle d'accès sécurisé, automatisé et adapté au contexte universitaire. Ce travail constitue une base méthodologique pour des implémentations futures, une validation expérimentale et l'intégration de technologies avancées.

Mots clés : *Contrôle d'accès ; QR-Code ; Unified Process (UP) ; SysML ; Modélisation.*

Abstract

Secure access management is a major challenge in university campuses, where traditional access control methods suffer from limitations in terms of security, traceability, and efficiency. This paper presents the design of a QR-Code-based access control system, applied to the campus of the Université Protestante de Lubumbashi (UPL). The proposed approach is based on the Unified Process (UP) to structure the requirements analysis and system design phases, and on the Systems Modeling Language (SysML) for modeling system requirements, functionalities, and architecture. This contribution proposes an integrated design model formalizing functional, structural and behavioural requirements of a university access control system, in a Congolese context where such a methodology remains scarcely documented. The study is limited to the system design phase and introduces key SysML models, including context, requirements, use case, sequence, block, and deployment diagrams.

This methodological approach enables the design of a secure, automated, and context-adapted access control system for university environments. This work provides a methodological foundation for future implementations, experimental validation, and the integration of advanced technologies.

Keywords : *Access control; QR-Code; Unified Process; SysML; Modelisation.*

Introduction

L'évolution rapide des technologies de l'information et de la communication (TIC) a profondément transformé les modes de gestion et de sécurisation des organisations modernes. Les institutions universitaires, en tant qu'environnements ouverts accueillant quotidiennement un grand nombre d'étudiants, de personnels administratifs, d'enseignants et de visiteurs, sont particulièrement concernées par les problématiques liées à la sécurité et au contrôle d'accès. La maîtrise des flux d'entrées et de sorties constitue aujourd'hui un enjeu pour garantir la sûreté des personnes, la protection des infrastructures et la préservation des ressources matérielles et immatérielles.

Dans de nombreux établissements universitaires en République Démocratique du Congo, et plus particulièrement au sein des campus universitaires, les mécanismes de contrôle d'accès reposent encore sur des méthodes traditionnelles telles que les registres manuels, les badges physiques non sécurisés ou la surveillance humaine permanente. Ces approches présentent plusieurs limites, notamment le manque de traçabilité, la vulnérabilité à la falsification, la lenteur des procédures, ainsi qu'une forte dépendance au facteur humain. Ces insuffisances exposent les campus à des risques d'intrusion, d'usurpation d'identité et de gestion inefficace des accès.

Face à ces défis, l'intégration de solutions technologiques innovantes apparaît comme une réponse pertinente et durable. Le QR-Code (Quick Response Code), en raison de sa simplicité, de son faible coût de déploiement, de sa rapidité de lecture et de sa compatibilité avec de nombreux dispositifs numériques, constitue une technologie prometteuse pour la mise en œuvre de systèmes modernes de contrôle d'accès. Utilisé conjointement avec une infrastructure logicielle adaptée, le QR-Code permet d'automatiser les processus d'authentification, de renforcer la sécurité et d'assurer une traçabilité fiable des accès.

Toutefois, la mise en place d'un système de contrôle d'accès ne saurait se limiter à une simple implémentation technologique. Elle nécessite une démarche méthodologique rigoureuse permettant d'analyser les besoins réels, de modéliser les exigences, de concevoir une architecture cohérente et de garantir l'évolutivité du système. C'est dans cette optique que s'inscrit l'ingénierie système, qui propose des approches structurées pour la conception de systèmes complexes. Parmi ces approches, la méthode UP (Unified Process) se distingue par son caractère itératif et incrémental, son pilotage par les cas d'utilisation, sa focalisation sur l'architecture et sa capacité à réduire les risques dès les premières phases du projet.

Par ailleurs, le langage de modélisation SysML (Systems Modeling Language), dérivé d'UML, offre un cadre formel pour représenter aussi bien les aspects fonctionnels, structurels que comportementaux d'un système. SysML permet de modéliser les exigences, les interactions entre composants, les flux d'informations ainsi que les états du système, favorisant ainsi une meilleure compréhension et une communication efficace entre les parties prenantes.

Ce travail se positionne également par rapport aux approches technologiques concurrentes de contrôle d'accès. Si les systèmes RFID et biométriques dominent historiquement ce domaine, des travaux récents montrent que les systèmes fondés sur le QR-Code constituent une alternative économique et conviviale aux systèmes RFID traditionnels, ce qui justifie leur adoption dans un contexte universitaire où les contraintes budgétaires sont fortes (Fauzi et al., 2020).

La contribution scientifique de cet article réside ainsi dans la proposition d'un modèle de conception intégré, combinant la méthode UP et le langage SysML, permettant de formaliser simultanément les exigences fonctionnelles, structurelles et comportementales d'un système de contrôle d'accès par QR-Code, dans un contexte universitaire congolais où ce type de démarche méthodologique reste encore peu documenté.

Dans ce contexte, le présent article porte sur la **conception par approche UP/SysML d'un système de contrôle d'accès basé sur le QR-Code**, appliquée au **cas du campus de l'Université Protestante de Lubumbashi (UPL)**. Ce travail se limite volontairement aux phases d'analyse des besoins et de conception du système, dans le but de proposer une architecture cohérente et adaptée au contexte universitaire local.

La problématique centrale de cette recherche est de savoir **Comment concevoir, à l'aide de la méthode UP et du langage SysML, un système de contrôle d'accès sécurisé, automatisé et traçable basé sur le QR-Code pour un campus universitaire ?**

L'objectif général de cette étude est de proposer un modèle de conception d'un système de contrôle d'accès répondant aux exigences de sécurité et de gestion du campus de l'UPL. De manière spécifique, il s'agit de :

- Analyser les besoins fonctionnels et non fonctionnels du système ;
- Identifier les acteurs et les exigences du système ;
- Modéliser les fonctionnalités à l'aide des cas d'utilisation ;
- Concevoir l'architecture structurelle et comportementale du système à l'aide de sysml.

La méthodologie adoptée repose sur l'application des principes de la méthode UP pour structurer les phases d'analyse et de conception, combinée à l'utilisation des diagrammes SysML pour la modélisation du système.

1. Cadre théorique et méthodologique

1.1. Ingénierie système et méthodes de conception

1.1.1. Définition de l'ingénierie système

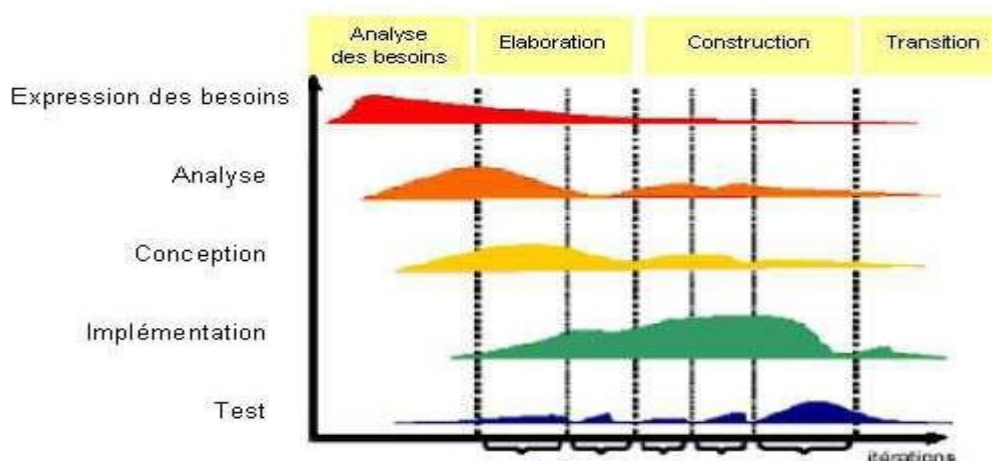
L'ingénierie système (ou ingénierie de systèmes) est une démarche méthodologique générale qui englobe l'ensemble des activités adéquates pour concevoir, faire évoluer et vérifier un système apportant une solution économique et performante aux besoins d'un client tout en satisfaisant l'ensemble des parties prenantes (Mesnier, n.d.).

Les pratiques d'ingénierie système sont principalement répertoriées dans trois normes : la norme ISO/IEC 15288 qui adopte le point de vue d'une entreprise participant à des projets d'ingénierie système, la norme ANSI/EIA 632 qui hiérarchise les processus techniques de transformation du besoin en solution et la norme IEEE 1220 qui définit les processus de conception.

1.1.2. Présentation de la méthode UP (Unified Process)

La méthode UP (Unified Process ou Processus Unifié) est un cadre générique de développement logiciel itératif et incrémental, centré sur l'architecture, piloté par les cas d'utilisation et les risques, qui guide les équipes dans toutes les phases de la vie d'un logiciel (exigences, analyse, conception, implémentation, test) en utilisant un langage de modélisation (Kruchten, 2000).

Figure N° 1 Cycle de de vie de la méthode UP



Source : (Kruchten, 2000)

Ses quatre phases principales sont l'Inception (lancement), l'Élaboration, la Construction et la Transition, adaptables à chaque projet.

1.1.2.1. Principes clés

UP repose sur cinq principes fondamentaux : itératif et incrémental, guidé par les cas d'utilisation, centré sur l'architecture, orienté risques, et visuel via des modèles :

- **Itératif et incrémental** : Développement en itérations courtes produisant des incréments fonctionnels pour valider progressif.
- **Guidé par les cas d'utilisation** : Priorité aux besoins utilisateurs via cas d'usage pour aligner sur attentes.
- **Centré sur l'architecture** : Définition précoce et validation de l'architecture pour stabilité et qualité.
- **Gestion des risques** : Identification et atténuation proactive des risques dès les phases initiales.
- **Focus sur la qualité et collaboration** : Tests continus, revues et communication entre parties prenantes

1.1.3. Le langage SysML

SysML (Systems Modeling Language) est un langage de modélisation graphique standardisé pour l'ingénierie des systèmes complexes, étendant UML pour inclure hardware, software, données et processus. Il facilite la spécification, l'analyse, la vérification et la validation des systèmes multidisciplinaires(*SysML vs. UML: What's the Difference?* | PTC, n.d.).

Ce langage reprend sept diagrammes UML (classe, objet, paquetage, état, activité, séquence, utilisation) mais supprime les aspects trop logiciels (déploiement, cas d'usage étendus) et ajoute deux diagrammes : exigences et paramétrique. UML est centré sur le logiciel orienté objet (14 diagrammes), tandis que SysML est plus flexible, moins verbeux et adapté aux systèmes physiques avec une sémantique enrichie pour les contraintes et performances.

1.1.4. Le QR-Code dans les systèmes de contrôle d'accès

Le code QR (en anglais QR Code) est un type de code-barres en deux dimensions (ou code matriciel) constitué de modules noirs disposés dans un carré à fond blanc L'agencement de ces modules définit l'information que contient le code QR (QR est l'abréviation de l'anglais Quick Response) ce qui signifie que le contenu du code peut être décodé rapidement après avoir été

lu par un lecteur de code-barres, un téléphone mobile, un smartphone, ou encore une webcam. Son avantage est de pouvoir stocker plus d'informations qu'un code à barres, et surtout des données directement reconnues par des applications.(Crompton et al., 2012)

1.1.4.1. Principe de fonctionnement

Le principe du code QR, qui en fait son principal atout, est d'utiliser la redondance d'informations. En informatique, la redondance des données (ou data redundancy en anglais) désigne le fait des données identiques soient disponibles dans différentes bases ou différents gisements de données. Ces données redondantes peuvent réapparaître dans différents champs d'une même base de données ou dans plusieurs emplacements différents(Crompton et al., 2012).

La redondance est employée dans le code QR de manière à prévenir toute altération du motif et ainsi fournir au lecteur l'information codée originale sans problèmes. C'est le code correcteur d'erreurs du code QR qui crée la redondance afin d'accroître la fiabilité de l'information. L'objectif d'un code correcteur est la détection ou la correction d'erreurs après la transmission d'un message, cette correction est permise grâce à l'ajout d'informations redondantes.

1.1.5. Approches concurrentes de contrôle d'accès

Au-delà du QR-Code, plusieurs technologies sont mobilisées dans la littérature pour le contrôle d'accès physique en milieu universitaire :

- ✚ RFID (Radio Frequency Identification) : Cette technologie reste largement répandue dans les campus, mais le coût du matériel RFID demeure un frein important par rapport aux solutions basées sur le QR-Code, qui restent moins onéreuses(*(PDF) Development of a Smart Lock System Using QR Code Technology*, n.d.).
- ✚ QR-Code couplé à des microcontrôleur : Des travaux récents combinent la lecture de QR-Code avec des plateformes matérielles telles qu'Arduino afin de comparer l'identifiant unique scanné à l'entrée avec celui enregistré dans une base de données, avant d'autoriser ou de refuser l'accès. Ces systèmes montrent qu'une solution QR-Code correctement implémentée permet d'accorder ou de refuser l'accès à un environnement protégé de manière rapide, efficace et fiable (Fauzi et al., 2020).

Sécurisation avancée du QR-Code Une revue systématique récente portant sur les systèmes de présence par QR-Code recense des innovations telles que les QR-Codes randomisés, animés ou

dynamiques couplés à la géolocalisation et à la validation IMEI, qui permettent de prévenir efficacement les fraudes telles que l'usurpation de présence (Alghamdi et al., 2019).

Alternatives biométriques et par carte Une étude récente souligne que les systèmes biométriques, RFID et à codes-barres présentent des défis persistants en matière de coût et de risque de détournement, par exemple le partage de cartes ou le transfert de liens de présence entre étudiants (K & Rohann, 2026).

Smart Campus / IoT Access Control : Le contrôle d'accès s'inscrit aujourd'hui dans une réflexion plus large sur le Smart Campus. La littérature montre que le concept de campus intelligent s'est imposé comme axe de recherche majeur en raison des apports des technologies IoT (Alghamdi et al., 2019), avec des architectures proposées comme systèmes de réponse instantanée aux incidents de sécurité (Sánchez-Torres et al., 2018). Plus récemment, il a été montré que l'amélioration des dispositifs de sécurité sur les campus universitaires par l'IoT contribue significativement à la qualité de vie de la communauté étudiante.

Critère	QR-Code	RFID	NFC	Biométrie
Coût de déploiement	Faible	Moyen à élevé	Moyen	Élevé
Facilité de mise en œuvre	Élevée (smartphone/imprimante)	Moyenne (lecteurs dédiés)	Moyenne	Faible (capteurs spécialisés)
Sécurité intrinsèque	Moyenne (renforçable par dynamisme/cryptographie)	Moyenne (clonage possible)	Moyenne-élevée	Élevée
Risque de fraude	Partage de code, capture d'écran	Clonage de tag	Proximité requise	Très faible
Traçabilité	Bonne	Bonne	Bonne	Très bonne
Adéquation au contexte UPL	Très adaptée (faible coût, smartphones répandus)	Coût limitant	Coût limitant	Coût prohibitif

Tableau 1 : Comparatif des technologies de contrôle d'accès (synthèse des auteurs)

1.2. Protocole méthodologique appliqué

Afin de garantir la reproductibilité de la démarche, le tableau suivant détaille, pour chaque phase de la méthode UP, les activités réalisées et les livrables produits dans le cadre de cette étude.

Phase UP	Activités réalisées	Livrables produits
Inception	Analyse du contexte, délimitation du périmètre du système	Description textuelle du processus d'accès actuel
Élaboration	Analyse des besoins, identification des acteurs et des exigences	Diagramme de contexte, diagramme des exigences
Construction	Modélisation des fonctionnalités et de l'architecture	Diagramme de cas d'utilisation, diagrammes de séquence, bdd, ibd
Transition	Non traitée dans le cadre de cette étude	(limite assumée du travail, cf. Discussion)

2. Analyse des besoins du système de contrôle d'accès

2.1. Analyse métier

L'objectif de cette partie est d'examiner en détail les besoins, les processus et les exigences liés au contrôle d'accès dans le contexte spécifique de l'université. Cette analyse métier fournira une compréhension des différents aspects du système de contrôle d'accès, y compris les acteurs impliqués et les flux d'informations.

Les besoins présentés dans cette section ont été recueillis par observation directe du processus d'accès actuel au campus de l'UPL, complétée par des échanges informels avec les agents de sécurité en poste. Cette approche qualitative permet de saisir le déroulement réel du processus, mais elle présente des limites de représentativité qui sont discutées en fin d'article.

2.1.1. Description textuelle du processus de contrôle d'accès actuel

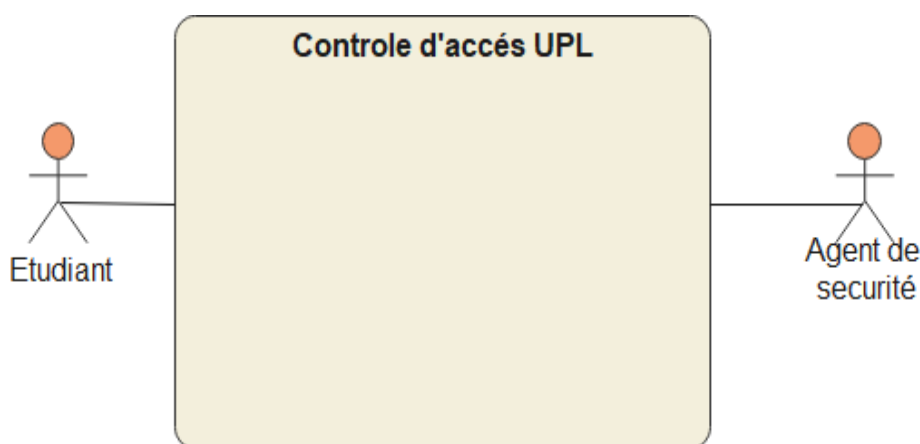
Le processus actuel de contrôle d'accès des étudiants à la cour de l'université de Lubumbashi se déroule de la manière suivante :

1. L'étudiant se présente à la porte d'entrée où des agents de sécurité sont postés.
L'agent demande à l'étudiant de présenter sa carte d'étudiant.

2. Si l'étudiant possède sa carte, il la présente à l'agent qui vérifie les informations et la validité de la carte. Si les informations sont correctes, l'agent autorise l'entrée de l'étudiant. En cas de données incorrectes, l'agent refuse l'accès à l'étudiant et le réfère à ses supérieurs.
3. Si l'étudiant ne possède pas sa carte, l'agent lui demande de se présenter.
4. L'étudiant se présente à l'agent qui vérifie les informations et la validité de son identité. Si les informations sont correctes, l'agent autorise l'entrée de l'étudiant. En cas de données incorrectes, l'agent refuse l'accès à l'étudiant et le réfère à ses supérieurs.

Ce processus décrit les étapes clés du contrôle d'accès des étudiants à la cour de l'université et en montrant le rôle des acteurs dans la vérification des identités et des cartes d'étudiant pour garantir un accès sécurisé et réglementé.

Figure N° 2 Diagramme de contexte

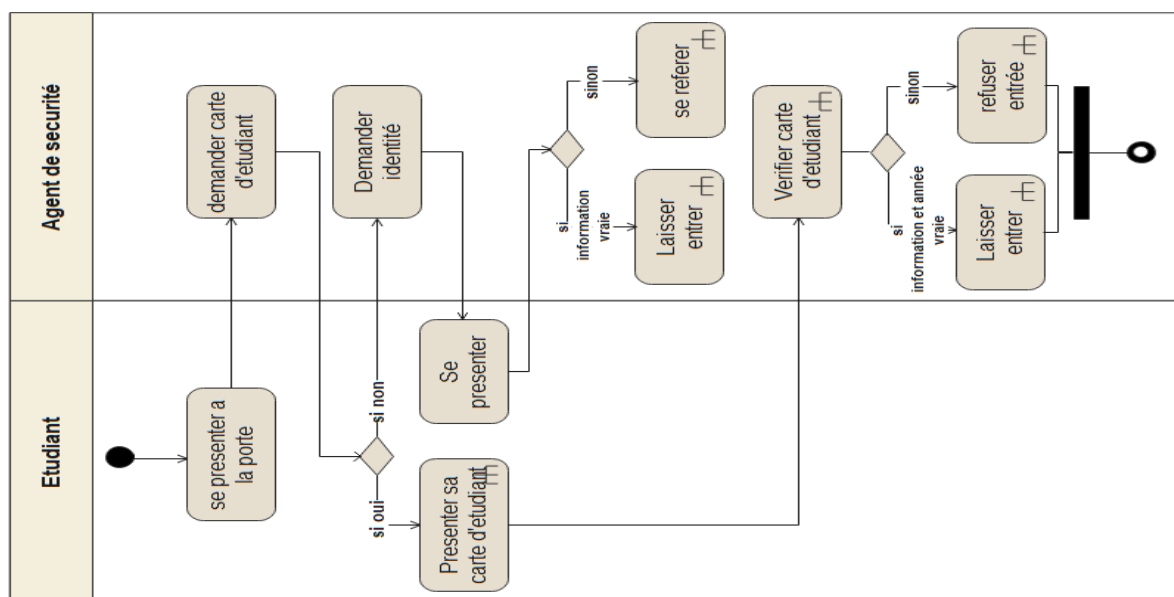


Source : Auteur

➤ Diagramme d'activité métier

Le diagramme d'activité est un diagramme qui modélise les aspects dynamiques d'un système. C'est une simplification du diagramme d'état de transition permettant d'améliorer les flux contrôle des processus informatiques et organisationnels. Le diagramme d'activité se diffère de celui d'état transition par le fait que le diagramme d'activité fournit une spécification d'un comportement et non, comme les diagrammes d'interaction, un seul scénario possible (Fyama).

Figure N° 3 Diagramme d'activité métier



Source : Auteur

2.1.1. Risques identifiés

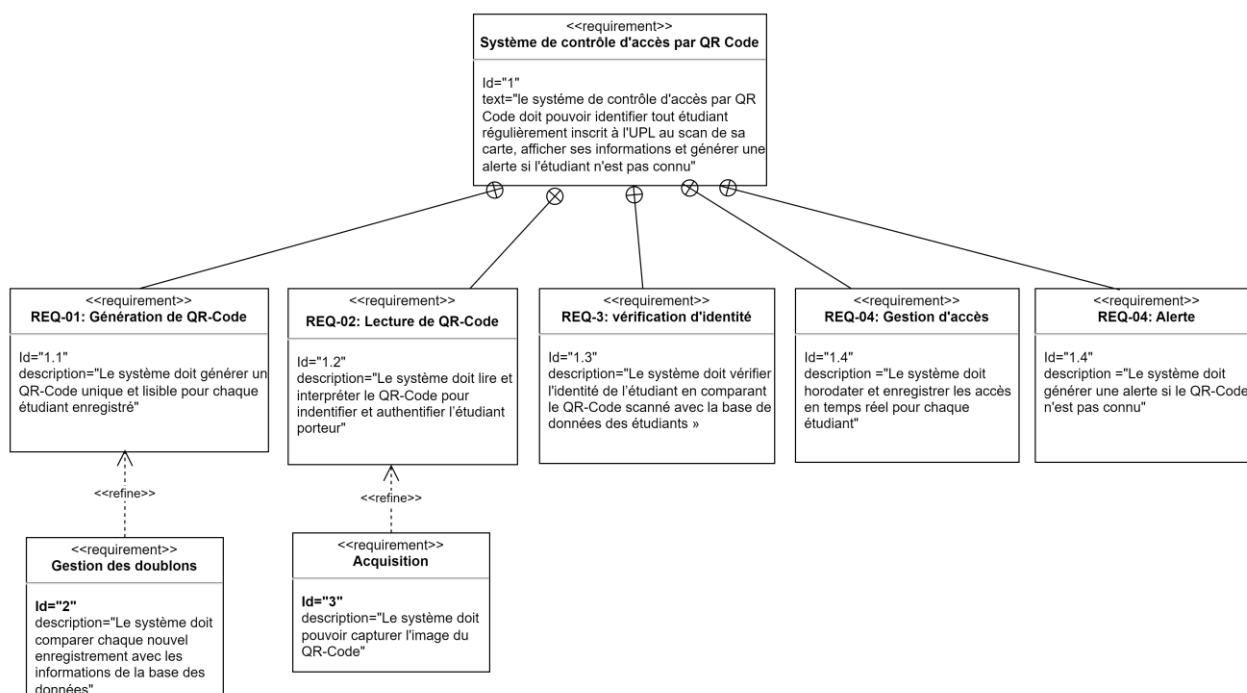
Les risques identifiés dans le processus actuel de contrôle d'accès incluent les intrusions, les falsifications et l'absence de traçabilité. En premier lieu, le manque de fiabilité constitue un problème majeur : la vérification manuelle des cartes d'étudiant et des pièces d'identité est sujette à des erreurs humaines, pouvant entraîner des accès non autorisés ou des refus injustifiés. Ensuite, le processus se révèle inefficace, car il est souvent lent et fastidieux, notamment durant les heures de forte affluence. De plus, l'absence de traçabilité complique le suivi des entrées et sorties, rendant difficile l'identification des personnes présentes dans la cour à un moment donné. Enfin, le risque de fraude est élevé, puisque les cartes d'étudiant et les pièces d'identité peuvent être falsifiées ou perdues, offrant ainsi une opportunité à des individus non autorisés d'accéder à la cour.

2.2. Identification des besoins système

2.2.1. Diagramme des exigences

Un diagramme des exigences SysML est une représentation visuelle utilisée pour spécifier et organiser les exigences d'un système. Il permet de représenter les relations entre les différentes exigences, les acteurs du système et les éléments de conception (Belloir et al., 2008).

Figure N° 4 Diagramme des exigences système



Source : Auteur

2.2.2. Identification des acteurs

Les principaux acteurs sont les utilisateurs du système, ils sont en générale faciles à repérer. Chaque acteur doit être nommé, mais pour trouver son nom, il faut penser à son rôle dans le système, un acteur représente l'ensemble cohérent de rôles joués vis-à-vis d'un système mais plusieurs personnes peuvent avoir le même rôle, les différents acteurs recensés dans les cas de ce système sont (GENDRE, 2012):

1. Etudiant ;
2. Administrateur ;
3. Système de contrôle ;
4. Alarme ;
5. Moniteur ;
6. Lecteur de QR-Code.

2.2.3 Identification des cas d'utilisations

L'identification des cas d'utilisation SysML est une étape cruciale dans le processus de modélisation d'un système, qui consiste à définir et à documenter les fonctionnalités principales que le système doit offrir à ses utilisateurs externes, voici les cas d'utilisation principaux :

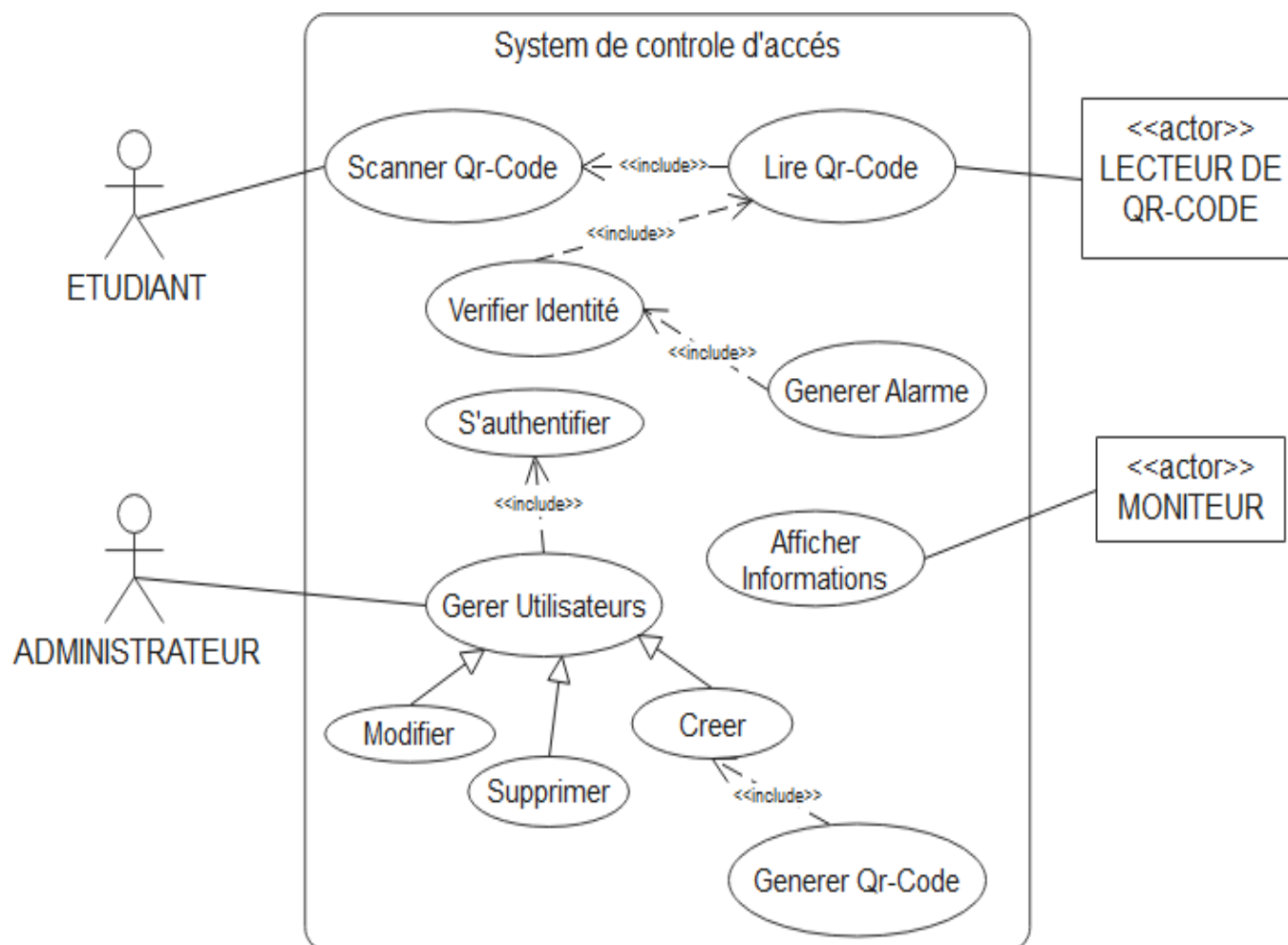
1. **Scanner QR-Code**
2. **Lire QR-Code**
3. **Vérifier identité**
4. **Afficher information**
5. **Générer Alarme**
6. **S'authentifier**
7. **Gérer utilisateur (CRUD)**
 - Créer
 - Modifier
 - Supprimer
8. **Générer QR-Code**
 - Générer
 - Supprimer
 - Rechercher

3. Conception du système de contrôle d'accès des étudiants

3.1. Diagramme de cas d'utilisation

Un diagramme de cas d'utilisation SysML est une représentation visuelle utilisée pour modéliser les interactions entre un système et ses acteurs externes. Il permet de décrire les fonctionnalités offertes par le système et comment les utilisateurs interagissent avec lui pour atteindre leurs objectifs (GENDRE, 2012).

Figure N° 5 Diagramme de cas d'utilisation système



Source : Auteurs

3.2. Description textuelle des cas d'utilisation

La description textuelle désigne une représentation détaillée et structurée d'un système, composant ou processus sous forme de texte narratif, sans diagrammes graphiques.

1. Cas d'utilisation : S'Authentifier

Acteur principal : Utilisateur

Objectif : ce cas d'utilisation permet de s'authentifier sur le système informatique, afin que chaque utilisateur puisse accéder aux fonctionnalités du système.

- Pré condition : Ouvrir l'application/ Demander formulaire d'authentification.
- Scenario nominal :

1. Remplir les informations sur le formulaire ;

2. Soumettre formulaire d'authentification ;
3. Le système vérifie et répond par un message de succès.

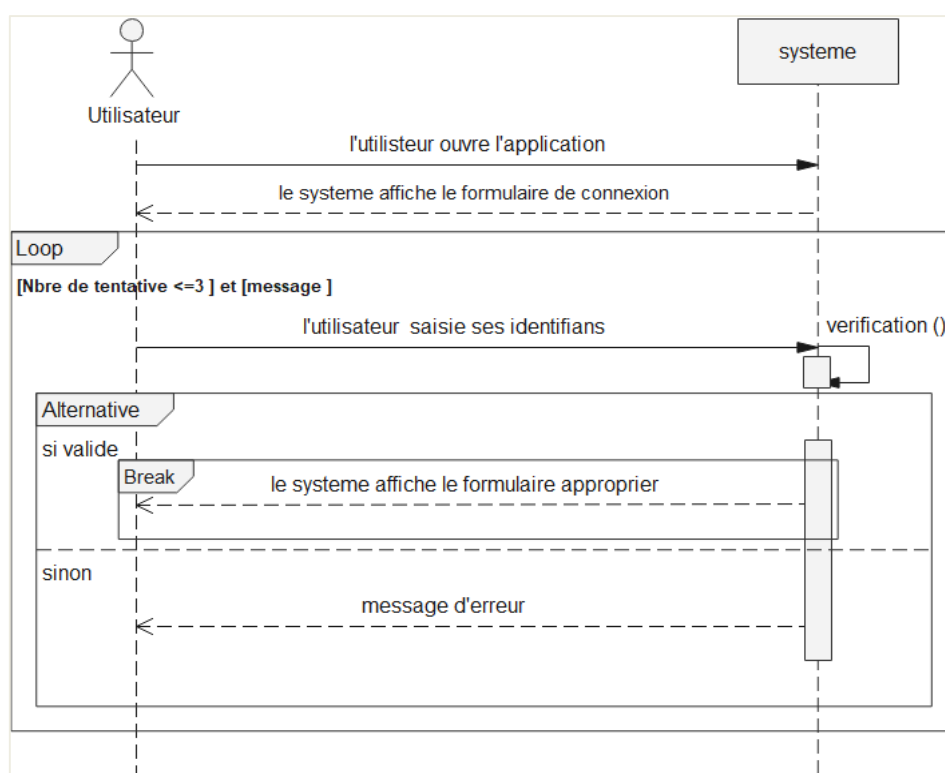
➤ Scenario alternatif :

1. a saisie des informations incorrectes, le système détecte et affiche un message d'erreur formulaire incorrecte, le cas d'utilisation s'arrête et reprise de la première phase du scenario nominal.

➤ Post condition :

Authentification réussi.

Figure N° 6 Diagramme de séquence s'authentifier



Source : Auteurs

2. Cas d'utilisation : Gérer Utilisateurs

Acteur principal : Administrateur

Objectif : Ce cas d'utilisation permet à l'administrateur de gérer les utilisateurs du système de contrôle d'accès. Cela inclut la création, la modification ou la suppression des comptes utilisateurs et de leurs accès.

Pré condition :

1. Être authentifié sur le système.
2. Accéder au module de gestion des utilisateurs.

Scénario nominal :

- L'administrateur accède au menu « Gérer Utilisateurs ».
- Le système affiche la liste des utilisateurs.
- L'administrateur choisit une opération (Créer, Modifier ou Supprimer).
- Le système affiche le formulaire correspondant.
- L'administrateur remplit ou modifie les informations nécessaires.
- L'administrateur valide l'opération.
- Le système vérifie les informations saisies.
- Le système enregistre les modifications dans la base de données.
- Le système affiche un message de succès.

Scénario alternatif :

- a. Si les informations saisies sont incorrectes ou incomplètes, le système détecte l'erreur et affiche un message d'erreur. Le cas d'utilisation reprend à l'étape 5 du scénario nominal.
- b. Si l'utilisateur existe déjà lors de la création, le système affiche un message « utilisateur déjà existant ». Le cas d'utilisation reprend à l'étape 5 du scénario nominal.
- c. Si une erreur de connexion à la base de données survient, le système affiche un message d'échec et le cas d'utilisation s'arrête.

Post condition :

1. Les informations des utilisateurs sont mises à jour.
2. Le compte utilisateur est créé, modifié ou supprimé avec succès.
3. Un QR-Code peut être généré pour un nouvel utilisateur.

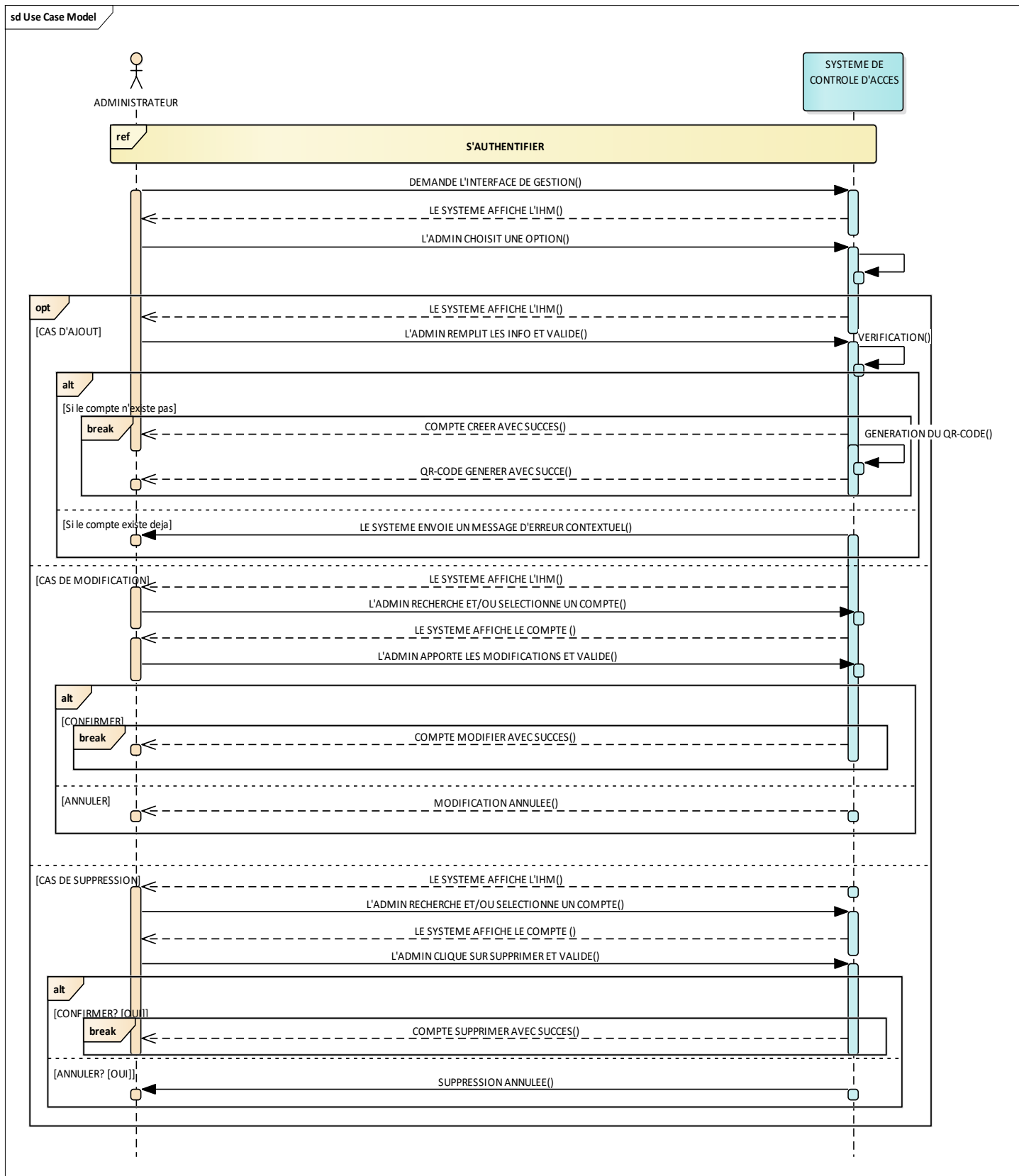


Figure N° 7 Diagramme de séquence de Générer Utilisateurs

Source : Auteur

3.3. Diagramme de définition de block

Le diagramme de définition de bloc (bdd : Block Definition Diagram) est un diagramme qui décrit la structure d'un système. Il est, avec le diagramme de bloc interne, un diagramme architectural (siloged, s.d.). Il décrit toutes les structures du système modélisé : Logiques, Matérielles et fonctionnelles.

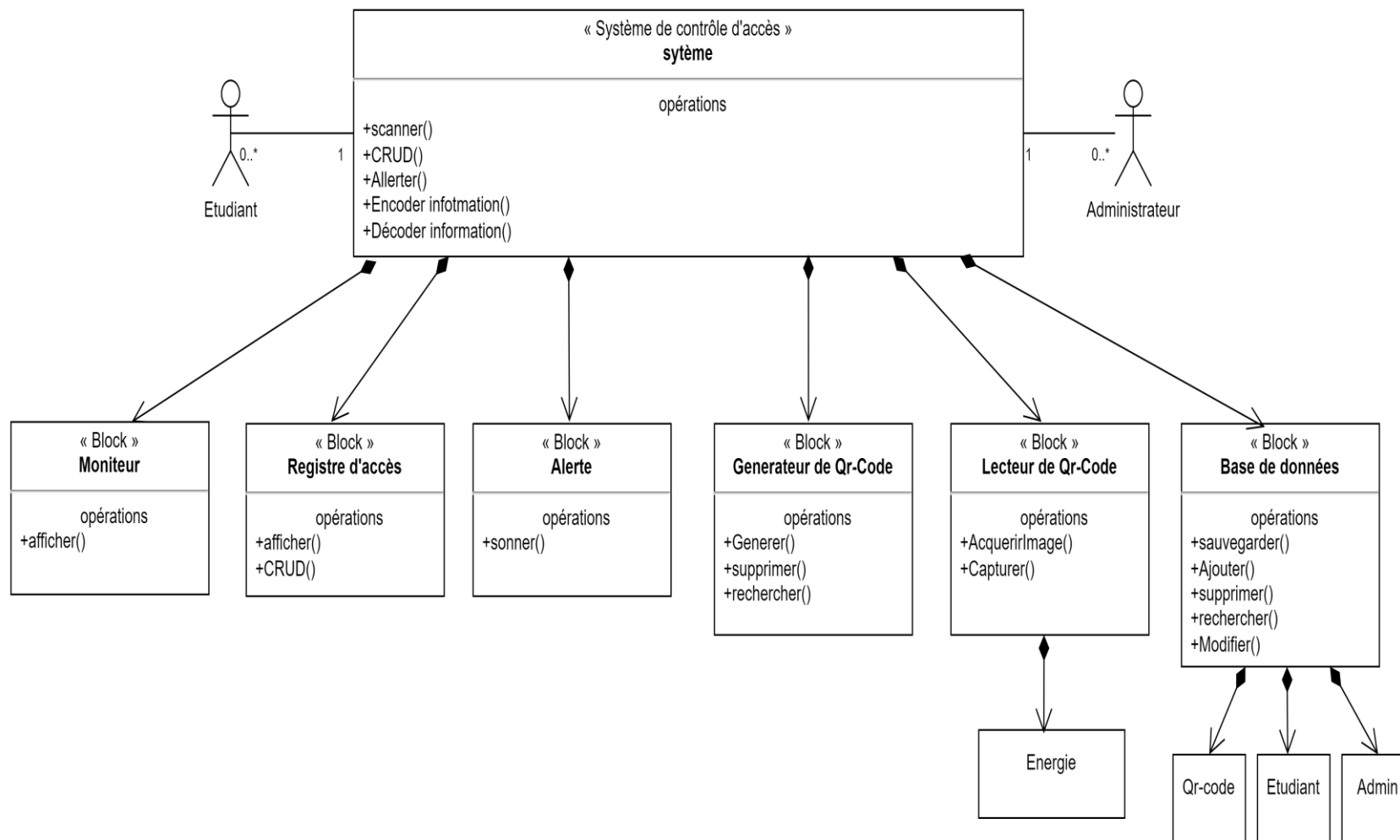
Le bloc représente le système complet, ou sous système ou un élément du système. Cela peut même être un composant. Un bloc est représenté graphiquement par un rectangle comportant plusieurs compartiments (GENDRE, 2012).

- Le compartiment supérieur contient le nom du bloc ;
- Le compartiment Operations détaille les actions réalisées par le bloc. Si le bloc représentait un petit programme, les opérations pourraient être les procédures de ce programme ;
- Le compartiment inférieur contient les paramètres qui définissent les instances du bloc : les parties, les références, les valeurs et/ou les propriétés.
- Le compartiment constraint permet de définir les contraintes de la fonction.

Dans un diagramme de définition bloc, il y a 3 relations possibles :

1. **La composition**, l'un des blocs est le contenant et l'autre est le contenu, mais le contenant n'a pas de raison d'être sans le contenu. Une relation de composition est représentée par un losange plein.
2. **L'association** représentée par un trait simple. Elle lie deux blocs égaux.
3. **L'agrégation** est identique à la composition, à la différence près que le contenu a une existence sans le contenant. Par exemple une salle de classe est composée de tables et de chaises mais sans tables ni chaise la salle peut encore être utilisée. Une relation d'agrégation est représentée par un losange vide.

Figure N° 8 Diagramme de Définition de Blocks

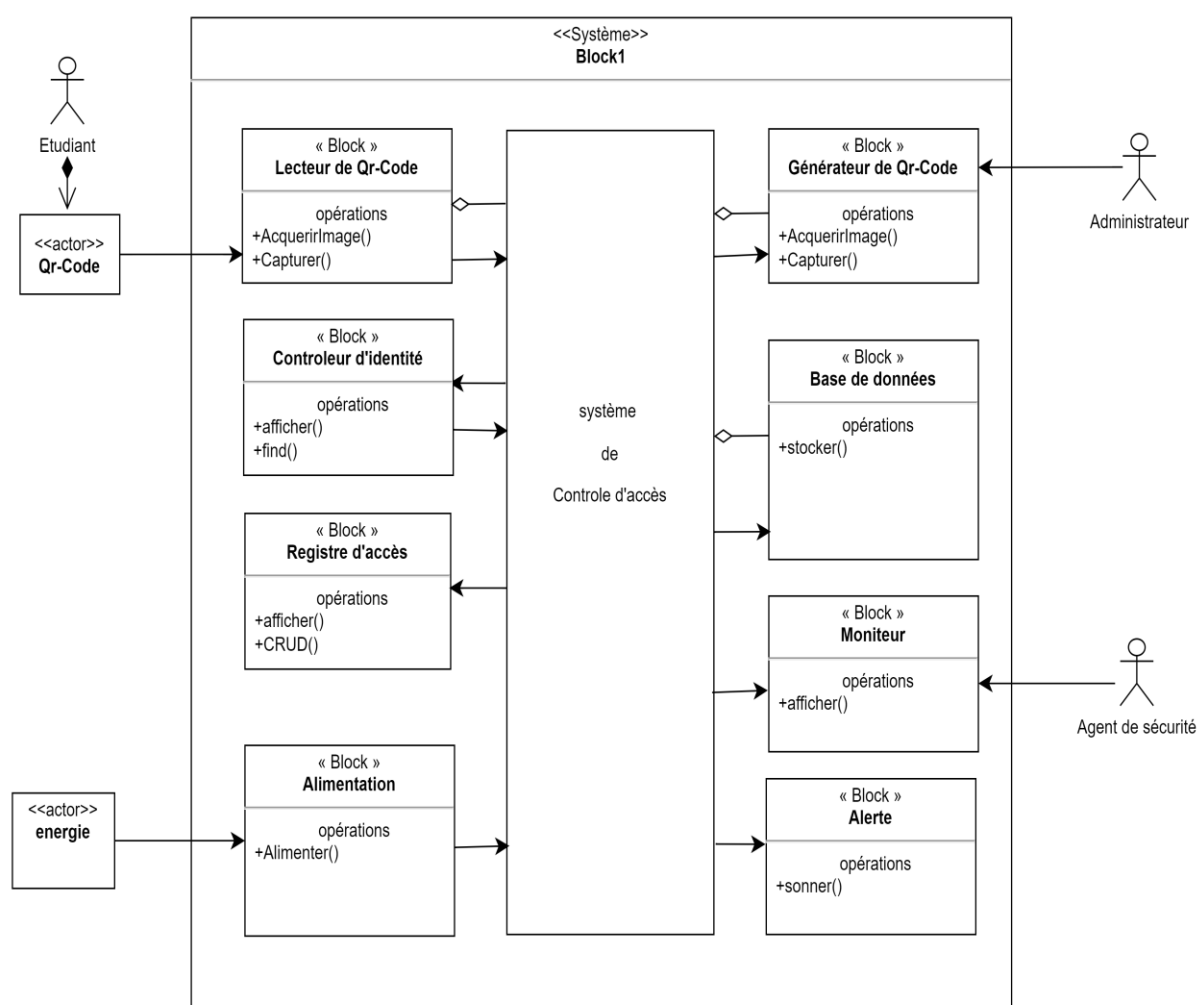


Source : Auteurs

3.4. Diagramme de block interne

Le diagramme de bloc interne modélise la structure interne d'un bloc. Il décrit les flux (MEI) et interactions entre des blocs qui caractérisent les fonctions (GENDRE, 2012). Un diagramme de bloc interne est obligatoirement un descendant d'un diagramme de bloc. On reconnaît le diagramme de bloc interne par les trois lettres ibd qui surplombent le diagramme.

Figure N° 9 Diagramme des Blocks Internes



Source : Auteurs

Discussion

La démarche UP/SysML adoptée présente plusieurs avantages par rapport aux méthodes de conception classiques telles que UP/UML, Merise ou BPMN. Contrairement à UML, dont SysML reprend sept diagrammes tout en supprimant les aspects trop logiciels et en ajoutant les diagrammes d'exigences et paramétrique, cette approche permet une traçabilité explicite entre les besoins exprimés et les éléments d'architecture, un atout pour un système de sécurité où chaque exigence (authentification, alerte, traçabilité) doit pouvoir être justifiée.

Par rapport aux approches RFID ou biométriques présentées en revue de littérature, le choix du QR-Code se justifie par son faible coût et sa compatibilité avec les smartphones déjà possédés par les étudiants, un critère déterminant dans le contexte du campus de l'UPL. Toutefois, cette solution présente des limites de sécurité intrinsèques notamment le risque de partage ou de capture d'écran du code que les travaux récents proposent de limiter par des mécanismes de QR-Code dynamique ou randomisé (Hendrawan et al., 2025).

Ce travail présente cependant des limites qu'il convient d'assumer explicitement. En premier lieu, seule la phase de conception a été traitée ; aucun prototype n'a été développé et aucune validation expérimentale (tests utilisateurs, simulation, comparaison avec UML ou Merise) n'a été réalisée. En second lieu, l'analyse des besoins repose sur une méthode qualitative dont la représentativité n'a pas été mesurée statistiquement. Ces limites ouvrent des perspectives de recherche futures, notamment l'implémentation d'un prototype fonctionnel et son évaluation en conditions réelles sur le campus.

Conclusion

La conception d'un système de contrôle d'accès basé sur le QR-Code pour le campus de l'Université Protestante de Lubumbashi illustre la pertinence d'une approche méthodologique rigoureuse combinant Unified Process (UP) et SysML. Cette démarche a permis d'analyser les besoins, d'identifier les acteurs et les cas d'utilisation, puis de modéliser une architecture intégrant des composants matériels (lecteurs QR-Code, serveurs, réseau) et logiciels (application, base de données). L'utilisation du QR-Code apporte une solution simple, économique et efficace pour automatiser l'authentification, renforcer la sécurité et assurer une traçabilité fiable des accès.

En s'appuyant sur l'ingénierie système et des outils de modélisation formels, ce travail démontre qu'il est possible de concevoir des systèmes complexes, évolutifs et adaptés au contexte



universitaire local. Cette approche constitue une base solide pour des développements futurs, notamment la réalisation d'un prototype fonctionnel et sa validation expérimentale par simulation ou test utilisateur. Les perspectives incluent également l'intégration de technologies émergentes telles que l'authentification multifactorielle, la reconnaissance biométrique, l'Internet des objets (IoT) pour une architecture de type Smart Campus, la blockchain pour garantir l'intégrité de la traçabilité des accès, ainsi que les architectures Zero Trust, afin de répondre aux exigences croissantes en matière de sûreté et de gestion intelligente des campus.

Bibliographie

- Alghamdi, A., Thanoon, M., & Alsulami, A. (2019). Toward a Smart Campus Using IoT: Framework for Safety and Security System on a University Campus. *Advances in Science, Technology and Engineering Systems Journal*, 4, 97–103. <https://doi.org/10.25046/aj040512>
- Belloir, N., Bruel, J.-M., Hoang, N., & Pham, C. (2008). *Utilisation de SysML pour la modélisation des réseaux de capteurs*.
- Crompton, H., LaFrance, J., & van 't Hooft, M. (2012). QR Codes 101. *Learning & Leading with Technology*, 39(8), 22–25.
- Fauzi, A., Mohamed, N. N., Hashim, H., & Saleh, M. (2020). *Development of Web-Based Smart Security Door Using QR Code System*. 13–17. <https://doi.org/10.1109/I2CACIS49202.2020.9140200>
- Hendrawan, J., Perwitasari, I. D., & Maulana, F. (2025). QR Code-Based Attendance Systems in Education: A Systematic Literature Review on Data Accuracy and Sustainable School Management. *Proceedings of The International Conference on Computer Science, Engineering, Social Science, and Multi-Disciplinary Studies*, 1, 80–87. <https://doi.org/10.64803/cessmuds.v1.14>
- K, R. A., & Rohann, S. (2026). Optimized QR Code-Based Authentication System for Attendance Management. *Acta Pedagogica Asiana*, 5(SI), Article SI. <https://doi.org/10.53623/apga.v5iSI.1124>
- Kruchten, P. (2000). *The Rational Unified Process—An Introduction* (p. 255).
- Mesnier, N. (n.d.). *Introduction à l'ingénierie système*.
(PDF) *Development of a Smart Lock System using QR Code Technology*. (n.d.). Retrieved July 27, 2026, from https://www.researchgate.net/publication/385764866_Development_of_a_Smart_Lock_System_using_QR_Code_Technology
- Sánchez-Torres, B., Rodríguez-Rodríguez, J. A., Rico-Bautista, D. W., Guerrero, C. D., Sánchez-Torres, B., Rodríguez-Rodríguez, J. A., Rico-Bautista, D. W., & Guerrero, C. D. (2018). Smart Campus: Trends in cybersecurity and future development. *Revista Facultad de Ingeniería*, 27(47), 104–112. <https://doi.org/10.19053/01211129.v27.n47.2018.7807>



SysML vs. UML: What's the Difference? | PTC. (n.d.). Retrieved January 8, 2026, from <https://www.ptc.com/en/blogs/alm/sysml-vs-uml>

Fyama, B. (n.d.). *Méthode d'analyse informatique : modélisation orientée objet*, p.39/UL/2017.

GENDRE, L. (2012). *SysML: un langage pour la modélisation des systèmes*. Paris: Univesité PARIS-SACLAY.

siloged. (n.d.). *siloged*. Retrieved 07 25, 2024, from https://www.siloged.fr/cours/STI2D_sysml/index.html?Exemplen2Controledacces.html