

Dossier Technique du projet « Accès campus » - Partie PEA

Sommaire

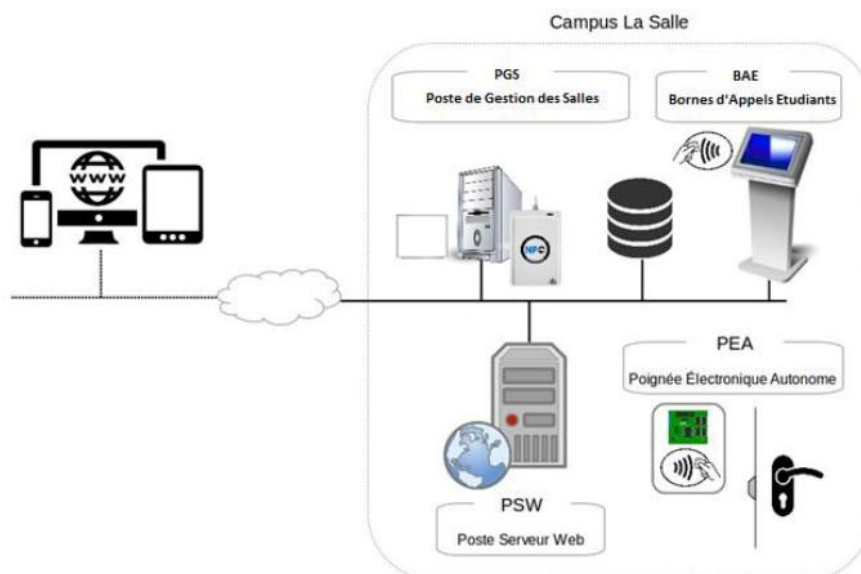
I – Introduction	2
Synoptique général et situation du projet dans son contexte industriel	2
II – Analyse fonctionnelle	3
Diagramme des cas d'utilisations	3
Le scénario	3
Le catalogue des acteurs	7
Le diagramme des exigences	7
III – La planification	9
IV - La conception	10
Recherche de solutions	10
La communication	11
L'alimentation	11
Le RFID	12
La gâche	12
Le digicode	13
L'affichage	13
Lecteur d'empreinte digitale optique	14
Autonomie	14
Microcontrôleur	14
Architecture réseaux	15
Diagramme de définitions de blocs	15
Diagramme de blocs internes	16
Schéma structurel	17
V – Les tests	18
Conclusion	19

I – Introduction

Le projet consiste en la création d'une solution d'accès pour les salles du Campus Saint Aubin La Salle qui permettra de contrôler l'accès aux salles de cours et de réaliser le contrôle de présence. L'accès se fera principalement avec le protocole RFID.

Synoptique général et situation du projet dans son contexte industriel

Le projet de contrôle d'accès campus peut être divisé en 5 grandes parties, chaque partie étant un projet soit électronique, soit informatique comme un serveur ou une interface homme-machine. Dans un premier temps, je vous présenterais rapidement les autres parties du projet, puis je vous partagerais plus en détail ma partie dans ce projet.



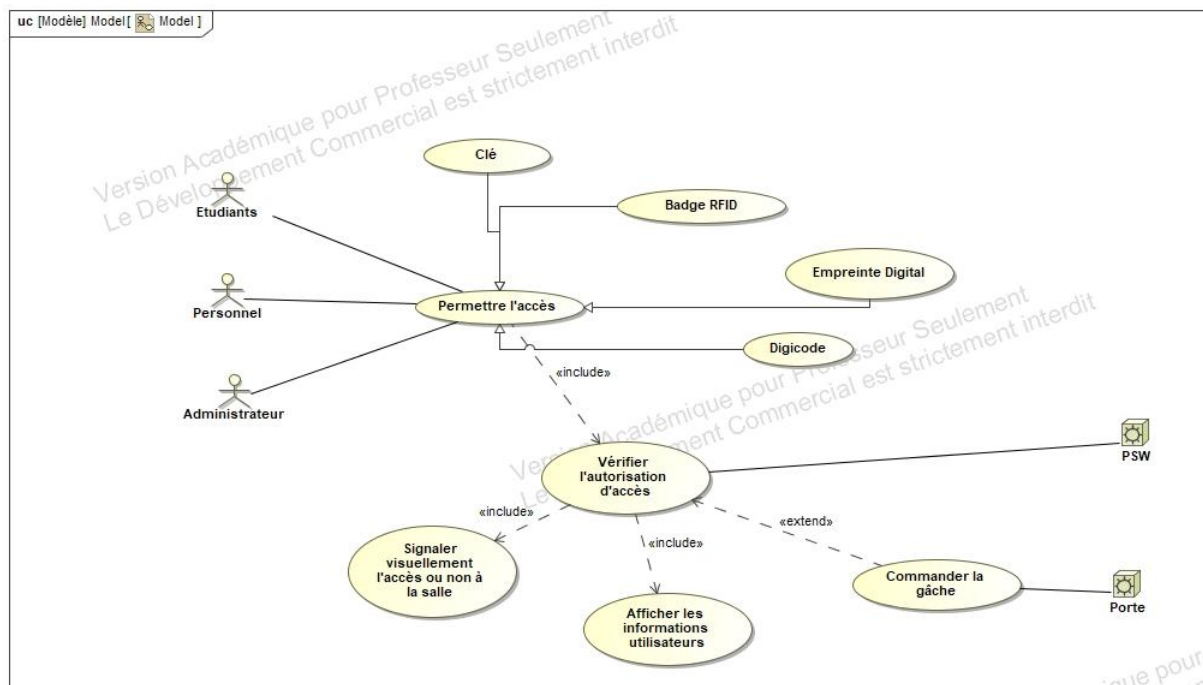
Tout d'abord, nous avons le **PSW** (poste serveur web). Le PSW sera une machine qui hébergera via un service WEB, une IHM qui permettra de visualiser la disponibilité des salles et les données de l'utilisateur. Elle permettra en plus de cela de réserver une salle. Sur cette même machine, nous pouvons aussi retrouver **une base de données** qui permettra de stocker toutes les informations et les données en lien avec la réservation des salles, les différents statuts des étudiants (retard, absence...), et les utilisateurs avec les badges. Nous avons ensuite le **PGS** (poste de gestion des salles) qui sera une application de management de badge et de salle pour les administrateurs. Pour les produits électroniques, il y a la **BAE** (Borne d'appel étudiant) et la **PEA** (Poignée électronique autonome). Commençons par la **BAE**, elle sera installée à l'entrée de chaque salle, elle permettra de faire des opérations simples, comme l'appel, et l'annonce d'un retard. Finissons par la **PEA**. Elle permettra l'ouverture d'une porte équipée d'une gâche électrique. La PEA est le produit dont je vais détailler la conception dans ce document.

II – Analyse fonctionnelle

Dans cette partie, je vous détaillerais le fonctionnement de la PEA à travers plusieurs diagrammes, schémas et tableaux. L'analyse fonctionnelle est une étape majeure dans la construction d'un projet en réseaux de ce type. Elle permettra de définir le fonctionnement de la PEA sous un grand nombre de facettes.

Diagramme des cas d'utilisations

Pour commencer, je vais vous introduire la PEA via le diagramme des cas d'utilisations proposé par le langage SysML.



Nous pouvons voir que la PEA utilisera plusieurs solutions pour permettre à l'accès à un utilisateur. Le badge RFID sera la solution principale pour avoir un accès à la salle. En effet, l'utilisateur présentera son badge pour faire une tentative d'accès. La PEA interrogera ensuite la base de données en donnant son identifiant fixe de badge. La base de données répondra par un oui ou un non, tout en envoyant les données de l'utilisateur (nom, prénom, statut...). Le diagramme ci-dessus nous permet de voir dans les grandes lignes les actions de la PEA.

Le scénario

Maintenant analysons ces cas d'utilisations à la loupe avec les scénarios. Les scénarios décrivent en détaille les actions du système.

Titre	Permettre l'accès	Réf	S1	Type	Détaillé
Résumé	L'opérateur souhaite accéder à une salle avec un badge RFID.				
Acteur(s)	Utilisateur, PEA, API de la BDD				
Fonctionnalités	Commander, communiquer		Responsable		Robin MARTINEAU
Création	01/03/24	Mise à Jour		Version	1.0
Préconditions	La solutions accès campus est connectée au réseau.				
Postconditions	Aucune				
Déclenchement	C'est l'utilisateur qui déclenche quand il veut.				

Scénario nominal :

1	L'utilisateur présente son badge RFID	La PEA lit l'identifiant du badge RFID de l'utilisateur La PEA prépare et envoie une requête HTTP pour interroger la base de données et transmettre l'horodatage.	L'API reçoit le message, interroge la base de données, et alimente les logs. L'API prépare la réponse affirmative pour la PEA (Nom, prénom, classe) et l'envoie.	
2				
3				
3				
4				
4				
5				
5				
6		La PEA reçoit la requête et la traite. La PEA commande la gâche afin d'ouvrir la porte et affiche les informations de l'utilisateur sur l'écran OLED.		
7				
7				

Scénario alternatif :

A1	Le badge de l'utilisateurs est invalide		
Validité	5		
1 1 1 2 3 3 3		La PEA reçoit la requête et la traite. La PEA informe l'utilisateur qu'il n'a pas de droit d'accès à cette salle et affiche ses informations.	L'API prépare la réponse affirmative pour la PEA (Nom, prénom, classe) et l'envoie.
Fin	7		

Scénarios d'Exception :

E1	Le badge de l'utilisateurs est défectueux	Badge partiellement lisible	
Validité	2		
1 1 2		La PEA n'arrive pas à lire l'identifiant fixe du badge. Il en informe l'utilisateur avec un message d'erreur « Badge défectueux »	
Fin	2		

E2	Le badge de l'utilisateurs est défectueux	Badge indetectable	
Validité	2		
1 2		La PEA ne détecte rien. Rien ne se passe.	
Fin	2		

Bien sûr, d'autres scénarios sont à prévoir. Nous n'avons pu traiter ici que le cas du badge RFID, mais la PEA dispose de d'autres périphériques permettant l'authentification. Elle peut identifier ses utilisateurs par le biais de la biométrie (l'empreinte digitale), par le biais d'une clé, ou encore par le biais d'un digicode. Ces périphériques seront utilisés dans d'autre circonstance. Par exemple, le digicode permettrait à des invités d'ouvrir une salle en particulier, sans avoir de badge RFID en leur possession, en attribuant un code à durée limité pour l'ouverture de la porte. Nous avons attribué l'empreinte digital à des utilisations plus régulière, pour le personnel, ou les administrateurs par exemple. *(Vous pourrez retrouver le reste des scénarios en annexe)*

Toutes ces données seront stockées dans une base de données, qui gèrerais les requêtes via une API.

Le catalogue des acteurs

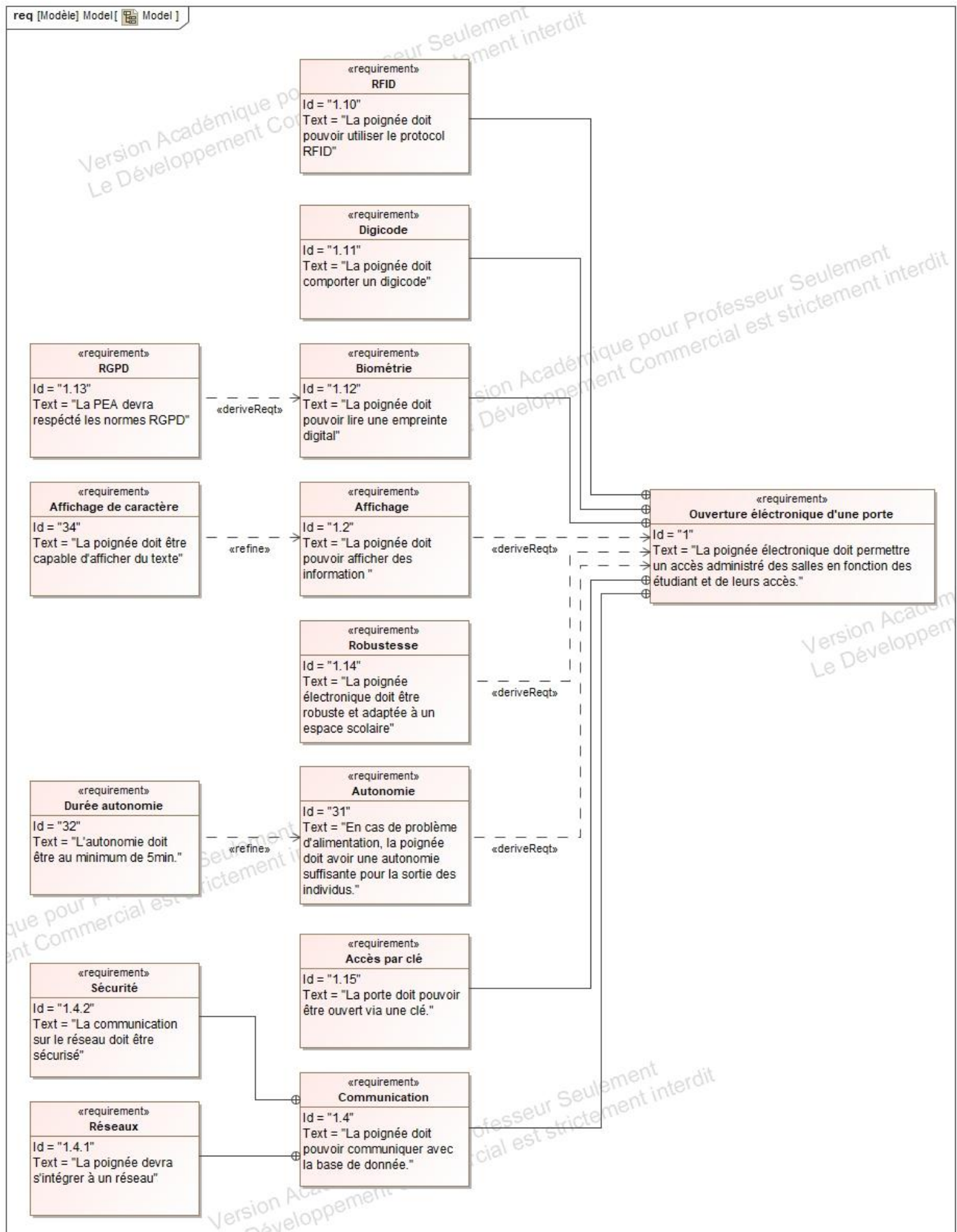
Le tableau ci-dessous liste tous les acteurs en lien avec la PEA.

Acteur	Rôle
Etudiant(s)	Les étudiant possèderons un accès par badge RFID à certaine salle.
Administrateur(s)	Les administrateurs possèderont un accès par badge RFID, et un accès par empreinte digitale.
Le personnel, professeur	Ces personnes possèderont un accès par badge RFID, et accès par empreinte digital en fonction de la fréquentation des salles.
Base de données (PSW)	La base de données devra répondre aux requêtes de la PEA, tout en lui envoyant des données en lien avec l'utilisateur.
Porte	La porte sera ouverte par le biais de la gâche.

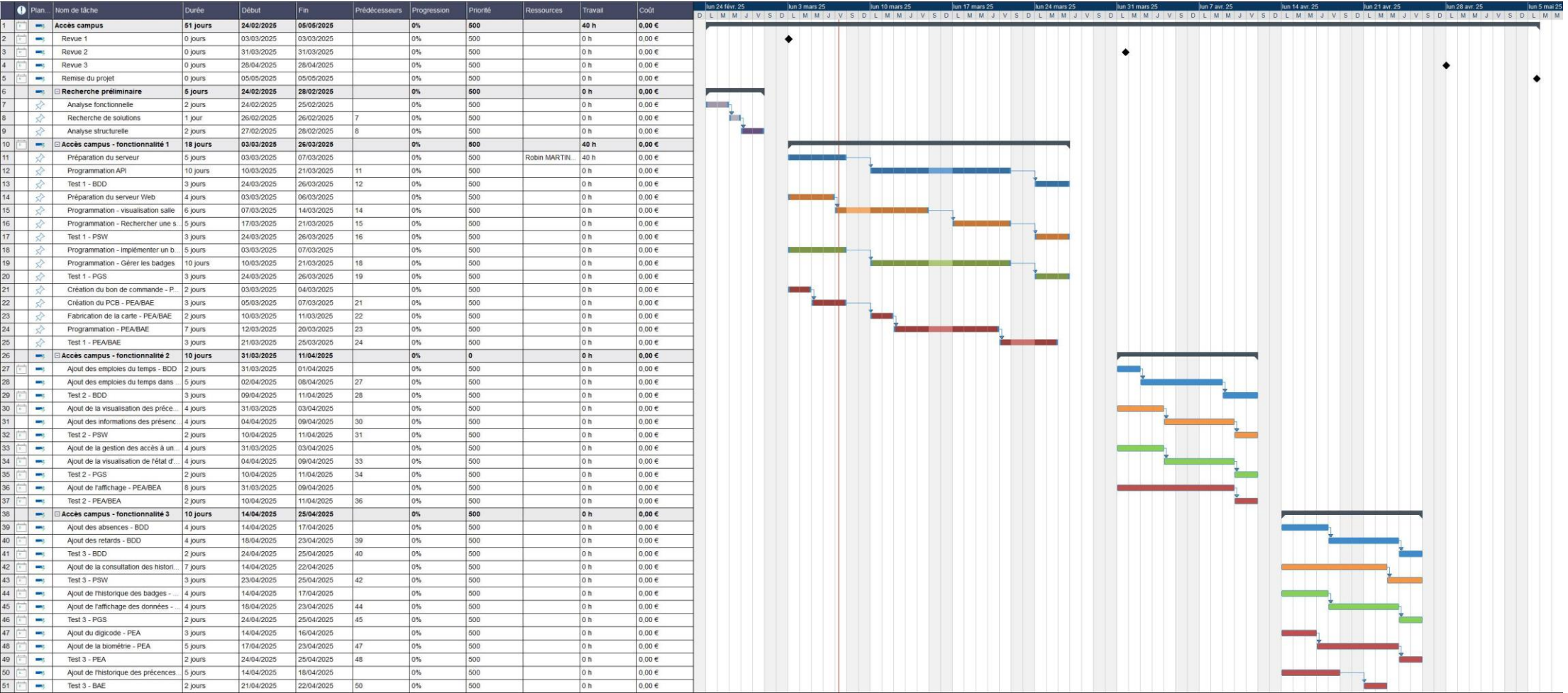
Le diagramme des exigences

Le diagramme des exigences dans le langage SysML permet de définir les exigences techniques et physique d'un objet. Ci-dessous vous pourrez retrouver le diagramme des exigences de la PEA.

Nous pourrons retrouver dans ce diagramme des exigences en lien avec la robustesse du système, en lien avec la sécurité, ou encore en lien avec des normes. Les diagrammes des exigences permettraient de définir précisément nos solutions par la suite.



III – La planification



La planification ci-dessus, nous permet, de nous situer dans le temps imparti pour rendre un système fonctionnel. Nous pouvons voir à travers la répartition des tâches principales que nous utilisons une méthodologie incrémentale. Cette méthodologie nous permet d'obtenir, quoi qu'il arrive au moins une partie des cas d'utilisations du projet fonctionnelle. Par exemple, nous pouvons voir la 2 deuxième tâche principale qui est pour notre part le projet minimal. C'est-à-dire que la tâche numéro 2 consiste en l'implémentation du RFID et de la communication avec la base de données. Chacune des grandes tâches se conclut par une phase de test, permettant de tester l'incrémentation dans son ensemble. Dans la planification, nous pouvons voir que les tâches principales sont illustrées par un crochet noir (nos tâches principales). Nos tâches principales sont communes à tout le groupe. Ensuite, nous avons les sous tâches, qui sont illustrés par des couleurs sur la planification. Ces sous tâches sont relatifs à chacune des parties du projet.

Les losanges en haut de la planification représentent nos jalons. Les jalons correspondent pour nous, aux différentes revues et aux moments importants de notre projet. Les 3 premiers jalons correspondent aux 3 revues, et le dernier correspond à la remise du projet.

La revue 2 est un jalon majeur de la planification, car nous devons rendre un prototype fonctionnel du projet. Il a donc été décidé de garder 2 jours de marge afin de pouvoir corriger une incertitude de dernière minute. Dans le cas, où nous avons de l'avance nous pourrions poursuivre sur l'incrément numéro 2.

Je vais maintenant vous citer à quoi corresponde les différents incréments. Comme cité plutôt, l'incrément de base, est lié aux fonctions de base du système « accès campus ». Nous pouvons retrouver dans l'incrément de base, les fonctions en lien avec l'identification par badge RFID, la vérification par l'interrogation de la base de données, et la manipulation de la gâche. Pour imager, nous retrouverons dans cet incrément tous les éléments du scénario S1. Ensuite, nous l'incrément numéro 1 en lien avec l'affichage des informations. Nous verrons par la suite comment seront affichées ses informations. Pour la PEA, il y aura en plus de cela l'ajout du digicode dans son fonctionnement. Et enfin l'incrément numéro 2 permettra d'ajouter les dernières fonctionnalisées à notre projet. Pour la PEA, nous aurons donc une poignée qui sera terminée.

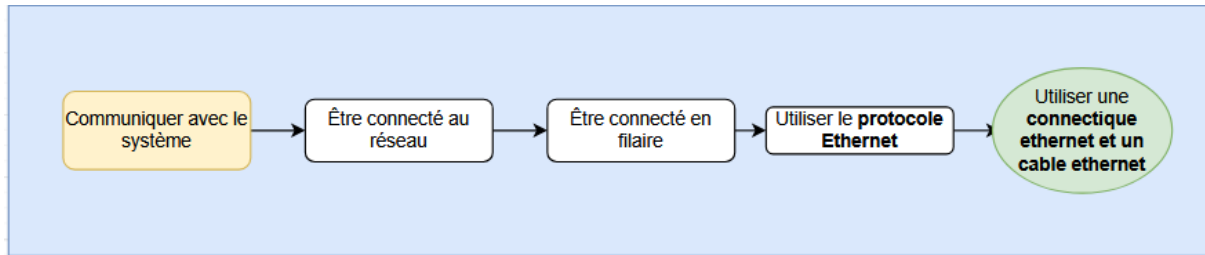
IV - La conception

Dans cette partie je vais vous parler de l'analyse structurelle de la PEA. Je vous parlerais dans un premier temps des solutions que j'ai pu trouver pour répondre aux exigences et au besoin du projet. Dans une seconde partie, je vous parlerais, à travers un diagramme de définition de blocs, de toutes les fonctions et les opérations que devons exécuter les différentes composantes du projet. Je continuerais ensuite avec le diagramme de blocs internes, ce diagramme permettra de définir tous les flux au sein du module PEA. Pour finir, j'ajouterais quelques détails sur les badges RFID, sur le réseau et ça configuration, et aussi sur l'affichage.

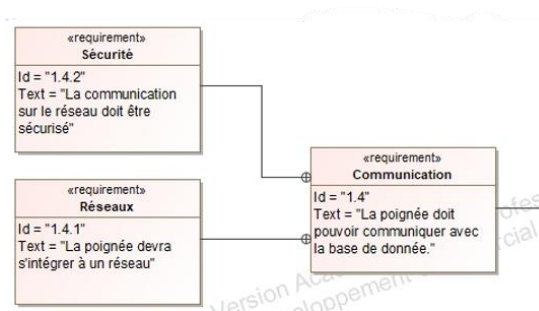
Recherche de solutions

Commençons par la recherche de solutions. Pour la recherche de solutions j'ai utilisé un diagramme de FAST. Ce diagramme permet de voir les détails ressortant d'un cas d'utilisation ou d'un besoin, tout en répondant aux exigences demandées.

La communication



Pour la communication, nous allons utiliser le protocole Ethernet. Nous devons avoir une communication sécurisée entre la base de données et la PEA, car des informations en lien avec le RGPD et les données personnelles de l'utilisateur (la biométrie par exemple). La communication filaire permet d'éviter les possibles portes d'entrées, avec le WiFi par exemple. Pour renforcer la sécurisation des données, nous pouvons utiliser des échanges de certificat entre la BDD et la PEA pour sécuriser la communication.

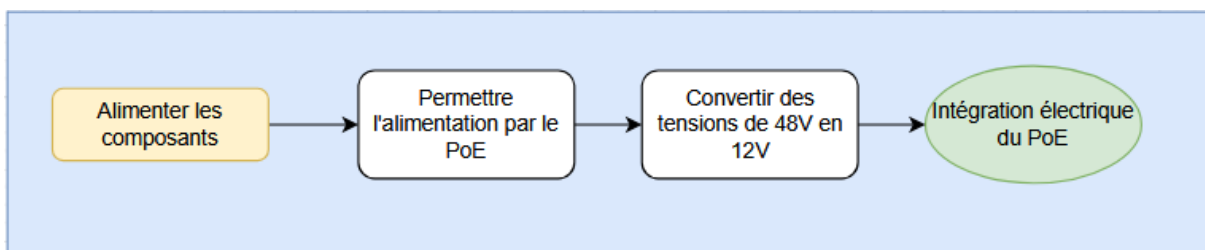


Autre avantage de l'Ethernet est sa capacité d'alimentation avec la technologie PoE. Cette technologie nous permet d'obtenir une alimentation de 15,4W et de 48V pour le module.

J'ai choisi comme composant pour gérer l'Ethernet un « Wiznet W5500 ». Ce permet de communiquer en Ethernet et il est équipé d'une pile TCP/IP.

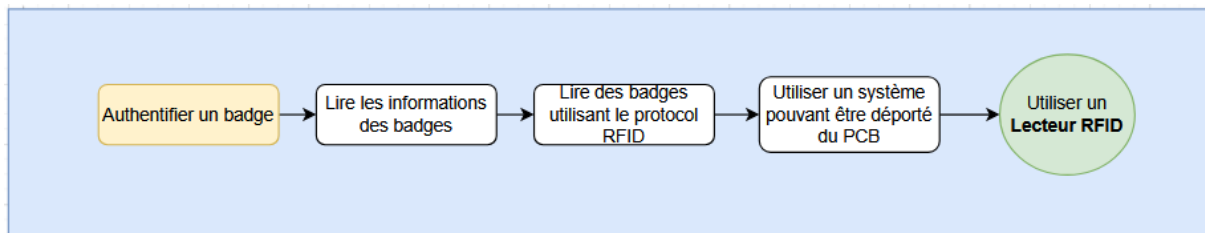
Exigences en lien avec la communication

L'alimentation



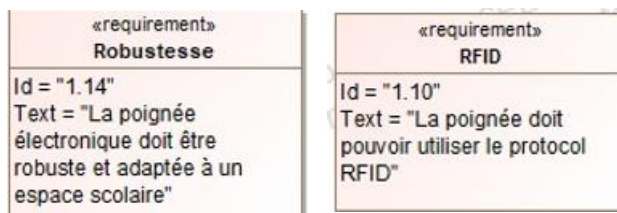
Comme nous venons de parler du PoE, je vais donc maintenant vous parler de la solution trouver pour alimenter la PEA. Le PoE fournit une tension de 48V avec une puissance de 15,4W. Pour transformer l'alimentation, il va falloir de multiple composant comme des ponts de diodes pour supprimer les variations de tensions, un transformateur pour changer la tension en une tension compatible avec les composants... Pour traiter tout ces besoins, je vais utiliser le composant Silvertel AG9700. Couplé à un port Ethernet adapté pour le PoE, la PEA pourra être alimenté.

Le RFID



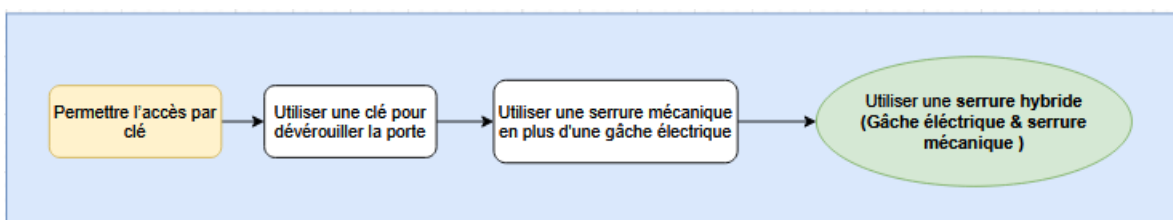
Le RFID est le moyen d'authentification principale de la PEA. Il sera utilisé pour tout le monde. Nous disposons déjà de matériel permettant de remplir nos exigences. C'est-à-dire un périphériques RFID robuste. Je parle ici du « LECHEM-WDT.

Mise à part sa robustesse très peu de chose diffère d'un lecteur RFID classique.

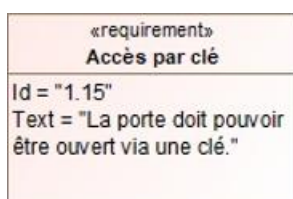


Cependant, il reste un besoin important à gérer, ce besoin est l'identification des badges par un attribut fixe. Cet identifiant fixe, va nous permettre d'attribuer un identifiant à chaque badge et donc de lier une personne à cet identifiant. La mémoire des badges RFID peut être manipulé facilement avec le matériel adapté. Si nous nous étions basés sur des données en mémoire de la carte, un utilisateur externe pourrait très bien usurper l'identité d'un administrateur. Des badges RFID équipé de la norme MIFARE possèdent un identifiant fixe.

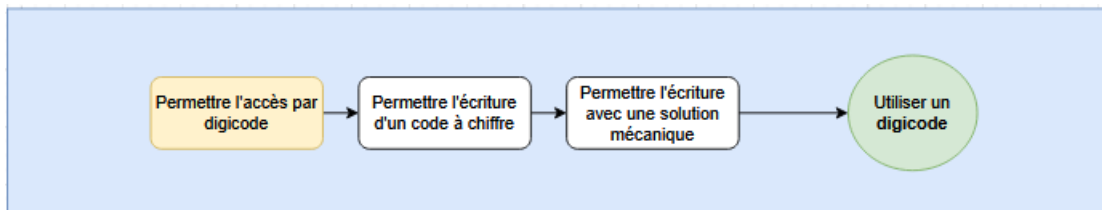
La gâche



Pour la gâche, nous avons déjà une solution fonctionnelle à disposition (GA30), nous allons pouvoir combiner la gâche électrique et une poignée de porte déverrouiller uniquement par clé de l'extérieur pour pouvoir répondre à l'exigence de l'ouverture par clé.



Le digicode

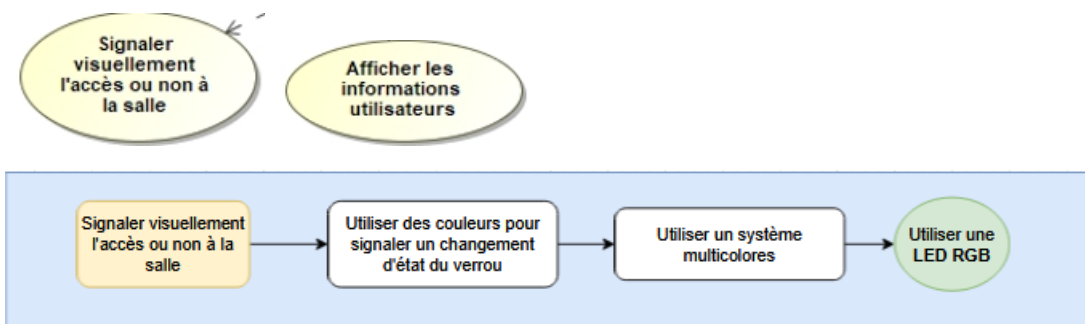


Pour le digicode, j'ai cherché une solution robuste. J'ai trouvé le PMOD KYPD 16 buttons.

«requirement» Robustesse
Id = "1.14" Text = "La poignée électronique doit être robuste et adaptée à un espace scolaire"

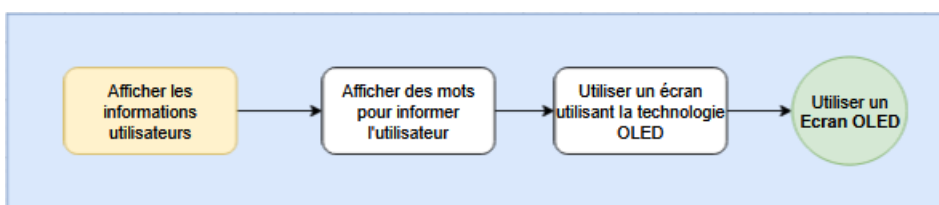
L'affichage

Pour l'affichage, je pensais utiliser 1 solution différente, pour les 2 cas d'utilisations suivant :

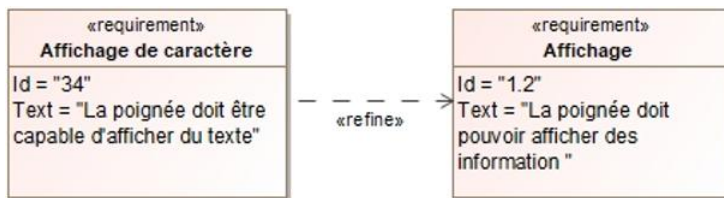


Pour signaler l'accès à la salle, j'ai prévue d'utiliser une LED RGB. La LED s'allumera en vert, si la gâche est déverrouiller et si elle reste verrouiller elle s'allumera en rouge.

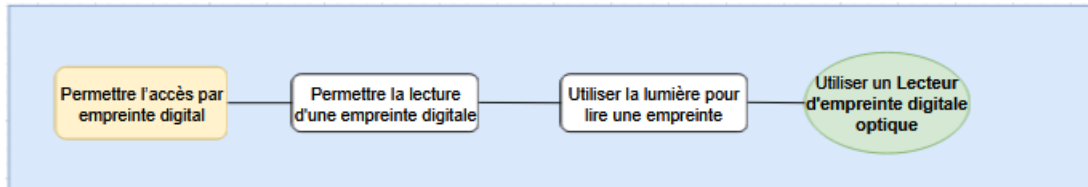
Pour le cas d'utilisation en lien avec les informations de l'utilisateur à afficher, nous pouvons utiliser un écran OLED.



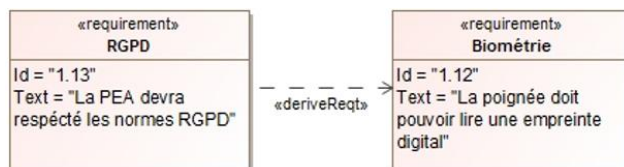
L'écran OLED nous permettra de répondre au besoin d'afficher des caractères (les informations).



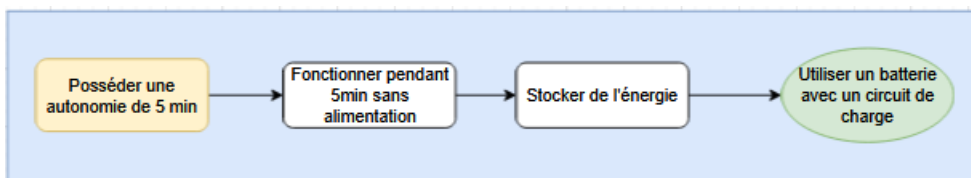
Lecteur d'empreinte digitale optique



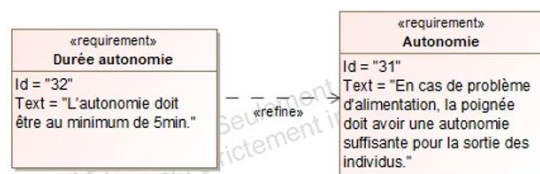
Pour le lecteur d'empreinte digital, nous allons utiliser une solution que nous avons déjà à notre disposition le capteur **R305**. Se capteur sera largement suffisant pour l'utilisation de la biométrie.



Autonomie

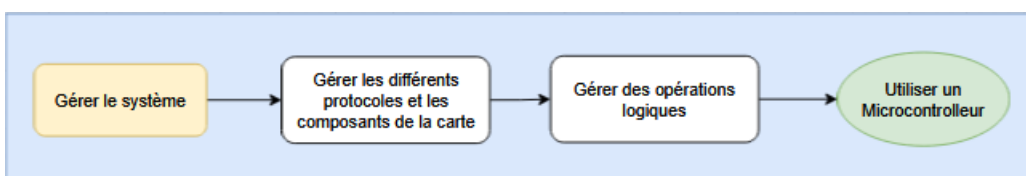


Pour l'autonomie, nous avons prévu d'utiliser une batterie avec un circuit de charge pour pouvoir alimenter la PEA, et lui permettre de faire les opérations de base.



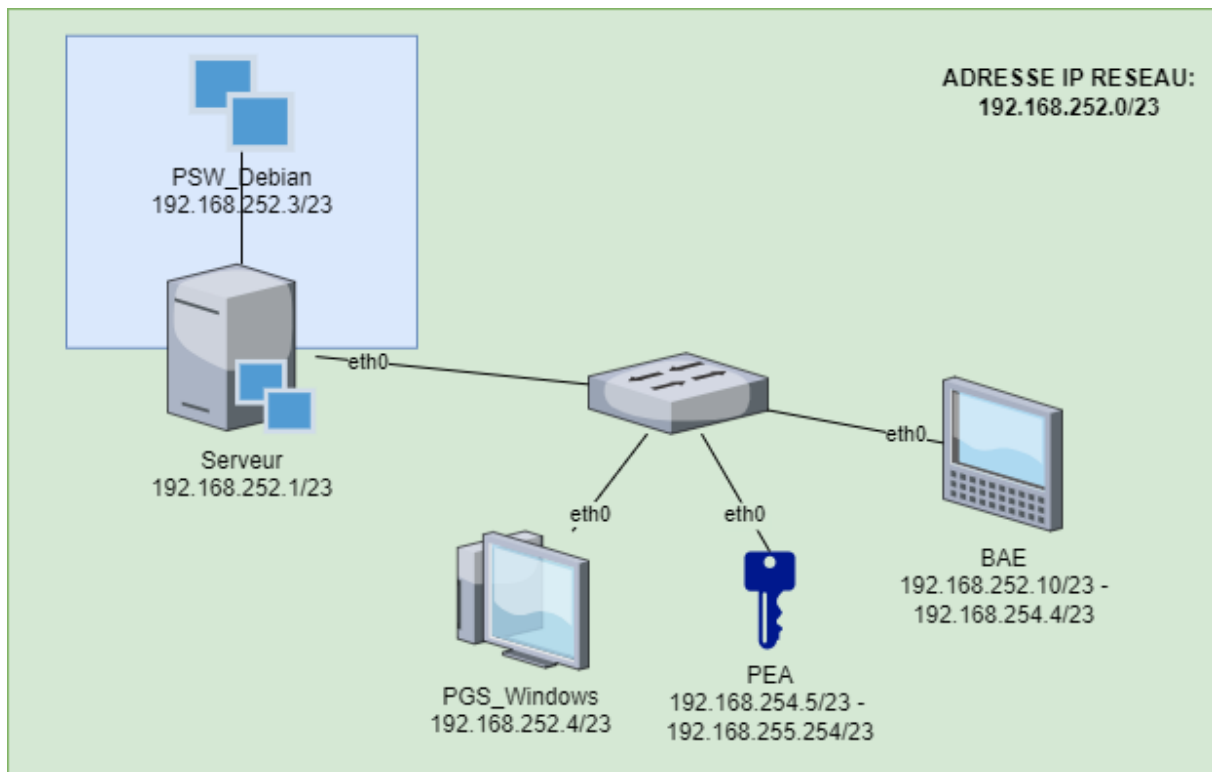
Microcontrôleur

Le microcontrôleur est un composant clé pour notre projet, car c'est lui qui va permettre à tous nos composants de communiquer entre eux.



Pour le microcontrôleur, j'ai choisi d'utiliser un STM32, car il possède des performances largement suffisantes pour les opérations qu'il a effectué. J'ai choisi un microcontrôleur de la gamme F. Cette gamme est la gamme de base des STM32.

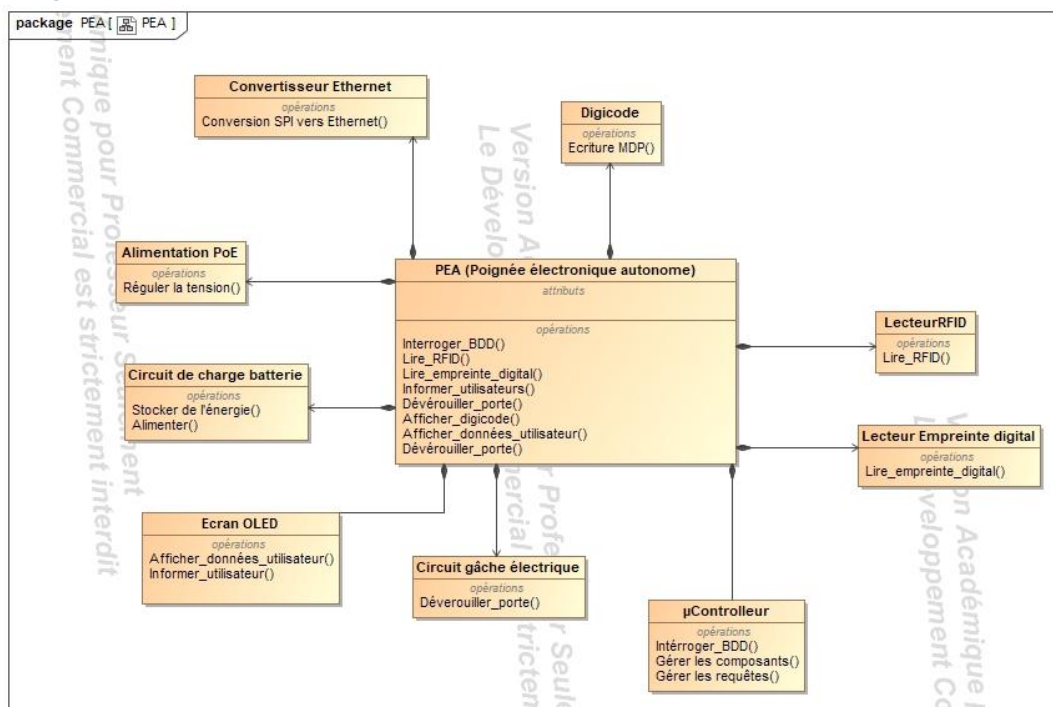
Architecture réseaux



Le schéma Réseaux ci-dessus montre de quelle façon seront connecté les éléments du projet entre eux. Nous pouvons voir que les PEA seront identifier par une adresse IP comprise entre 192.168.254.5 et 192.168.255.254 avec un masque de sous réseau codé sur 23 bits.

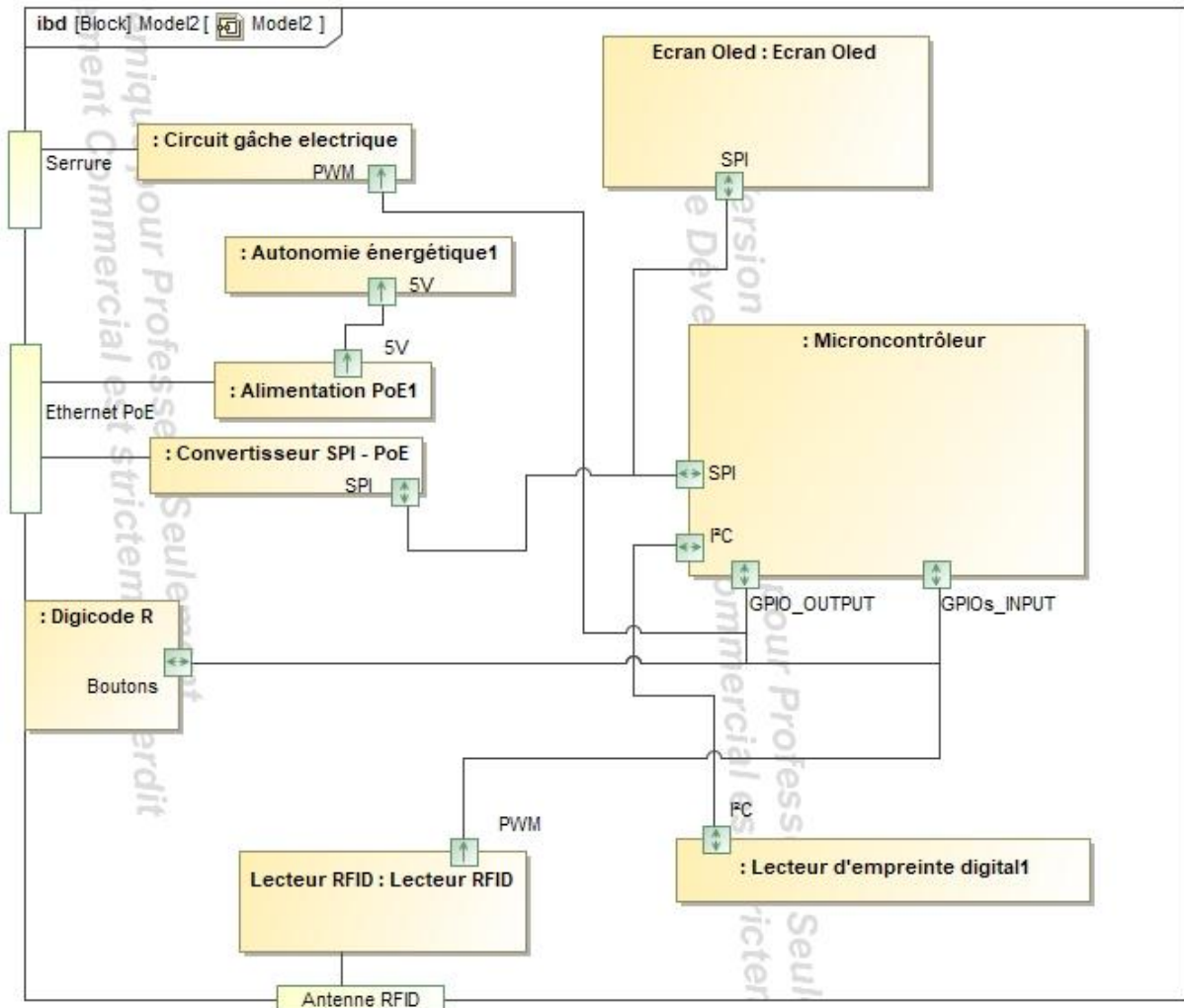
La PEA sera donc en lien avec tout le système accès campus, même si elle ne communiquera qu'avec la base de données du PSW.

Diagramme de définitions de blocs



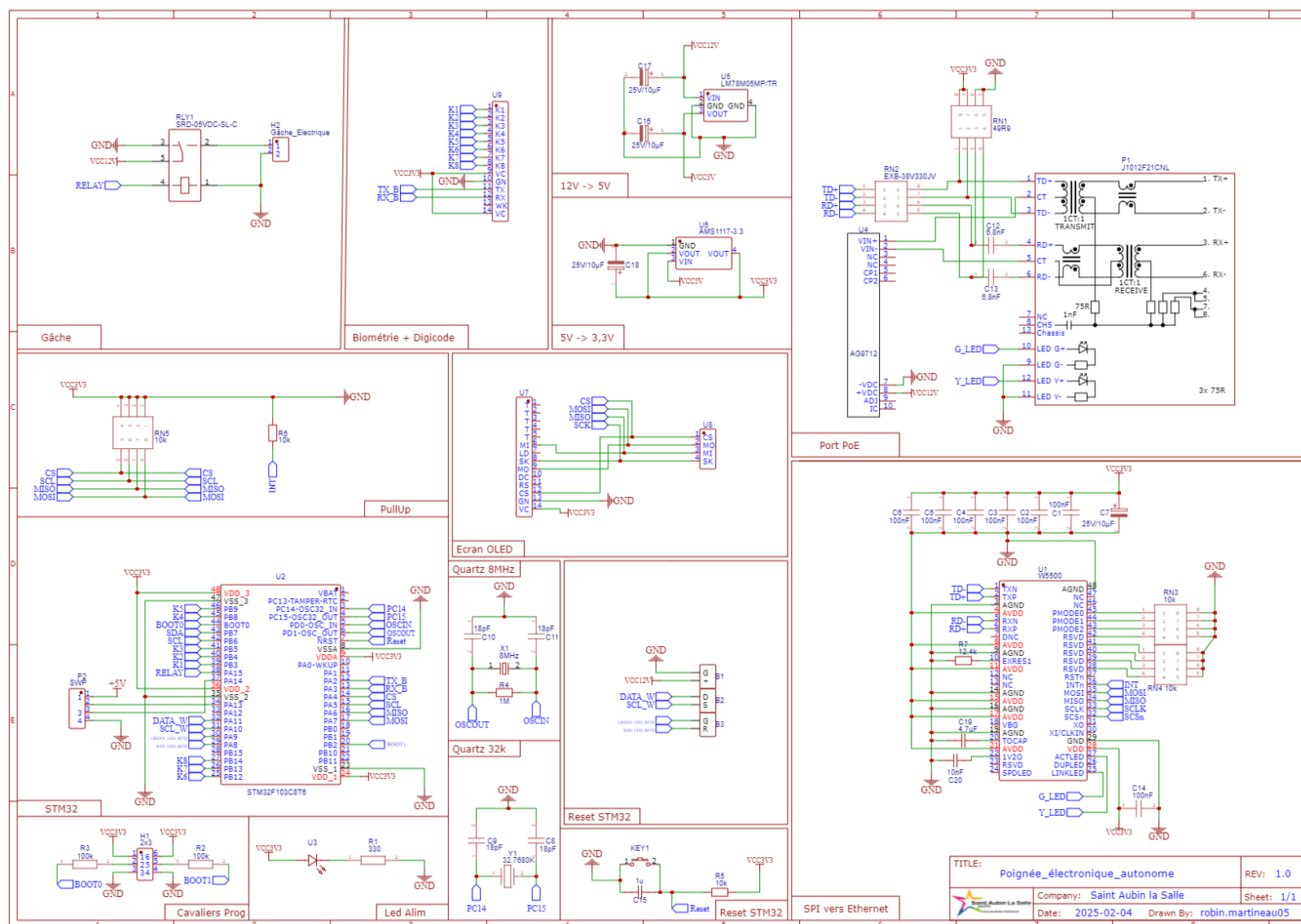
Ce diagramme permet de montrer les différentes composantes de notre système et leurs fonctions dans ce système. Au centre, nous pouvons voir toutes les fonctions que doit pouvoir exécuter la PEA. Toutes les fonctions sont ensuite rangées dans le composant qui aura permettra cette tâche. Ce diagramme est lié à un autre diagramme qui permet de voir les flux entre les composants, le diagramme de blocs internes.

Diagramme de blocs internes



Comme dit précédemment ce diagramme, nous permet de voir les différents flux entre les composants. Nous pouvons voir des bus comme un bus SPI ou encore un bus I²C. Ce diagramme, nous montre dans les grandes lignes ce qui va transiter et dans quel sens ces informations vont transiter.

Schéma structurel

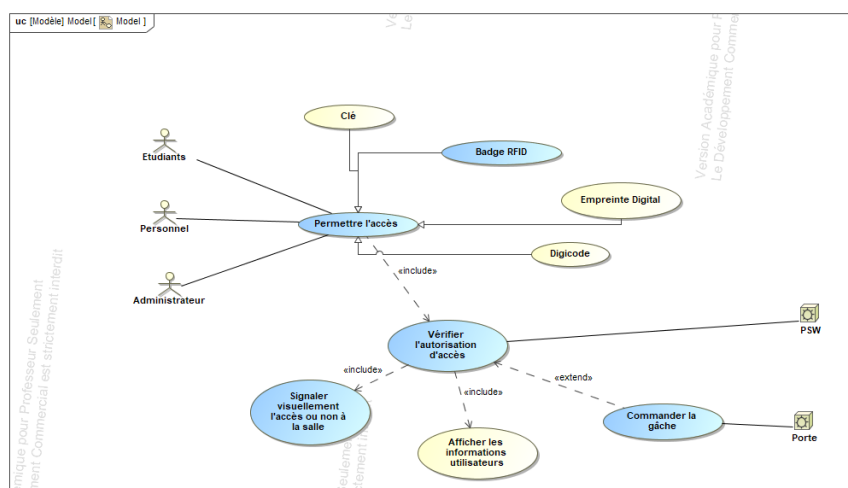


V – Les tests

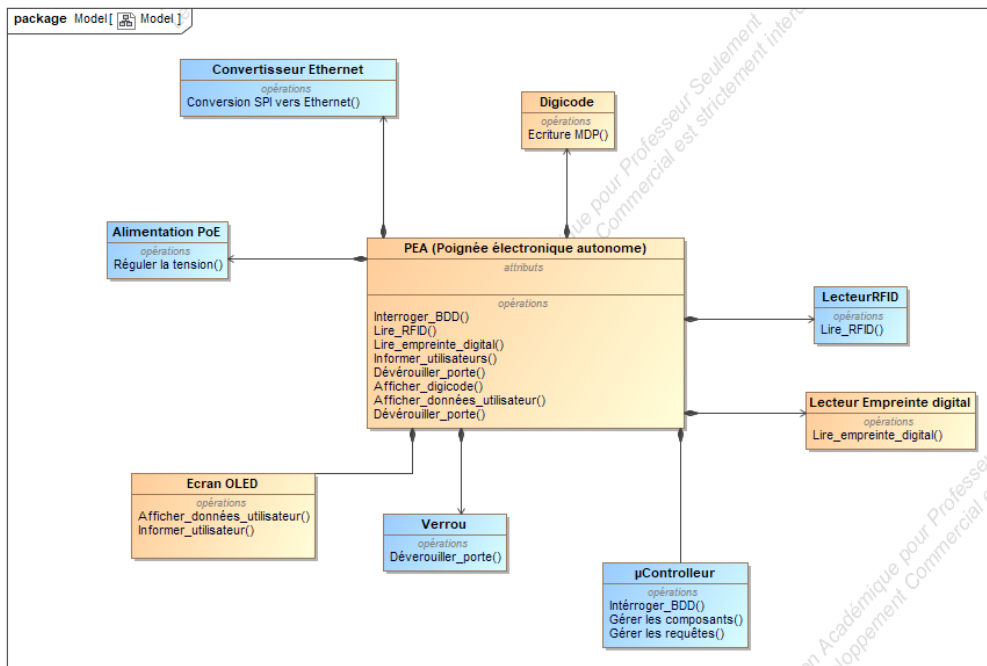
Comme dis précédemment pour construire le projet nous utilisons la méthode agile, aussi appelé méthode incrémentale. Avec cette méthode, des tests sont nécessaires à chaque incréments/étapes du projet. Les tests importants à effectuer seront les tests unitaires, de non-régression, et bien sûr de prendre en compte l'avis du client sur l'avancer des travaux et l'état du premier livrable. Vous trouverez ci-dessous le plan de test qui permettra de déterminer si le produit actuel répond aux demandes principales du client.

Identification du Plan de Tests	P1	Référence du module testé	PEA	
Objectif du test :	Tester le bon fonctionnement du jalon 1 de la PEA			
Type de test :	Tests unitaires et test d'intégration			
Environnement du test	Laboratoire			
Ressources matérielles :	Oscilloscope, multimètre	Ressources humaines	Manipulation d'outils de mesure et d'un serial monitor.	
Conditions du test				
Critères d'Entrée		Critères de Sortie		
L'utilisateur doit disposer d'un badge RFID valide et dont il connait l'UID.				
Procédures du test				
ID Test	Description du Test	Planification	Responsable	Commentaire
T1.1	Le test permet de vérifier que tout le programme s'effectue normalement.	jj / mm / aaaa	Robin MARTINEAU	
T1.2	Le test consiste à vérifier que la bon fonctionnement du Wiegand (lecture)	jj / mm / aaaa	Robin MARTINEAU	
T1.3	Le test consiste à vérifier que la bon fonctionnement du SPI (lecture et écriture sur le BUS)	jj / mm / aaaa	Robin MARTINEAU	
T2.1	Le test consiste à vérifier que la bon fonctionnement du lecteur RFID	jj / mm / aaaa	Robin MARTINEAU	
T3.1	Le test permet de vérifier que la communication Ethernet est valide.	jj / mm / aaaa	Robin MARTINEAU	
T4.1	Le test permet de vérifier que la gâche fonctionne correctement et qu'elle est bien contrôlier	jj / mm / aaaa	Robin MARTINEAU	
T5.1	Le test permet de vérifier que l'alimentation PoE est valide.	jj / mm / aaaa	Robin MARTINEAU	

Ce plan de test permet de tester le prototype montré au client. Celui-ci doit répondre au cas d'utilisation du premier livrable visible ci-dessous en bleu.



Le plan de test possède aussi des tests unitaires permettant de tester un composant du système en particulier. Pour visualiser les composants à tester vous trouverez ci-dessous le digramme de définition de blocs, avec les blocs concernés par les tests en bleu.



VI - Conclusion

Actuellement, nous sommes sur la période de tests afin de valider notre premier livrable. Nous enchaînerons par la suite sur l'implémentation de l'incrément du livrable 2, en lien avec l'affichage et le digicode.