Rapport de PSE – Partie Numérique

Livraison intermédiaire – Hardware.

Keylogger

1. Cahier des charges

Un Keylogger est un dispositif de piratage permettant de capturer et récupérer toutes les actions effectuées sur un clavier.

Il existe plusieurs types de keylogger :

- Les Keyloggers software qui sont des malwares qui s'exécutent en arrière-plan sur le PC de la cible.
- Les Keylogger hardware qui eux sont sous forme de clé USB avec une entrée femelle et une sortie male (l'entrée sera relié au Clavier et la sortie au PC).

Aujourd'hui, la majorité des claviers sont en USB, cependant il existe encore des claviers en PS/2. Nous allons réaliser notre keylogger de manière à pirater un clavier PS/2 car les contraintes techniques lié à la vitesse de la communication ainsi que le protocole qui est utilisé sont moindre. Si le temps nous le permet, le passage à un keylogger USB pourra être envisagé.

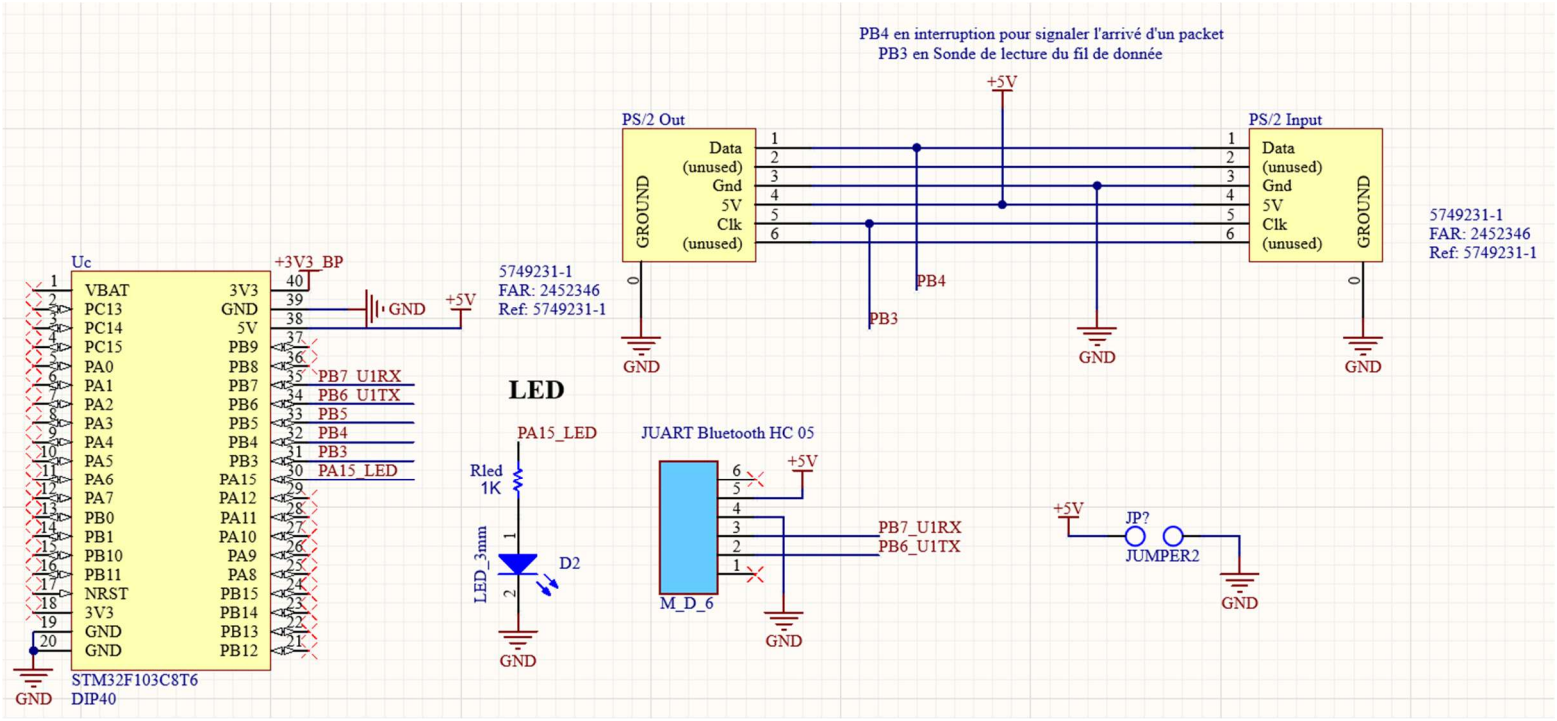
Aussi, l'intérêt d'un keylogger étant de récupérer les données, nous ajouterons un module Bluetooth HC_05 afin d'envoyer les données vers une application Android.

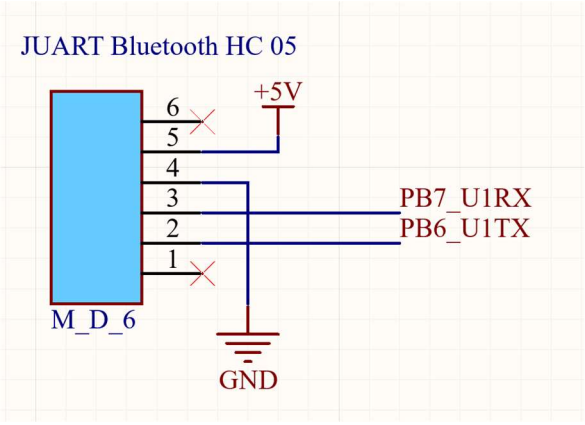
Pour réaliser notre projet, il nous faut donc :

- 2 prises PS/2
- 1 module HC_05
- 1 led + resistance pour debug/état d'utilisation
- Une alimentation 5V de debug (la carte est sensée s'alimenter directement avec l'alimentation du câble PS/2 par la suite)

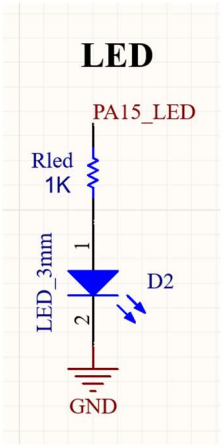
2. Schéma électrique

Voici le schéma électrique global du projet :



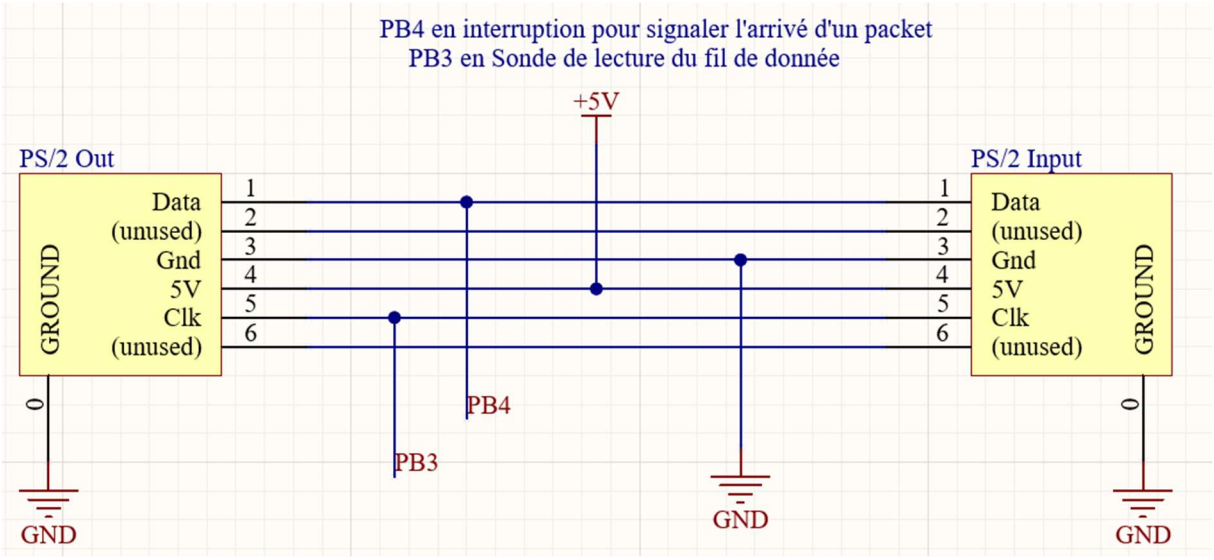


Voici le connecteur qui permet la liaison avec le module HC_05. On y retrouve les pins GND/5V et RX/TX.



Ici, nous retrouvons la Led de debug qui à terme servira de Led d'état.

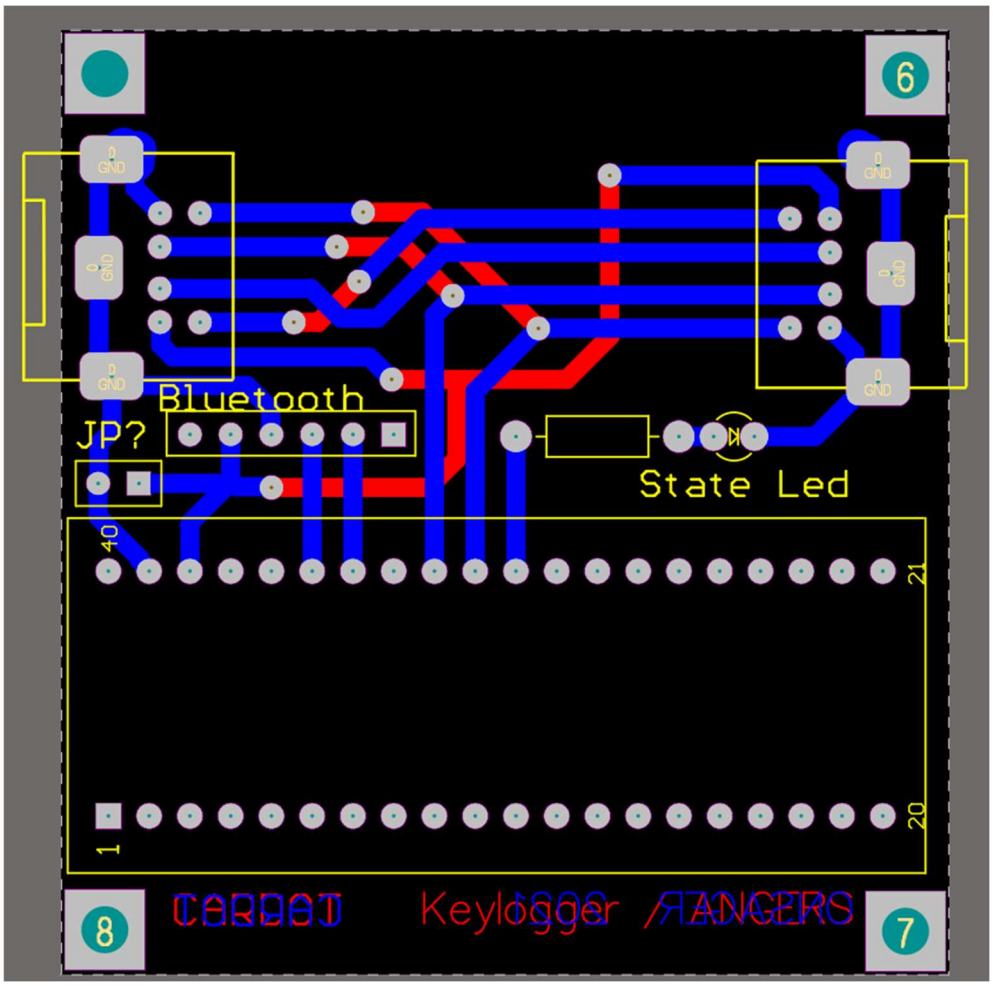
Et enfin, les connecteurs PS/2 nous permettent de récupérer le signal passant dans le câble du clavier, mais aussi d'utiliser son alimentation pour obtenir un keylogger autonome en énergie.



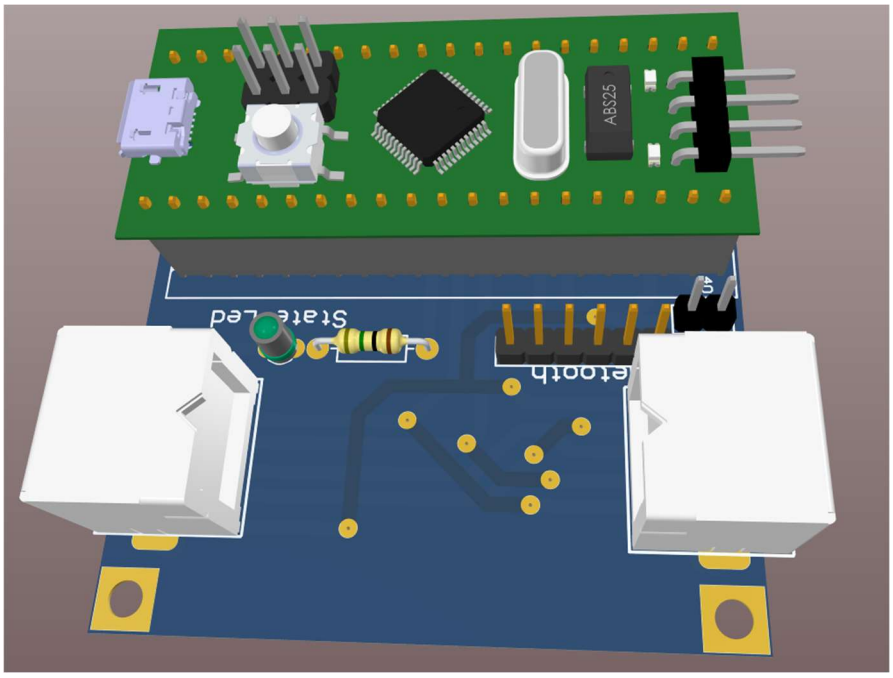
Nom ou Référence du composant	**Description/rôle dans l'application/Caractéristiques principales dans le projet.**
Blue Pill	La bluepill est le composant le plus essentiel du projet, c'est elle qui va écouter et décoder le signal PS/2 pour ensuite l'envoyer au module bluetooth.
Module HC_05	Le HC_05 va permettre d'envoyer les informations vers une application Android
PS/2 Input	Connecteur relié au Clavier
PS/2 Output	Connecteur relié au PC
LED	Led servant à débug et de led d'état
JUMPER	Pin permettant l'utilisation d'une alimentation externe 5V.

3. Routage

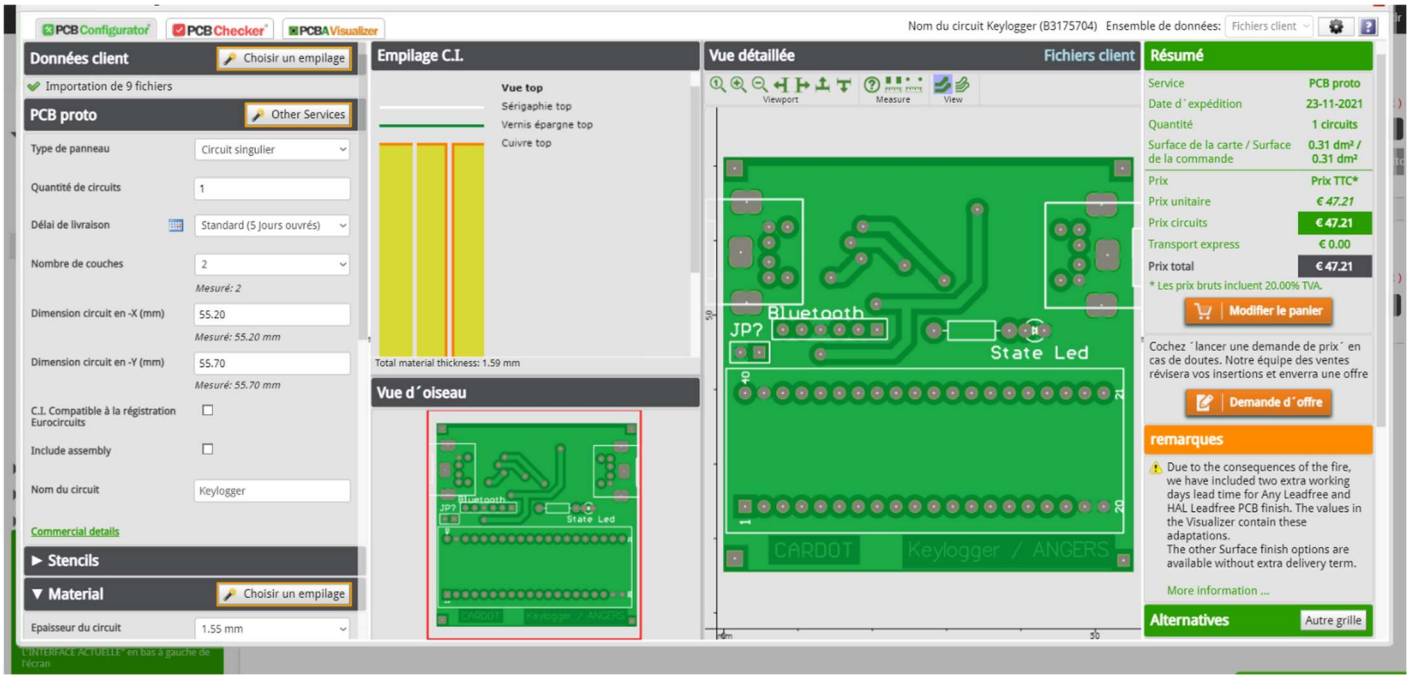
Voici une vue 2D du routage réalisé sur Altium :



Voici une vue 3D :



4. Validation du PCB



5. Cahier de suivi

Date	Tâches, difficultés rencontrées	A faire la prochaine fois
9/11	Réalisation du Schéma Electrique / Routage	Vérifier cahier des charges PCB
16/11	Finalisation de la conception du PCB, Dernières vérifications avant dépôt Dépôt du PCB	Application Andoid
18/11	Création de l'appli Android APP Inventor	Perçage + soudure PCB
25/11	ABSENT	ABSENT
02/12	Réception du PCB, perçage, soudure, vérification de continuité de courant	Préparation Software
10/12	Recherche liée à la solution Software à apporter	

6. Etat d’avancement et analyse du projet réalisé

[16/11] : Clément CARDOT

La conception du PCB s’est bien déroulée, pas de problème spécifique à remonter pour le moment.

Vérification du PCB via la batterie de tests et de vérification fournie.

Dépôt du PCB pour réalisation

Dans le cas où le projet fonctionne bien et que la date finale n’est pas atteinte, il aurait pu être intéressant d’avoir des connecteurs USB de l’autre coté du PC pour tester avec des claviers plus récents.

La conception du software n’est pas commencée mais une modélisation UML sera réalisé sur les prochaines séances afin de clarifier le fonctionnement du système.

[18/11] : Clément CARDOT

Création d’une application Android grâce à MIT APP INVENTOR, l’application est pour l’instant composé d’une page d’appairage Bluetooth, une page de paramètre et une page de réception de donnée.

[25/11] : Clément CARDOT

ABSENT car présent au Rencontres des Technologies de l’ESEO.

[02/12] : Clément CARDOT

Réception du PCB réalisé, Perçage des trous via les tourets du labo. Soudure des composants déjà reçu. Validation de l’alimentation par M. POIRAUD et attribution de la Bluepill.

Composants reçu et placé à ce jour :

-BluePill

-Led + Résistance

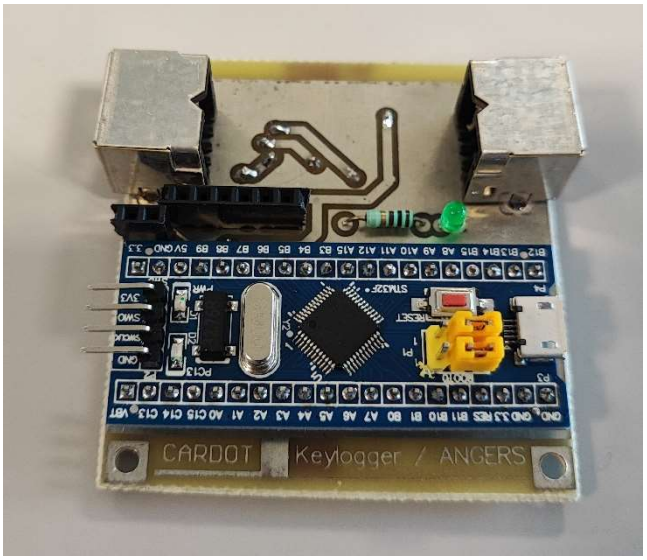
-Barrette 2 pins + 6 pins

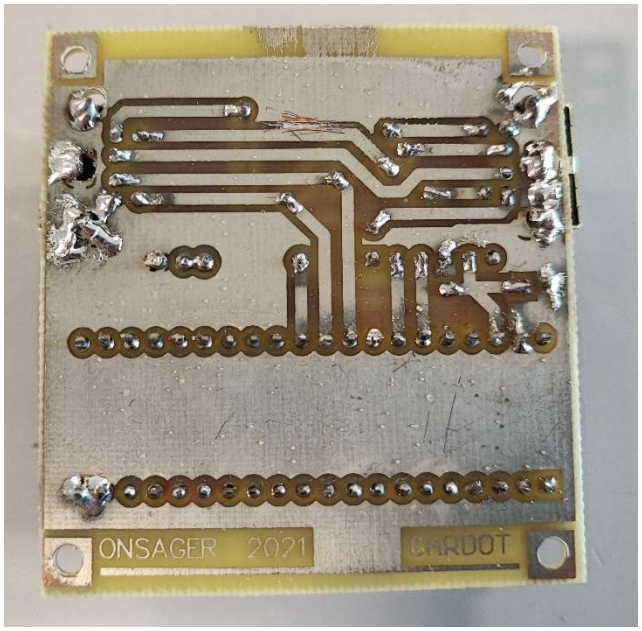
[10/12] : Clément CARDOT

Réception du module Bluetooth HC05. Il ne reste plus que les deux prises PS/2 qui sont toujours en transit

[EDIT] : Prise PS/2 Reçu et soudées

Ci-dessous on peut retrouver une photo du PCB final (côté composant et côté soudure) :

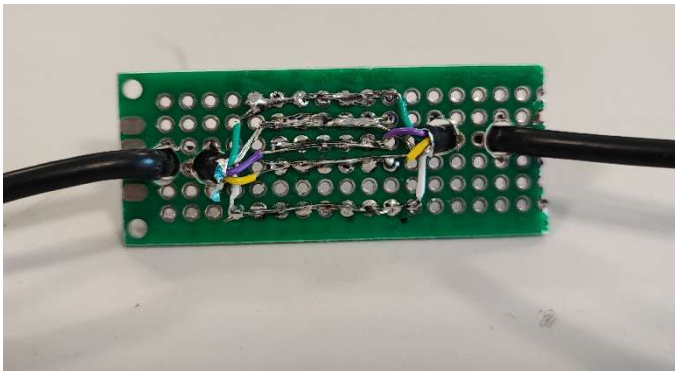




J’ai aussi remarqué qu’il allait me manquer un câble PS/2 M/M.

Je suis donc allé chercher 2 câbles PS/2 de clavier et je les ai reliés entre eux afin d’obtenir un câble M/M

Voici quelques photos du résultat :



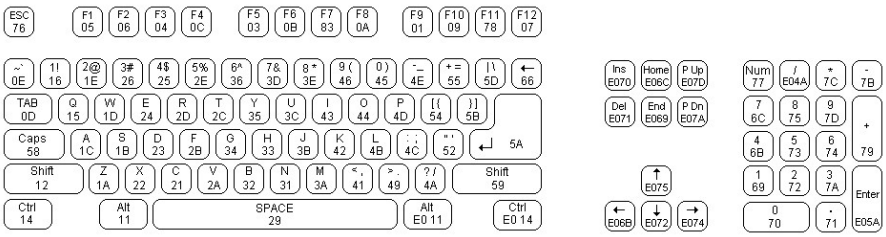
7. Software

- Application APP Inventor :
    - Page d'appairage
    - Page de paramètre
    - Page de lecture des données reçu

L'application comprend aussi une base de données interne permettant la sauvegarde des données reçu lors de la fermeture de l'application.

Afin de réaliser les tests plus sereinement, j'utiliserais une application terminal Bluetooth du Play Store pour réaliser les premiers tests.

- Software Bluepill
    - Utilisation du protocole PS/2 : http://www.lucadavidian.com/2017/11/15/interfacing-ps2-keyboard-to-a-microcontroller/



    - Utilisation du module bluetooth : https://www.electronicshub.org/interfacing-hc-05-bluetooth-with-stm32f103c8t6/

      Pour le Bluetooth, il faudra utiliser la bibliothèque uart.c qui nous permettra d'utiliser correctement