

# Rapport et suivi journalier - Avancées du projet Cyber EM

## Jours 1 :

- Visite des locaux de l'IETR, premier contact avec les chercheurs et doctorant
- Assistance à une soutenance de thèse
- Commencement du projet
- Premier pas avec l'USRP sur mon ordinateur personnelle
- Premier bloc gnu radio

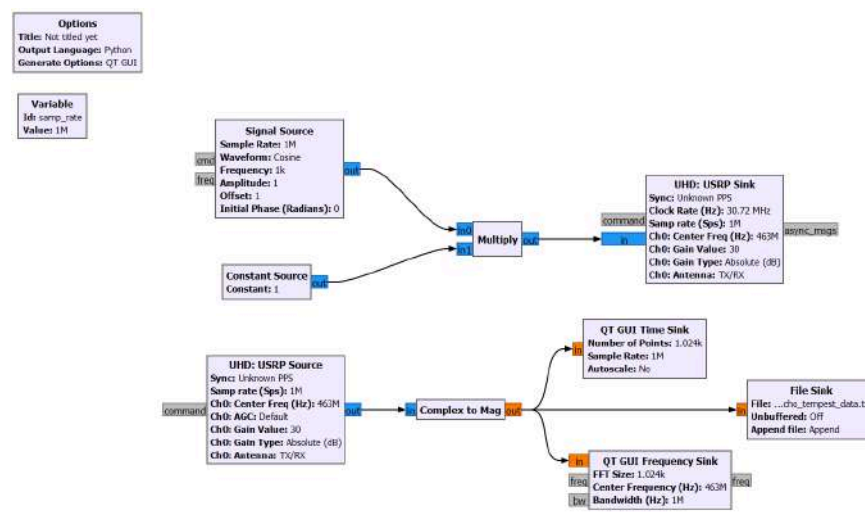


Diagramme Gnu radio - Emission et réception d'une onde modulé avec l'USRP

## Jours 2 :

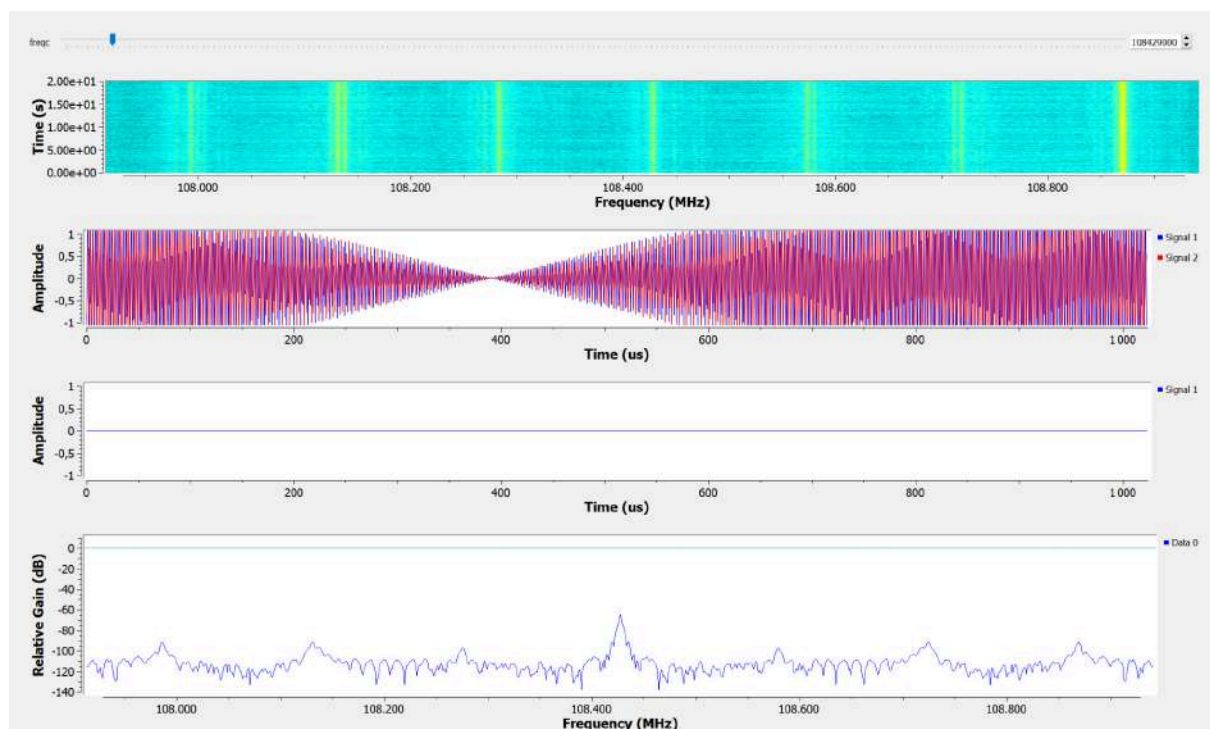
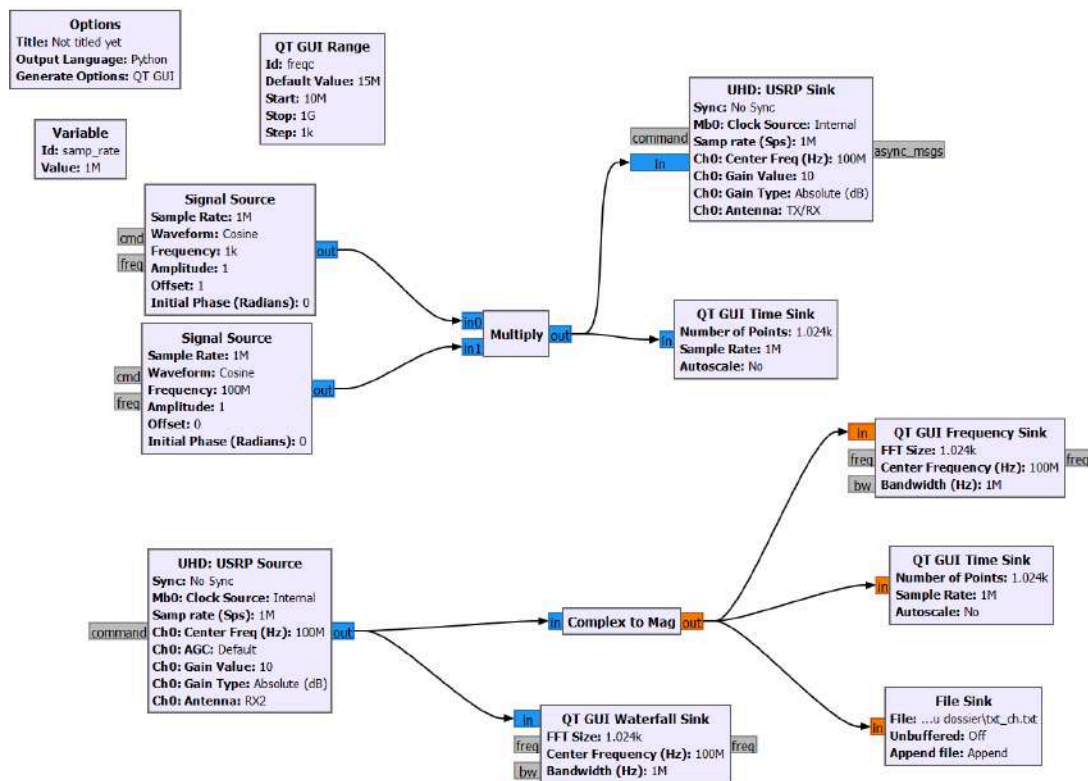
- Connexion entre deux carte STM32 grâce à mbed studio (envoi de 1 et 0)
- Réglage du problème d'horloge sous GNU Radio pour USRP source et USRP Sink
- Modification et gestion du fichier .py de mon programme GNU Radio
- Probleme de connexion au réseau de la fac (hack)

## Jours 3 :

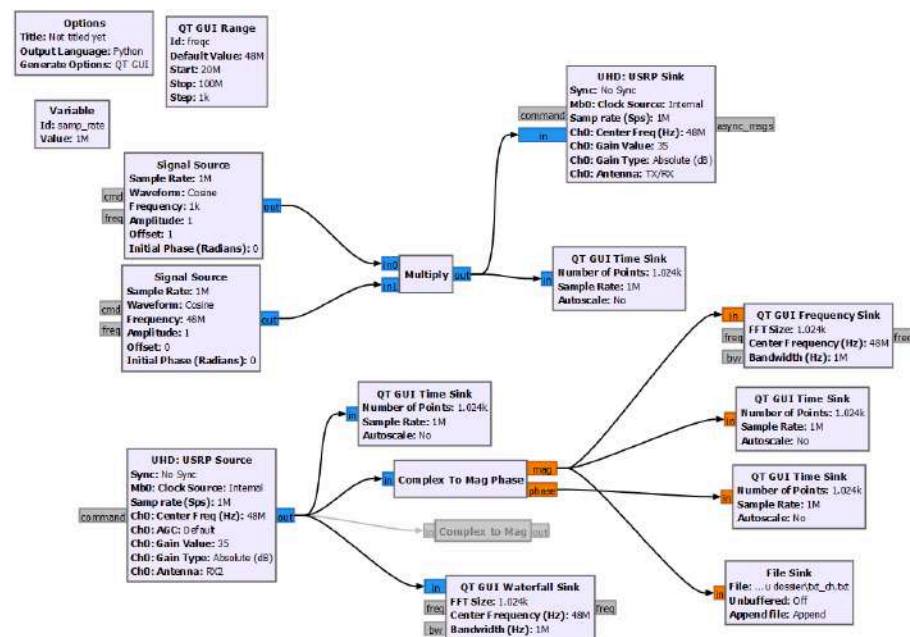
- Problème d'USRP réglé !!
- Problème de connexion réglés
- Début de programme pour balayer en fréquence

## Jours 4 :

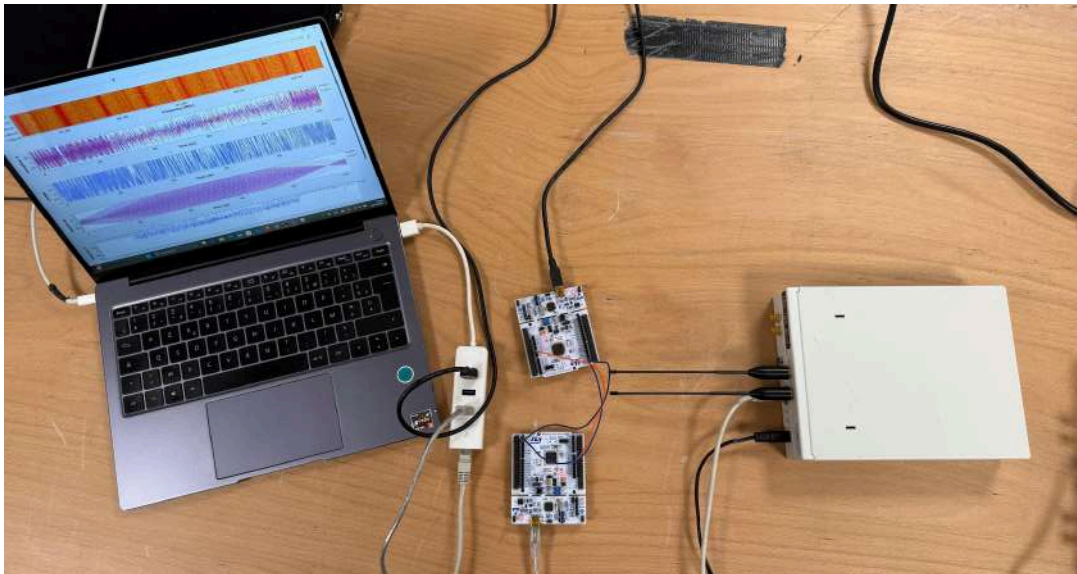
- mise en place d'une attaque émission réception sous gnu radio
- compréhension des notions de modulation sous gnu radio



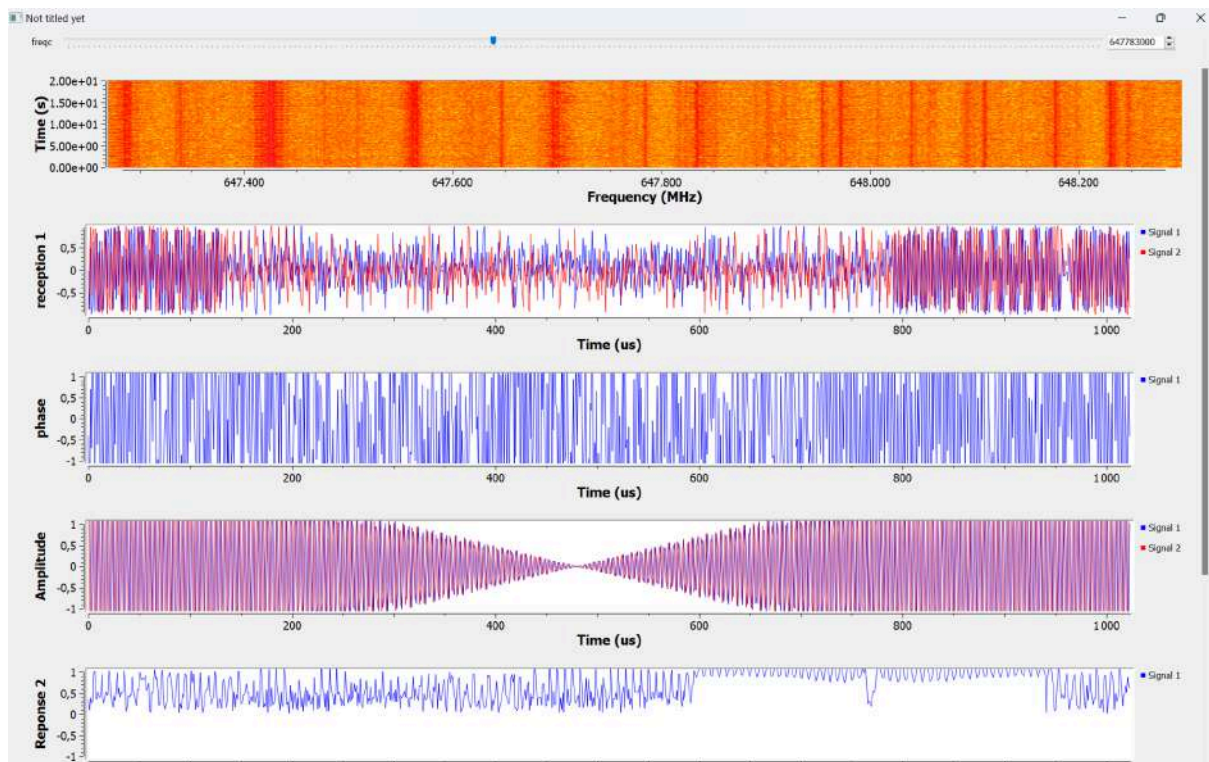
Communication entre les 2 STM32 :



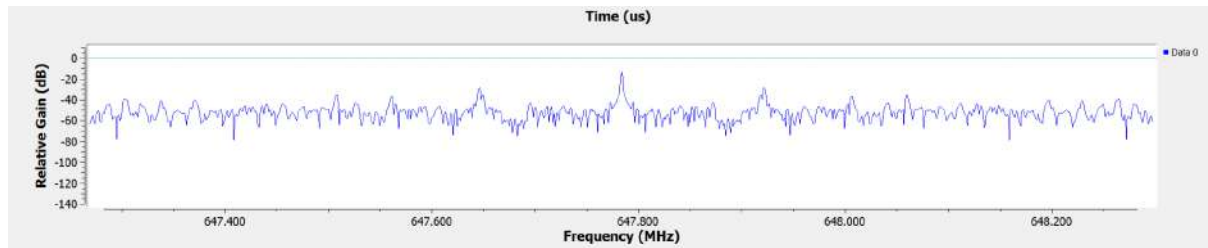
## Setup expérimental USRP NI-2922



## Interface



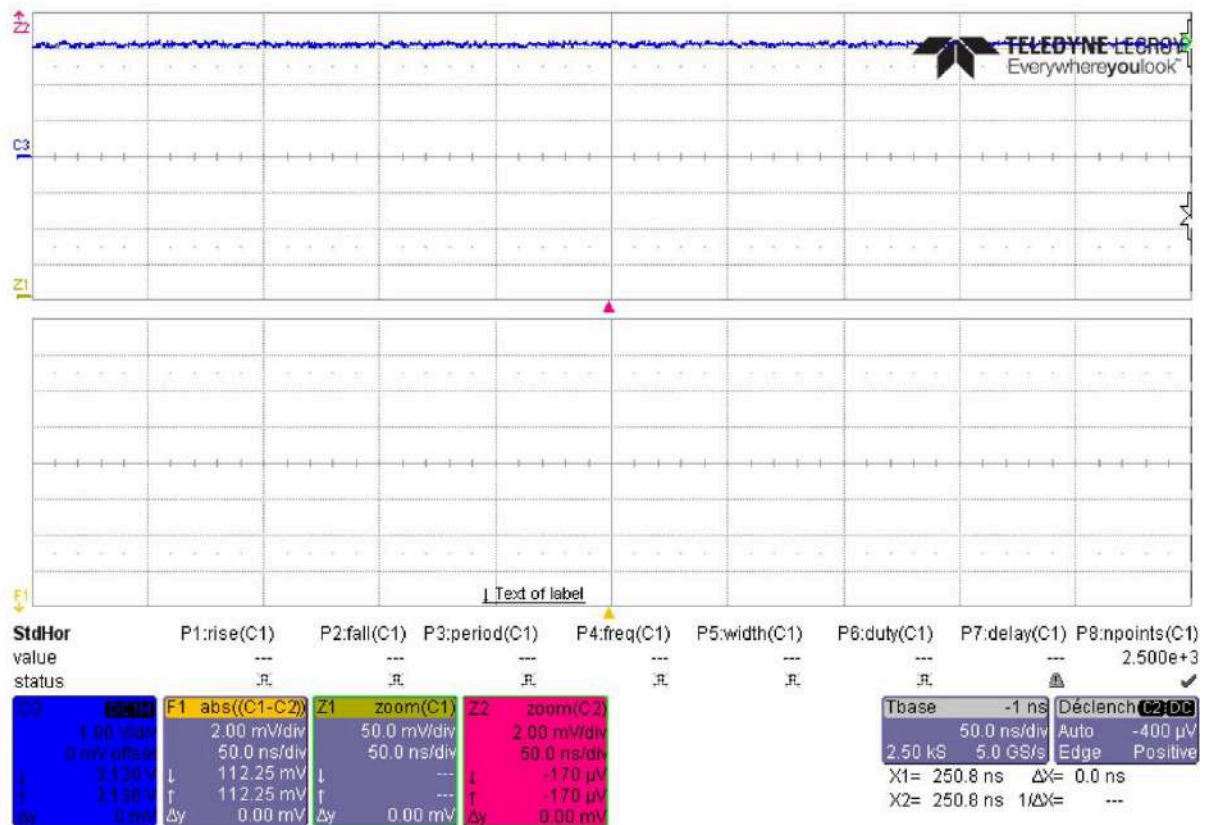




## Mesure des signaux envoyé et reçu sur par et sur les STM32 via l'oscilloscope

Objectif : s'assurer de l'envoi et de la bonne réception des données via UART, et mise en évidence de la consommation des modules.

1. Envoie des données 1 et 0 depuis un STM vers l'autre
2. Je m'aperçois que je ne mesure rien à l'oscilloscope
3. Localisation du problème :
  - J'envoie un programme de mon pc sur un stm pour faire clignoter les LED, la led clignote : communication pc vers stm fonctionnelle
  - Je mesure à l'oscilloscope un courant continu de 3V pour voir si le problème ne vient de pas de l'oscilloscope : l'oscilloscope est fonctionnelle
  - Je réalise un programme permettant d'envoyer des 0 et des 1 à un stm32, une fois reçu et fonction de la valeur reçu il éteint et allume sa led : le deuxième stm32 ne reçoit pas les 1 et 0 et sa led ne s'allume pas



Mesure de la tension à l'oscilloscope à la sortie de générateur DC (3V injecté)

## Communication maître-esclave (SPI) pour localiser le STM32 défectueux :

```

Envoyé : A, Reçu :
Envoyé : A, Reçu : A
Envoyé : A, Reçu : ?
Envoyé : A, Reçu : ?
Envoyé : A, Reçu : ?
Envoyé : A, Reçu :
Envoyé : A, Reçu :
Envoyé : A, Reçu :
Envoyé : A, Reçu :
Envoyé : A, Reçu :
Envoyé : A, Reçu : ?
Envoyé : A, Reçu : ?
Envoyé : A, Reçu : ?
Envoyé : A, Reçu : ?
Envoyé : A, Reçu :

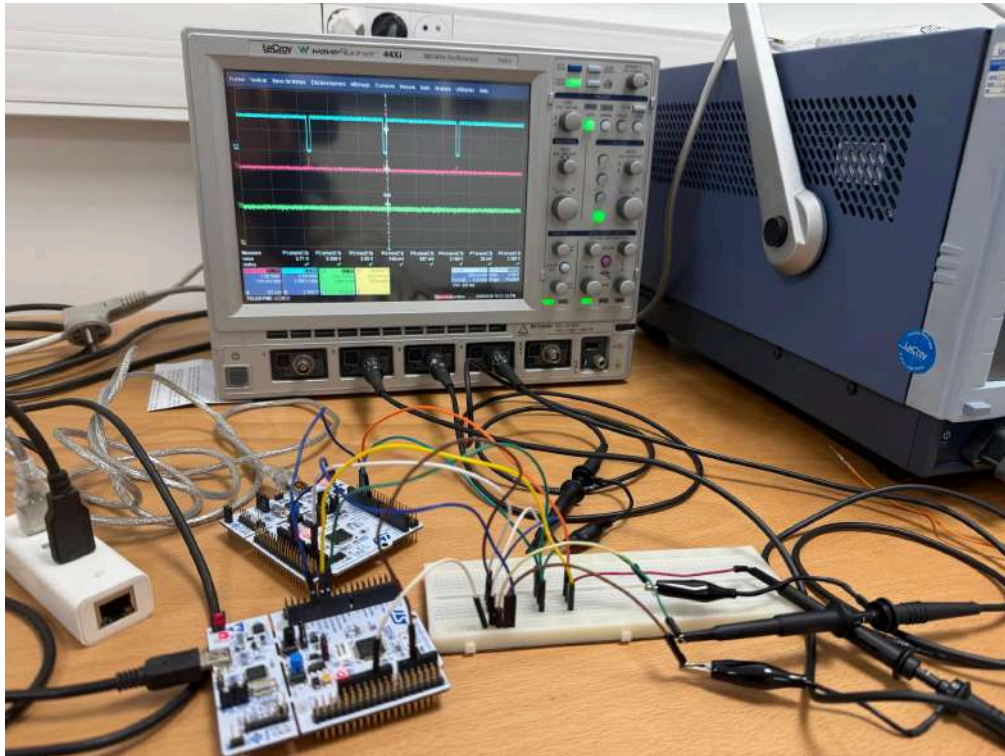
```



STM fonctionnelle

STM défectueux

## Test avec un nouveau STM32 (F446) :

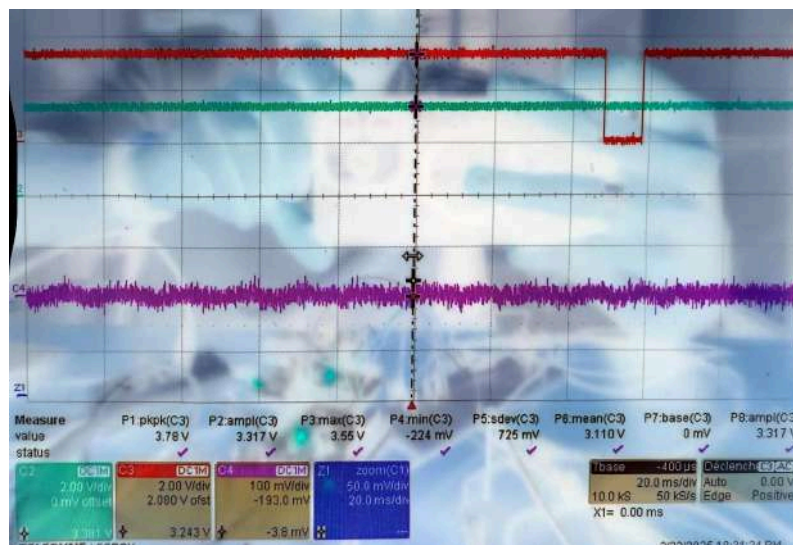


*Nouveau setup expérimental*

### Problèmes rencontrés :

Maître et esclave branché en même temps :

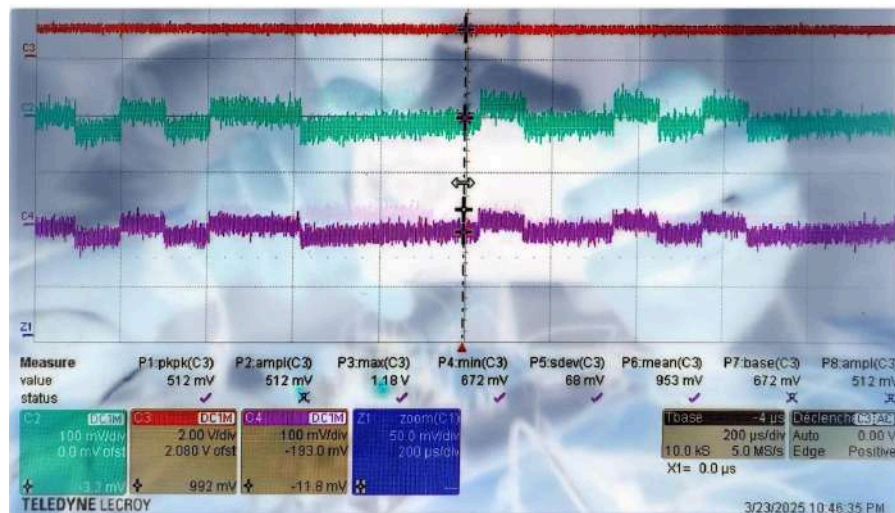
- signal SS (select slave fonctionnel et observable), envoie caractérisé par une impulsion au moment du SS observable
- Rien n'est renvoyé par l'esclave



*Maître et esclave branché en même temps*

Esclave branché seulement :

- retour de données sur les broches MOSI et MISO similaire (surement le retour de l'information à envoyer si le maître envoie quelque chose)



*Esclave seul*

Idée : Attaquer le SS :

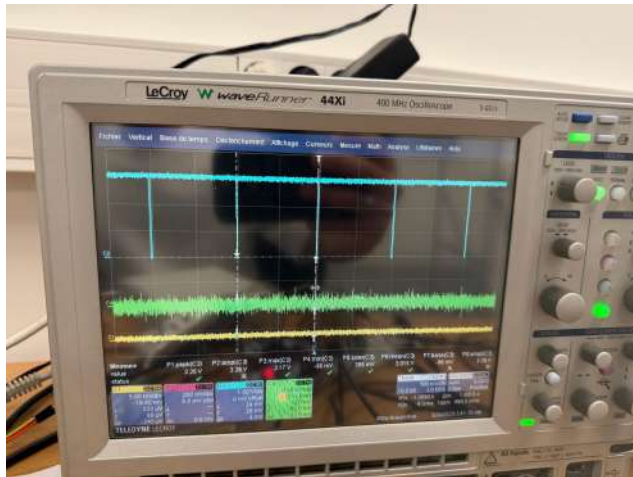
- Rôle critique : La broche SS (active LOW) contrôle l'activation d'un esclave SPI. Son état (HIGH/LOW) est directement lié à l'activité du bus.
- Variation d'impédance : Comme tout signal numérique, la broche SS est connectée à un buffer de sortie chez le maître. Une transition HIGH → LOW modifie l'impédance du circuit, ce qui peut générer un Echo TEMPEST détectable.

Idée : détecter la perturbation de mon fil via l'oscilloscope pendant l'envoi de la porteuse

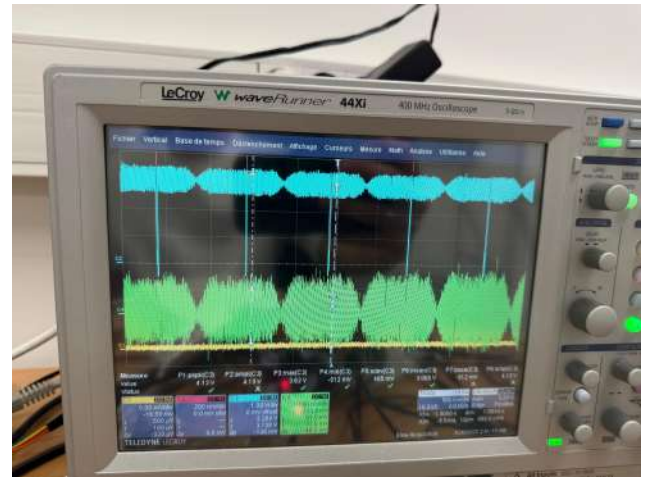
### TEST avec 1 Hz en fréquence du modulant (fréquence ss) :

- Perturbation des fronts d'onde du ss sur l'oscilloscope à la fréquence de 400 Hz (optimal de l'antenne tribande) pour la porteuse et 1 Hz pour le modulant (le fil joue surement le rôle d'antenne involontaire)

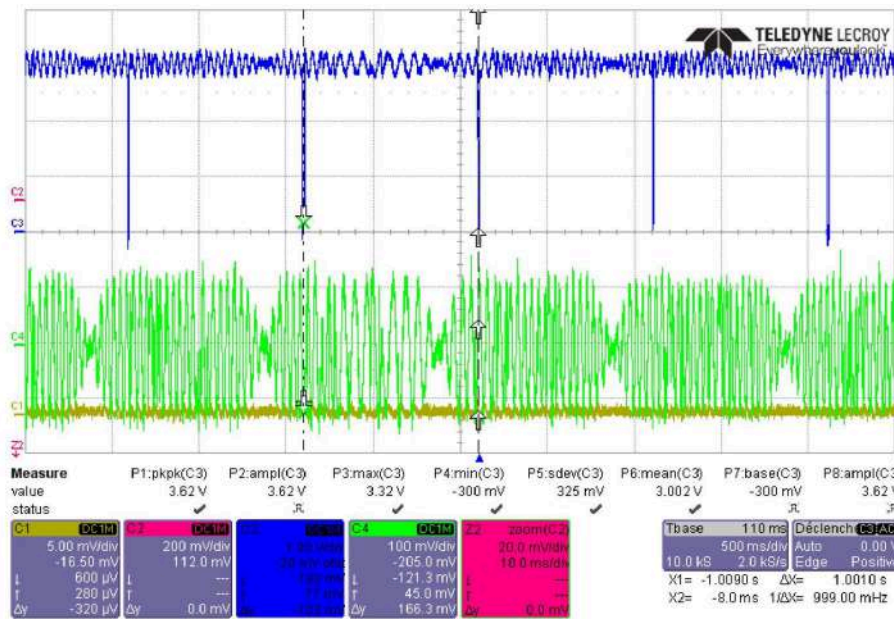




fréquence arbitraire



fréquence de 400 MHz porteuse et 1 Hz modulant



Conflit à régler sur l'envoi et la réception

```

Envoyé : A, Reçu : A
Envoyé : A, Reçu : A
Envoyé : A, Reçu :
Envoyé : A, Reçu :
Envoyé : A, Reçu :

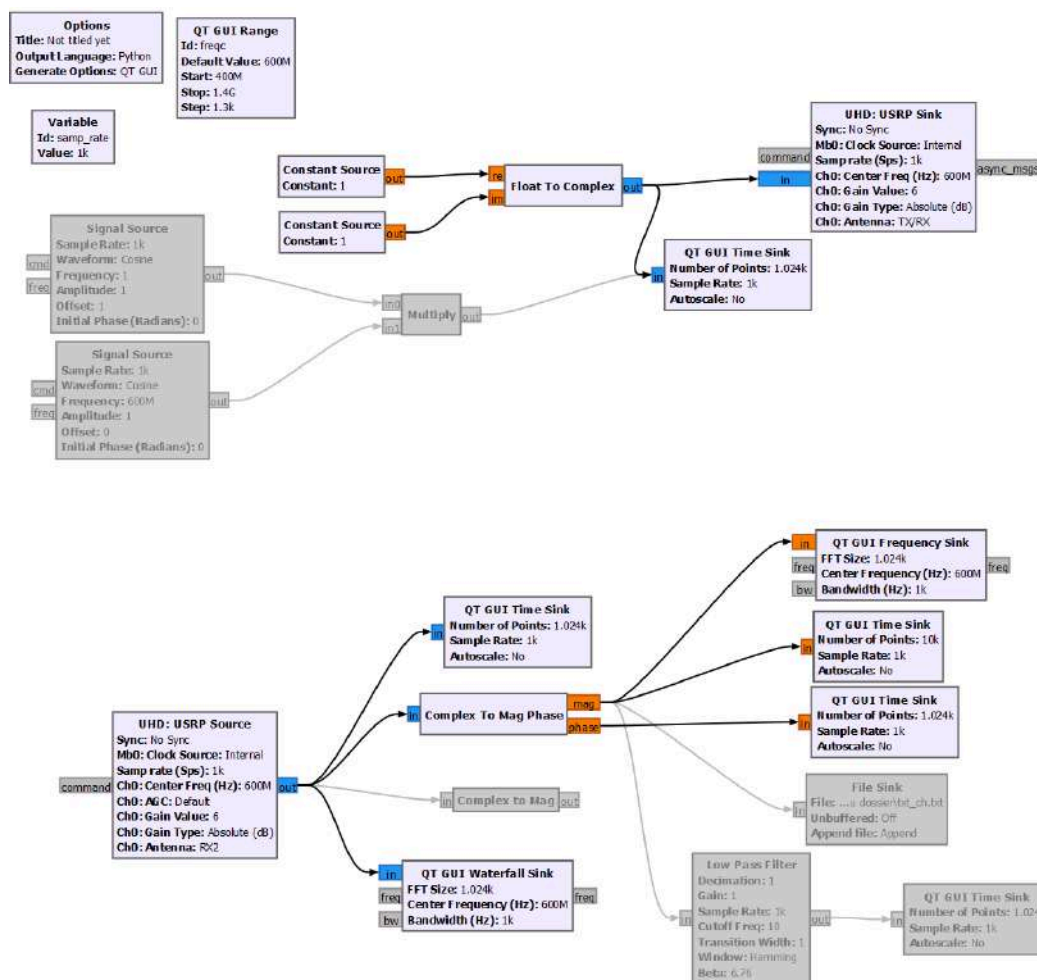
```

```

Reçu : B
Reçu : B
Reçu : B
Reçu : B

```

### Nouveau diagramme GNU Radio :

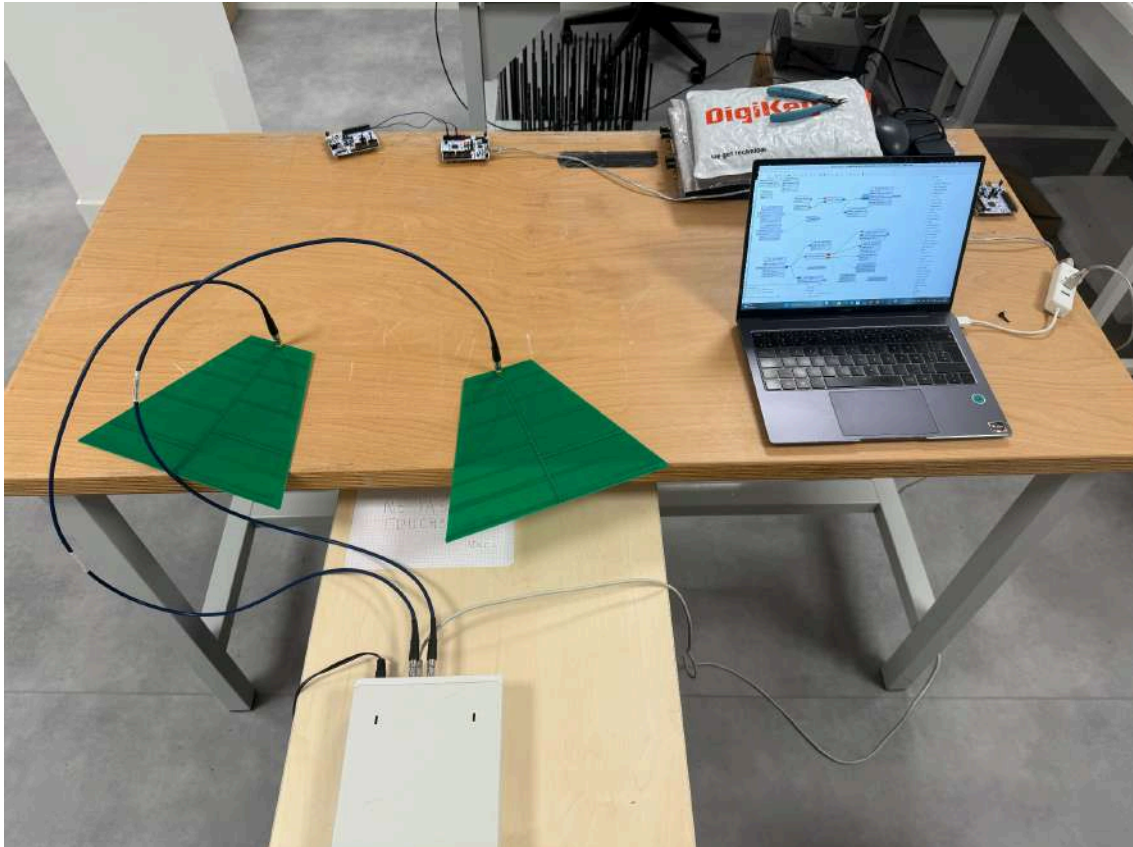


Nouveau programme en désactivant les signaux source car il s'ajoute au mélangeur de l'usrp et donc je me retrouve à additionner des fréquence, à la place et pour envoyer une porteuse pur, je ne modifier que la fréquence dans UHD USRP sink et ajoute des constant source (i et q) afin d'envoyer juste 1.

## Utilisation d'antennes log périodique :

Avantages :

- Plus directifs
- Meilleur gamme de fréquence
- Evite le couplage intra antennes



*Dispositif expérimental de l'attaque*

### Pré tests avant l'attaque echo tempest :

#### **Test recuperation “Écho” avec un fil :**

Dans ce premier test nous avons décidé (frank COLIN et moi) de tester la réflexion d'un fil non alimenté afin de pouvoir récupérer un premier écho et d'évaluer le couplage entre deux antennes log périodique :

Matériel utilisé :

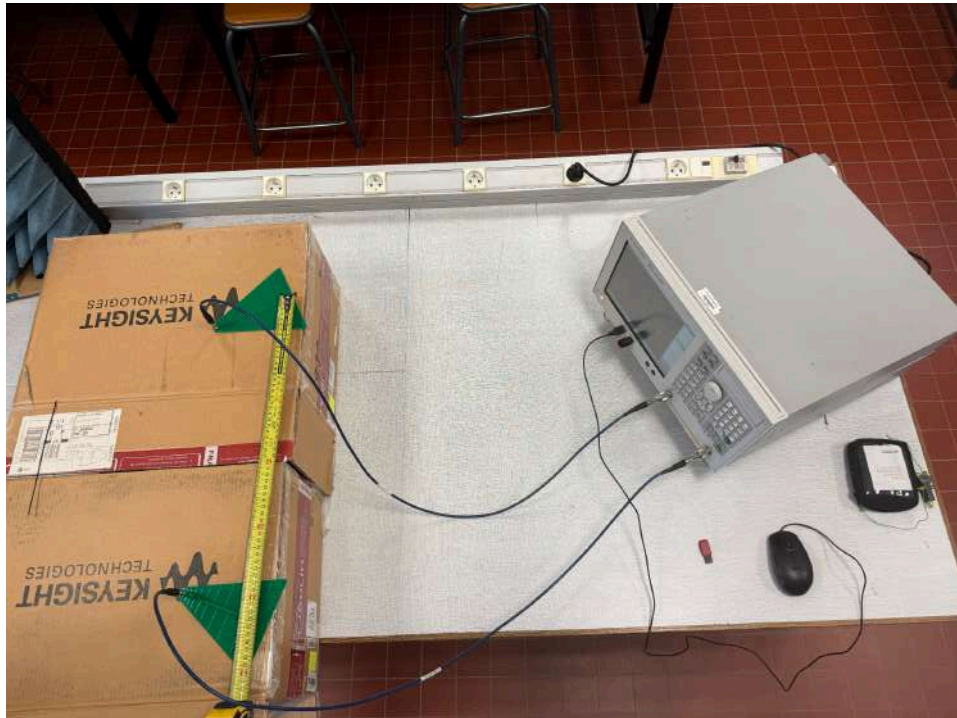
- Fil de longueur  $\Lambda/2$
- Antennes Log périodique
- VNA

BOUAMAMA. O

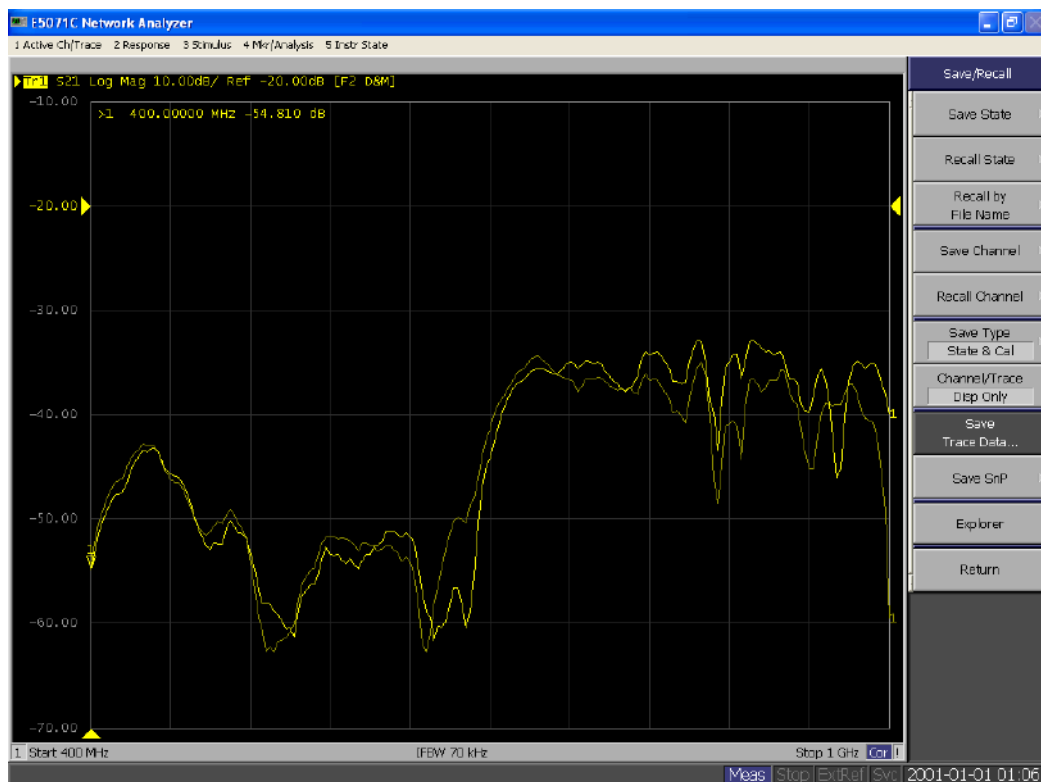
Etape préliminaire : calibration du VNA

2nd étape : mise en place du dispositif

3ème étape : Mesure du S21 (echo réflexion)

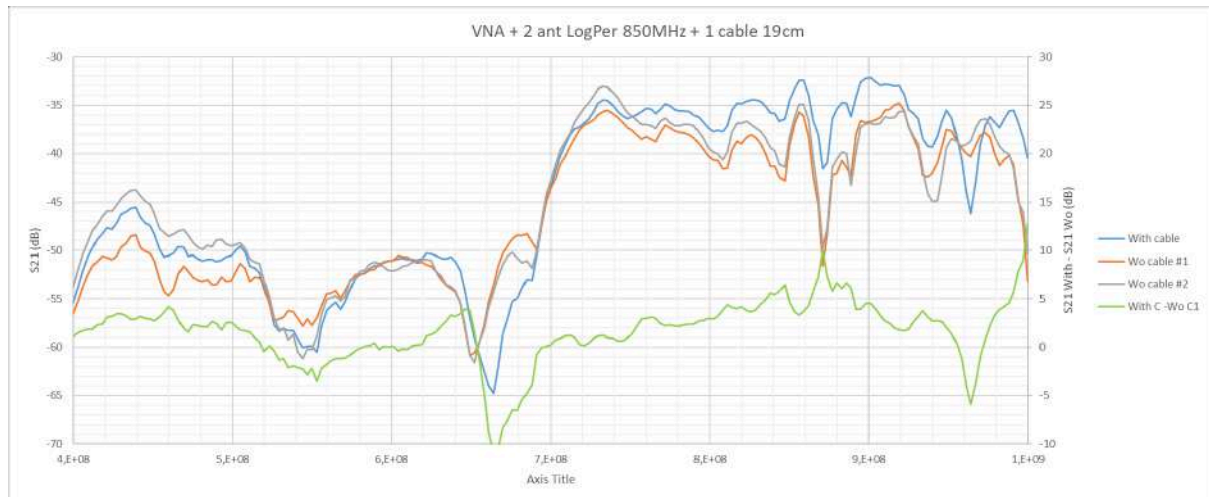


*Dispositif expérimental*



*Mesure du S21*





*Traitement des données sur excel*

### Légende

- courbe bleu : avec le câble
- courbe orange : sans le câble ref 1
- courbe grise : sans le câble ref 2
- courbe verte : différence entre la courbe avec le fil et celle sans le fil (5 dB diff max)

### Test variation d'impédance

Avant de réaliser les tests avec les log périodique, je décide d'entamer une série de tests préliminaires me permettant de localiser au mieux la fréquence à laquelle je pourrai réaliser l'attaque. En effet, et conformément à l'article d'Hayashi "echo tempest", des test sur la variation d'impédance en fonction de la fréquence en filaire sera réalisé.

Matériel à utiliser :

- VNA ou analyseur de spectre (+ coupleur directionnel)
- DUT (STM32)

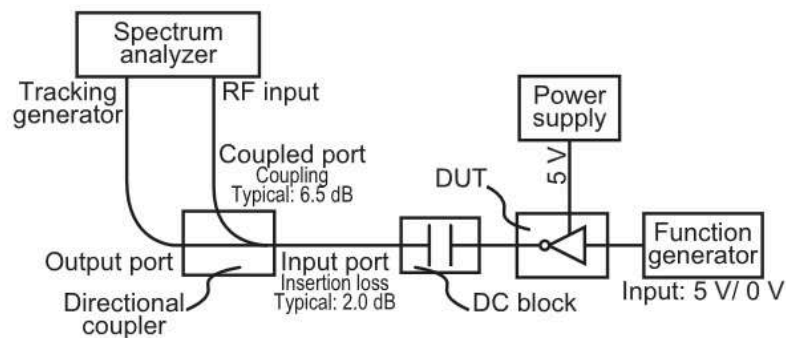


Fig. 5. Input impedance measurement setup based on the value of the inverter element's output signals.

*Dispositif expérimental de référence réalisé par Hayashi et son équipe*

BUT de la manipulation :

Pour et conformément au papier d'Hayashi je décide d'attaquer et de récupérer un signal simple, pour ce faire je décide d'établir une communication SPI (maître/esclave) entre deux STM32, le test d'impédance ne se fera que sur un seul des deux, en l'occurrence la maître qui envoie des signaux à esclave, afin de l'activer et lui transmettre des données, c'est ce qu'on appelle dans la communication SPI le SS (Select Slave ou encore CS Chip Select). Cette communication semble particulièrement intéressante car elle permet d'obtenir un signal carré, simple, en tout ou rien avec un Etat LOW à 0V (ground) et un état HIGH à 3,3 V, on se rapproche de la configuration qu'avait M. Hayashi pour ces tests d'impédances. Le tout serait alors, et sur le même graphique, de tracer l'état HIGH et LOW en impédance en fonction de la fréquence et de localiser à quelle fréquence il y a la plus grande différence, et donc la où il faudra focaliser la fréquence d'attaque pour l'Echo Tempest.

Allongement du SS :

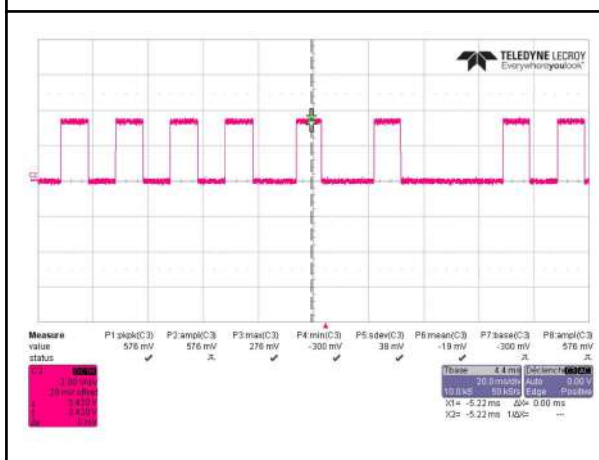
Pour ce faire, et dans un premier temps je dois augmenter la durée de mon signal Select Slave pour l'état LOW (activation de l'esclave) et l'état HIGH (désactivation de l'esclave) à quelque seconde environs plutôt que de l'ordre du ms, afin de pouvoir bien observer la différence d'impédance par la suite sur le VNA :

```
void loop() {
  digitalWrite(SS_PIN, LOW); // Activation de l'esclave (etat low)
  delay(5000); // Temps du ss (5s car en ms)
```

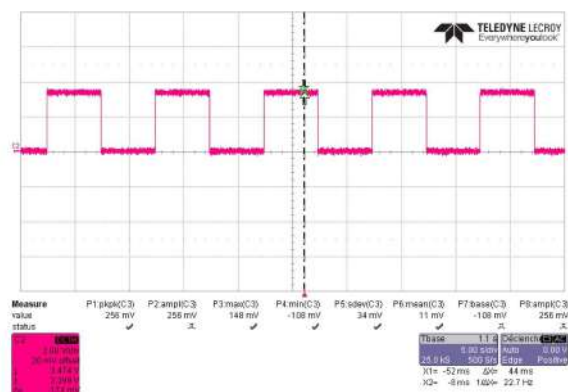
```
  digitalWrite(SS_PIN, HIGH); // Désactivation de l'esclave (etat high)
  delay(5000); // Pause 5 seconde avant l'envoi suivant
```

*Allongement du SS avec la fonction delay (en ms)*

Avant modification du SS (temps trop court ms)



Après modification du SS (ordre de la sec)

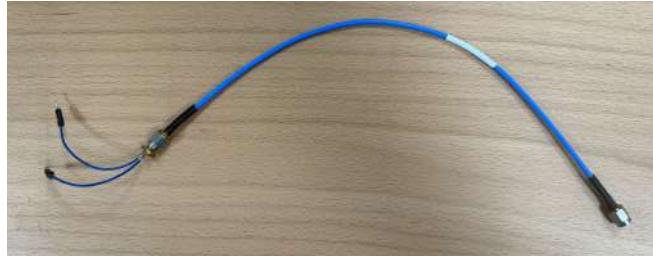


BOUAMAMA. O

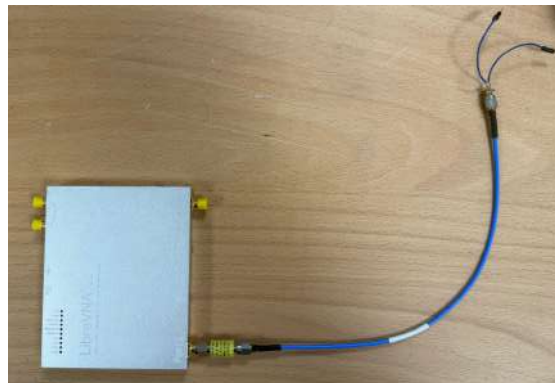
Avec ce signal carré je peux maintenant travailler sur un temps d'acquisition bien plus abordable à l'aide du VNA.

Montage du dispositif avec VNA :

- Cable SCM soudé sur GPIO :



Ajout d'un coupleur DC empêchant la tension de remonter jusqu'au VNA



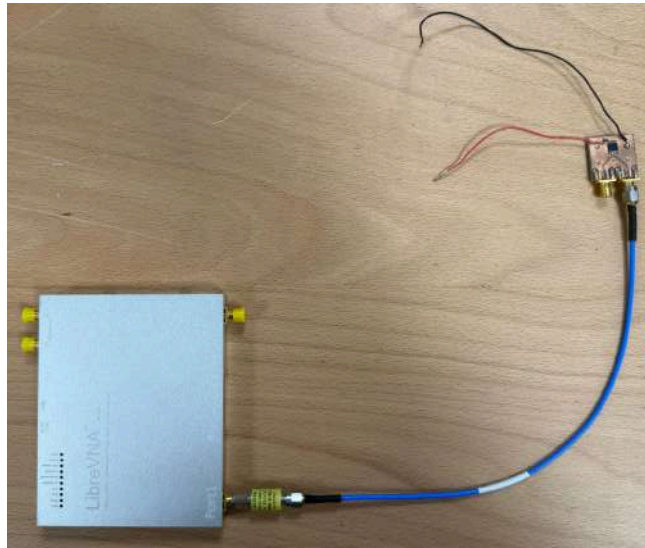
Modification de la mesure :

Après discussion avec mon encadrant, il m'a suggéré plutôt, et comme sur l'article de Hayashi de mesurer dans un premier temps l'inverseur, le même qu'eux avait utilisé afin de mesurer l'impédance en fonction de la fréquence de l'inverseur avant de commencer à mesurer les variations d'impédances de la communication entre les STM32. Mon signal SS ne servira que d'alimentation pour l'état HIGH et LOW qui sera injecté à l'entrée de l'inverseur.

Pourquoi ? Car c'est plus simple à mesurer car l'inverseur est adapté en impédance et que l'on veut retrouver l'écho avec la courbe de l'impédance en fonction de la fréquence.

BOUAMAMA. O

Ajout de l'inverseur :



Ajout de la mise en HIGH ou en LOW manuellement grâce à la fonction *commande* :

```
void loop() {  
  if (Serial.available()) {  
    char command = Serial.read();  
  
    if (command == 'b') { // Appuyer sur b pour activer l'esclave  
      digitalWrite(SS_PIN, LOW);  
      Serial.println("SS = LOW (esclave activé)");  
    }  
    else if (command == 'h') { // Appuyer sur h pour désactiver l'esclave  
      digitalWrite(SS_PIN, HIGH);  
      Serial.println("SS = HIGH (esclave désactivé)");  
    }  
  }  
}
```

*Contrôle du SS avec la fonction command*

```
SS = HIGH (esclave désactivé)  
SS = LOW (esclave activé)  
SS = HIGH (esclave désactivé)  
SS = LOW (esclave activé)
```

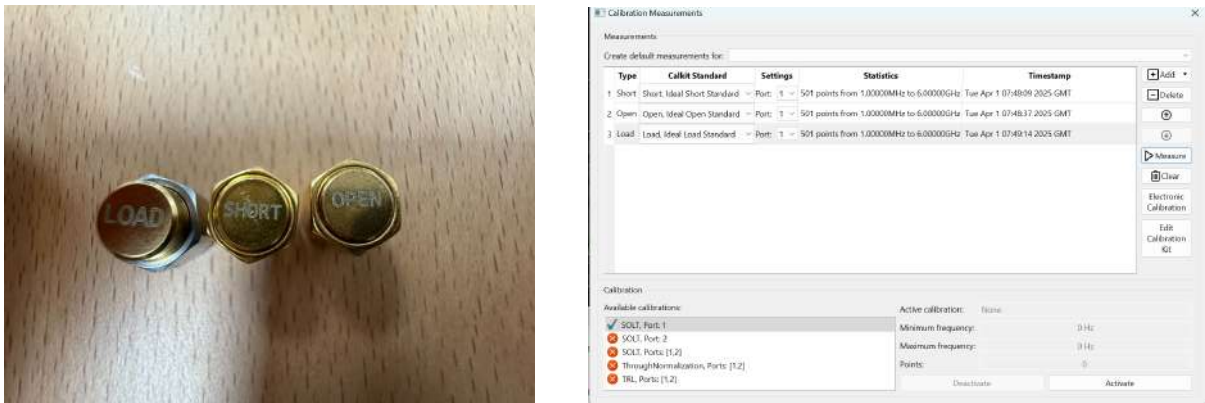
*Résultat de la commande*

Comme convenu, le SS ne servira que d'envoi d'état HIGH et LOW afin d'alimenter l'inverseur.

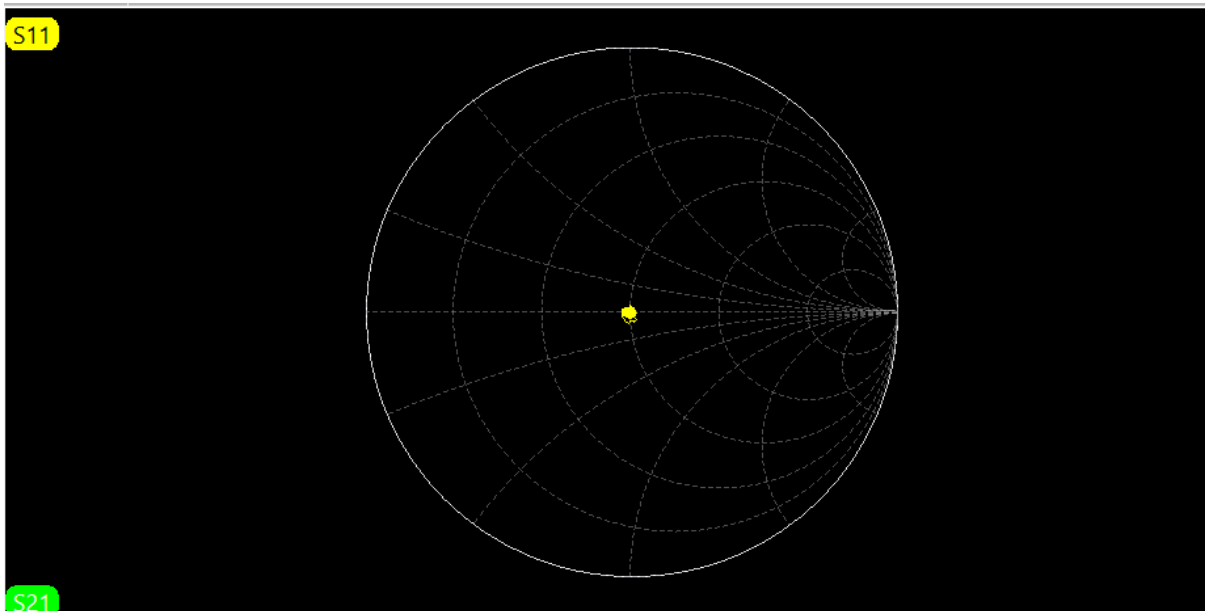


BOUAMAMA. O

Calibration du VNA sur un seul port :

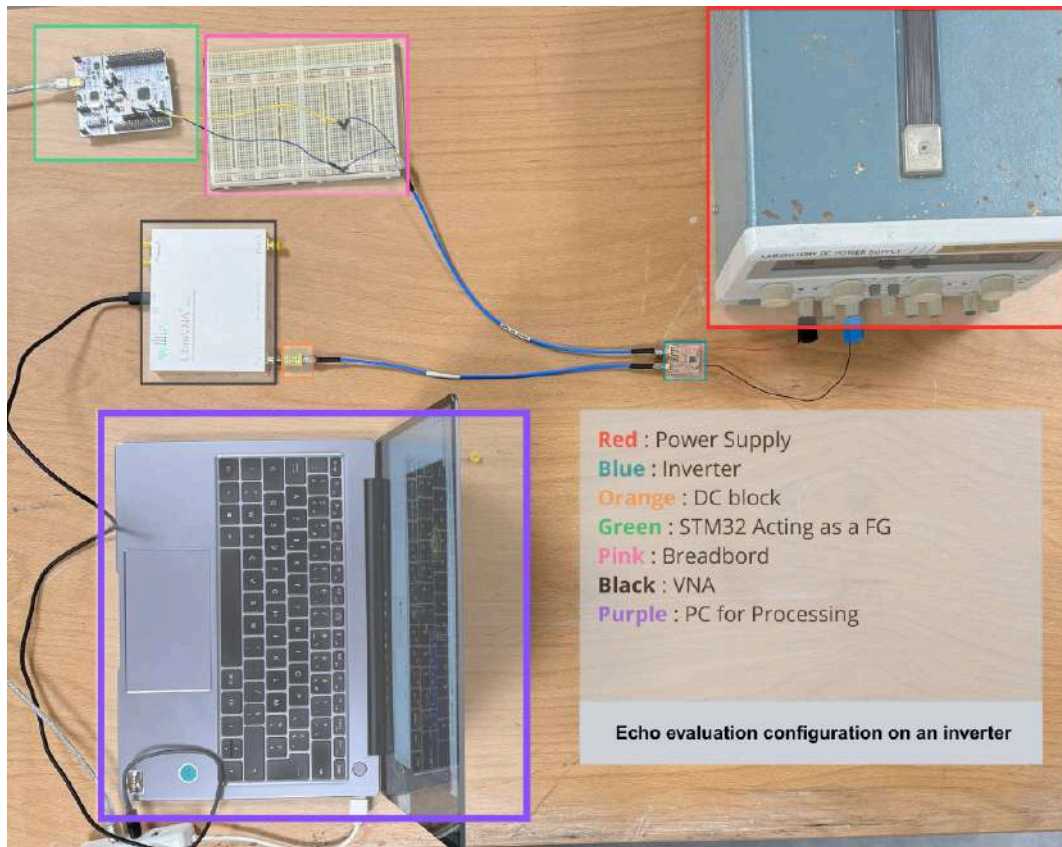


Résultat de la calibration (S11)



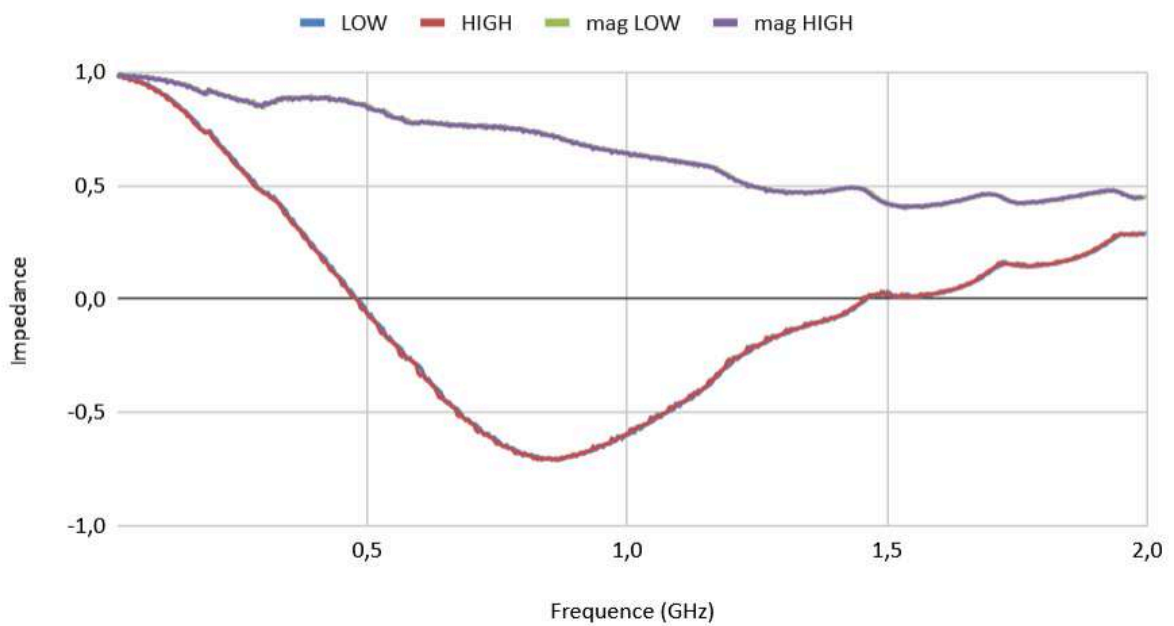
PUCE #1 : 74HCU04: non-bufferisé





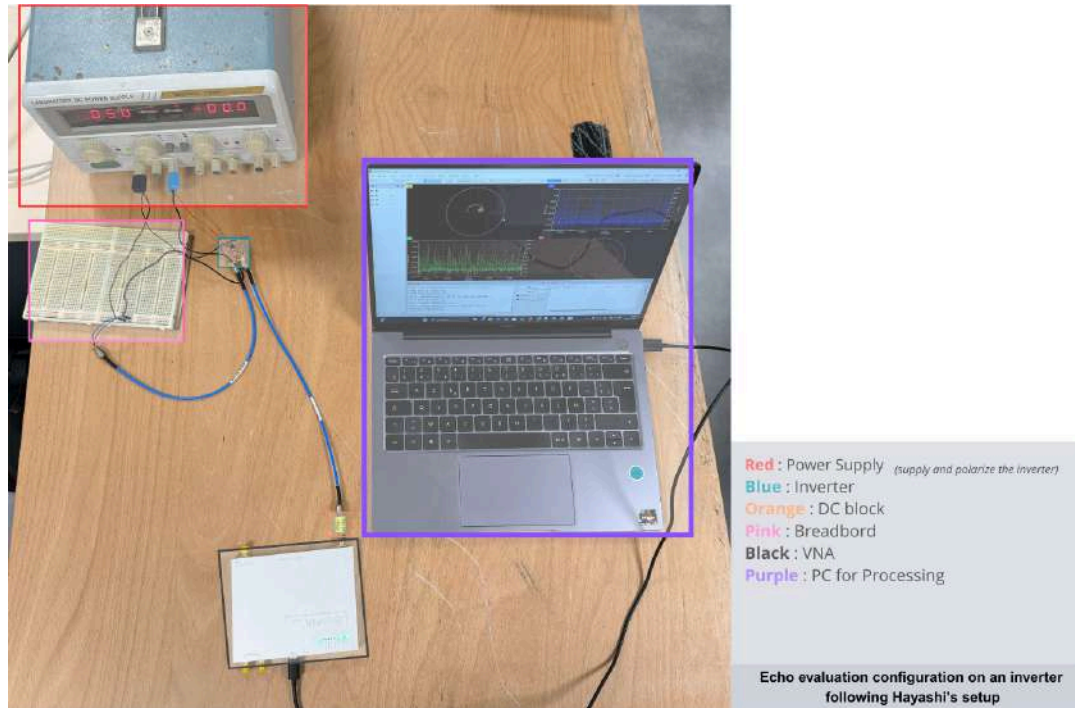
*Setup pour l'évaluation d'écho sur inverseur*

## Impedance en fonction de la Frequence



## Test avec polarisation de l'inverseur (HCU04) avec le DC supply power

### Dispositif expérimental

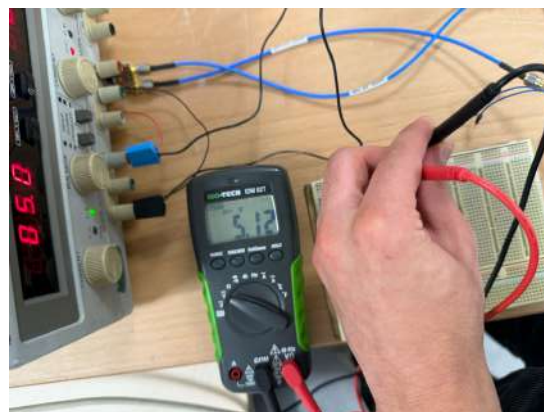


Prétest :

Je m'assure que la tension est correcte dans toutes les branches du circuit pour une tension de 5V appliquée par l'alimentation :



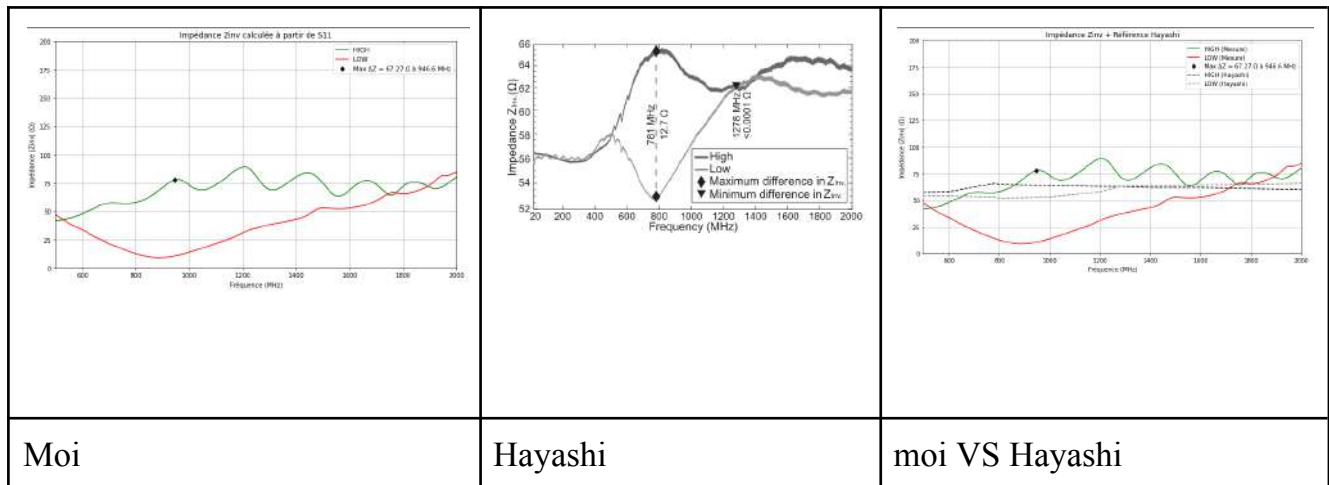
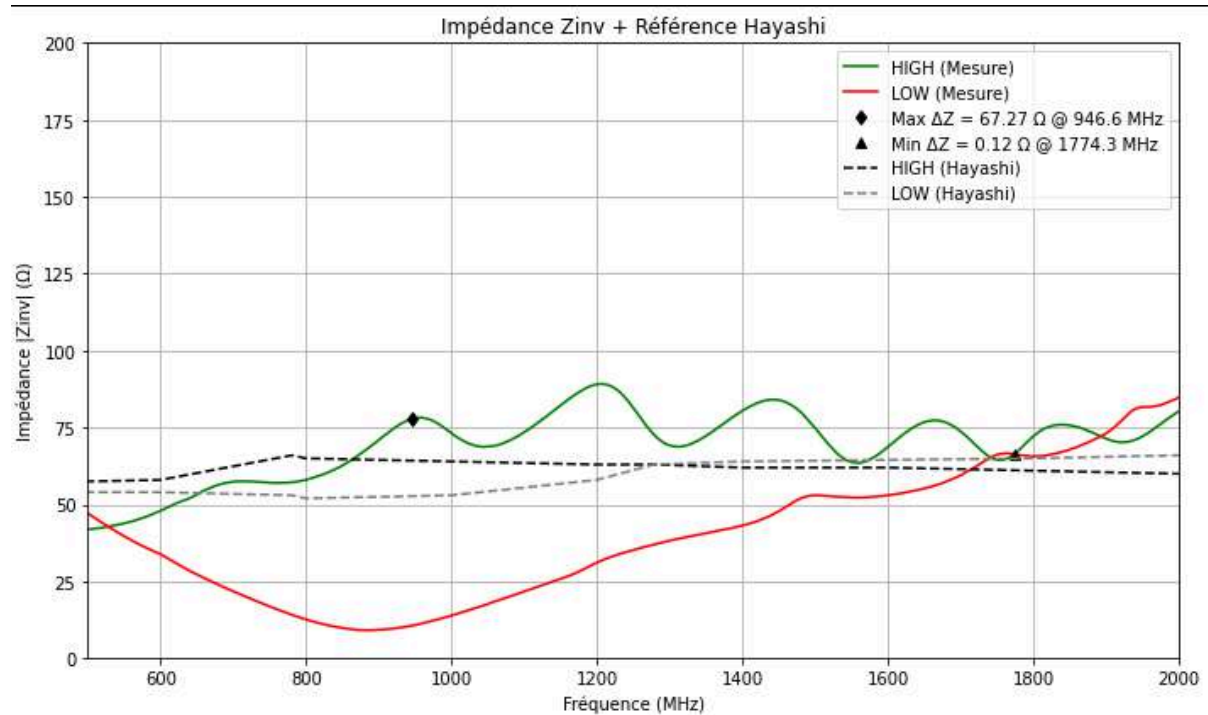
Sur le câble SMA = ok



Sur la breadboard = ok

Un autre test à l'entrée de l'inverseur et la valeur en tension était bien de 5V  
Pas de problème a priori d'alimentation au sein du montage.

Phase de test :

Impédance  $Z_{in}$  en référence à celle de Hayashi

Les mesures que j'ai effectuées présentent des similarités intéressantes avec les résultats obtenus par Hayashi, tout en révélant quelques différences notables. La courbe d'impédance montre une évolution comparable entre 600 MHz et 1200 MHz, avec une séparation claire



entre les états HIGH et LOW qui confirme le comportement attendu du dispositif. Cette similarité dans la tendance générale valide dans l'ensemble l'approche expérimentale.

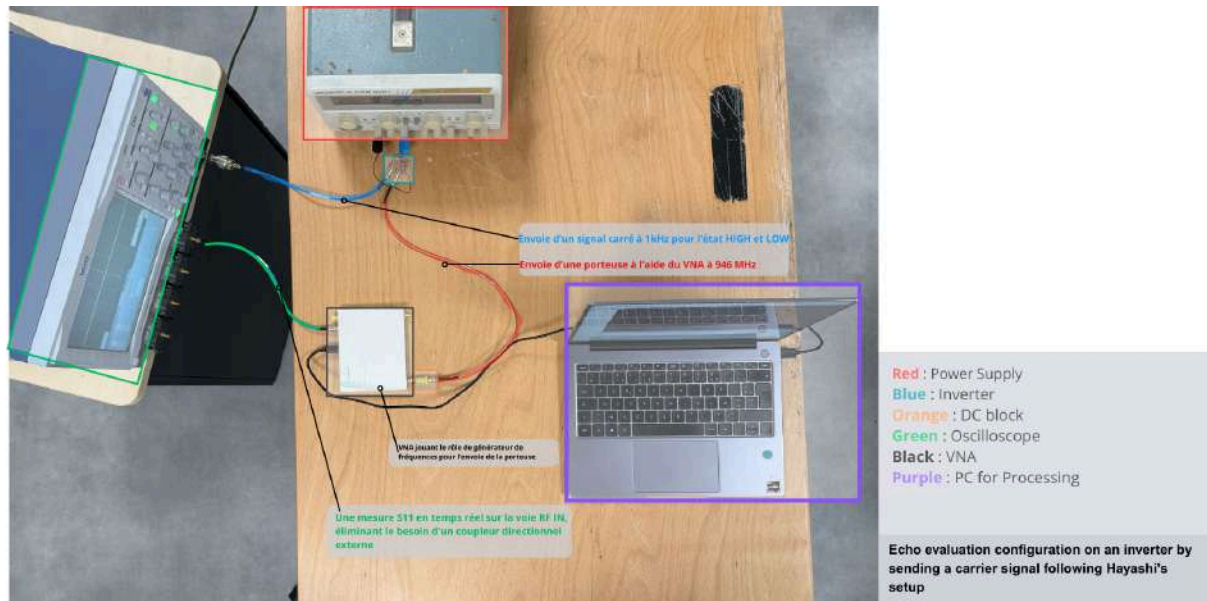
Cependant, plusieurs écarts quantitatifs apparaissent dans les résultats. L'écart maximal d'impédance ( $\Delta Z$ ) que j'obtiens atteint  $66.11 \Omega$  à 954.6 MHz, alors que les valeurs rapportées par Hayashi semblent légèrement différentes. De plus, la plage fréquentielle où les états HIGH et LOW restent distincts s'étend jusqu'à 1800 MHz dans mes mesures, contre 1200 MHz dans les données de référence. Ces variations pourraient s'expliquer par plusieurs facteurs expérimentaux.

L'utilisation d'un VNA plutôt que d'un analyseur de spectre constitue une différence méthodologique importante. Bien que plus directe et précise pour les mesures d'impédance, cette approche peut introduire des spécificités dans les résultats. J'ai vérifié l'influence des câbles SMA en testant deux configurations différentes, sans observer de variation significative, ce qui élimine ce paramètre comme source d'erreur. La calibration du VNA a été soigneusement effectuée, mais des différences subtiles dans la procédure pourraient contribuer aux écarts observés.

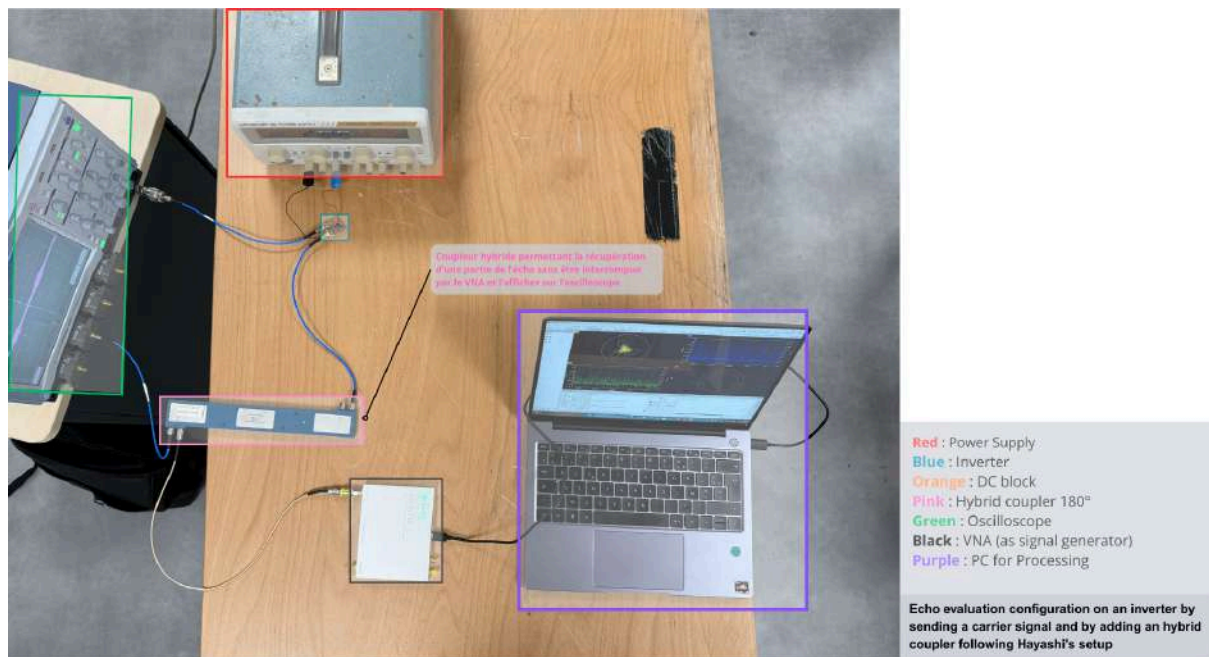
Pour approfondir cette analyse, il serait particulièrement instructif de réaliser des mesures supplémentaires sur d'autres exemplaires de la puce. Cette approche permettrait de vérifier la reproductibilité des résultats et de s'assurer que les différences observées ne proviennent pas de variations entre composants. Une telle validation expérimentale apporterait une confirmation solide de la fiabilité des mesures et de la cohérence de la méthodologie employée.

## Setup récupération de l'écho par l'envoi d'une porteuse

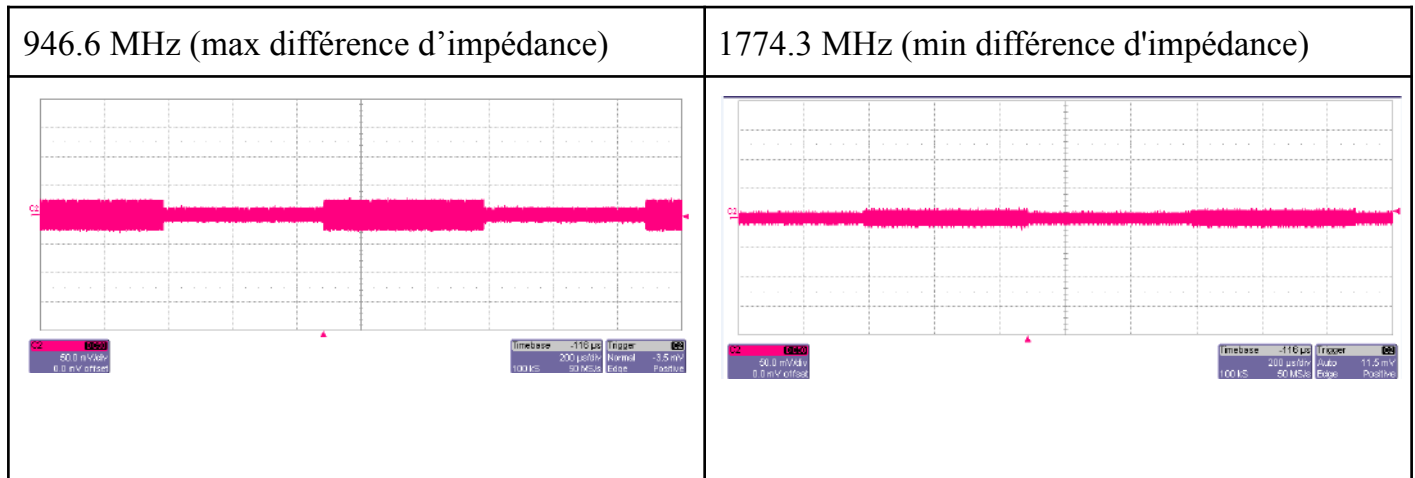
Sans coupleur hybride 180° :



avec coupleur hybride 180°:



## Visualisation de l'écho via l'oscilloscope



Dans le cadre de mes travaux, j'ai cherché à reproduire le protocole expérimental décrit par Hayashi dans ses recherches sur l'Echo TEMPEST. L'objectif principal consistait à observer et caractériser les phénomènes d'écho générés par la modulation d'impédance d'un circuit inverseur (DUT) soumis à une excitation RF, tout en commutant ses états logiques HIGH et LOW à une fréquence de 1 kHz. Cette étude s'inscrit dans le cadre plus large de l'analyse des vulnérabilités électromagnétiques des systèmes électroniques.

### Première configuration expérimentale

Initialement, j'ai mis en place un montage simplifié reprenant les éléments clés du dispositif de Hayashi. L'oscilloscope jouait un double rôle : d'une part, il générait le signal carré de 1 kHz via sa sortie AUX OUT pour piloter la commutation du DUT, et d'autre part, il devait permettre l'observation temporelle de l'écho. Le VNA était utilisé comme générateur de la porteuse RF, tandis que son entrée RF IN servait à capter le signal réfléchi. Cependant, cette configuration n'a pas donné les résultats escomptés. Après plusieurs tentatives, j'ai constaté que l'architecture interne du VNA semblait bloquer ou atténuer considérablement le signal d'écho, rendant son observation impossible sur l'oscilloscope.

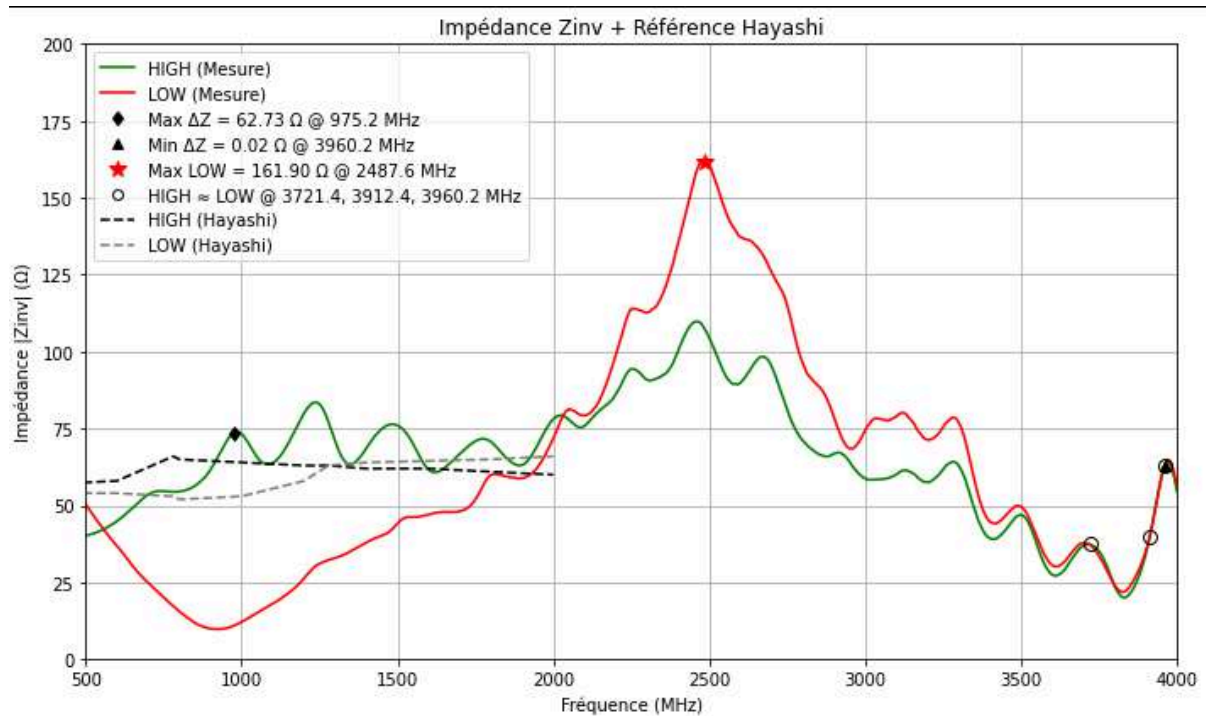
### Optimisation du dispositif de mesure

Afin de pallier cela, j'ai modifié le montage en introduisant un coupleur hybride 180° (prêté par M. HIMDI). Le coupleur m'a permis de récupérer l'écho et de le diriger vers l'oscilloscope sans être affecté par les caractéristiques du VNA. Le coupleur hybride permettait ainsi une mesure directe et fiable de la réflexion générée par le DUT, tout en conservant la possibilité d'injecter la porteuse RF.

## Analyse des résultats obtenus

En appliquant une porteuse à 946,6 MHz, fréquence correspondant au maximum de variation d'impédance, j'ai pu observer clairement sur l'oscilloscope le signal carré de 1 kHz commutant l'état HIGH et LOW de l'inverseur. L'amplitude importante de ce signal confirmait la forte variation d'impédance entre les états HIGH et LOW du DUT à cette fréquence. À l'inverse, lorsque la porteuse était réglée à 1774,3 MHz sur le générateur de fréquence, le signal de modulation apparaissait beaucoup plus atténué, ce qui confirme bien les résultats que j'avais obtenue lors du tracé de l'impédance en fonction de la fréquence. Ces résultats démontrent que l'amplitude de l'écho est directement liée à la variation d'impédance du circuit à la fréquence de la porteuse utilisée.

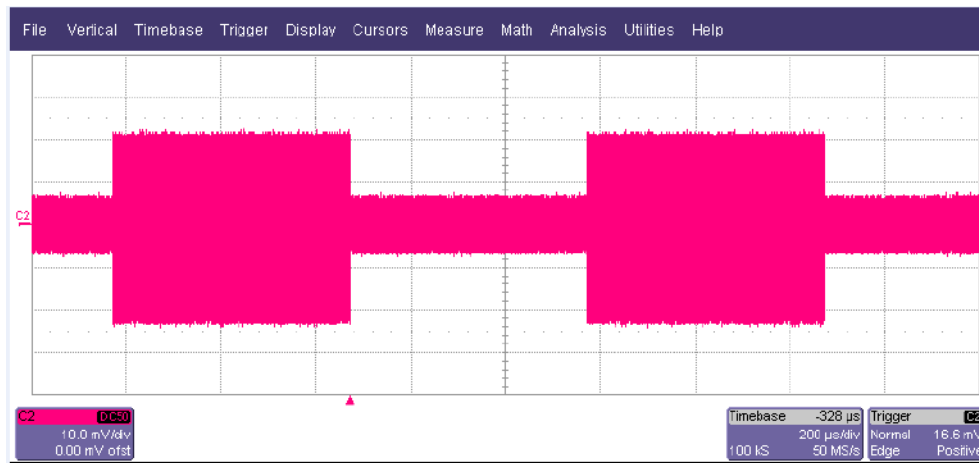
Test de l'impédance en fonction de la fréquence jusqu'à 4 GHz



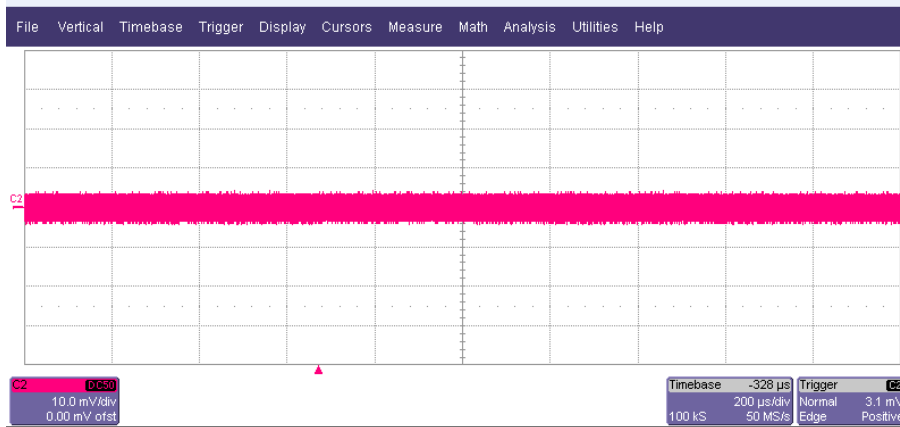


BOUAMAMA. O

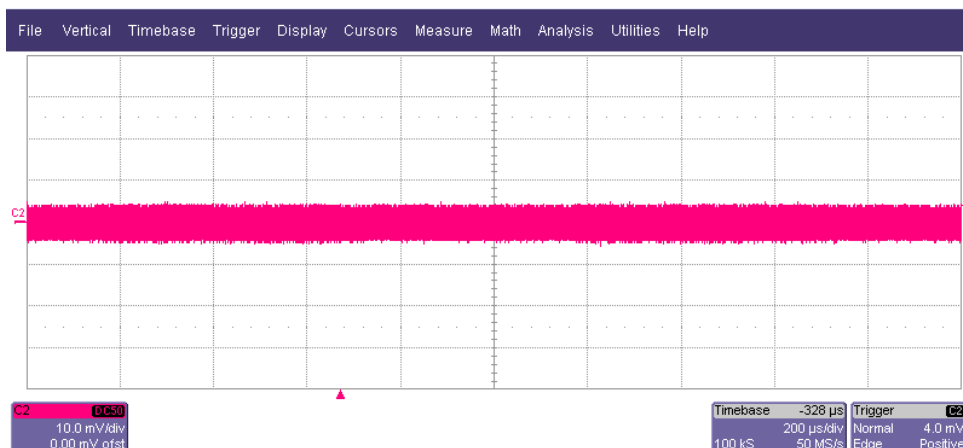
Pour 975.2 MHz (différence max en impedance)



Pour 3960.2 MHz (différence min en impedance)

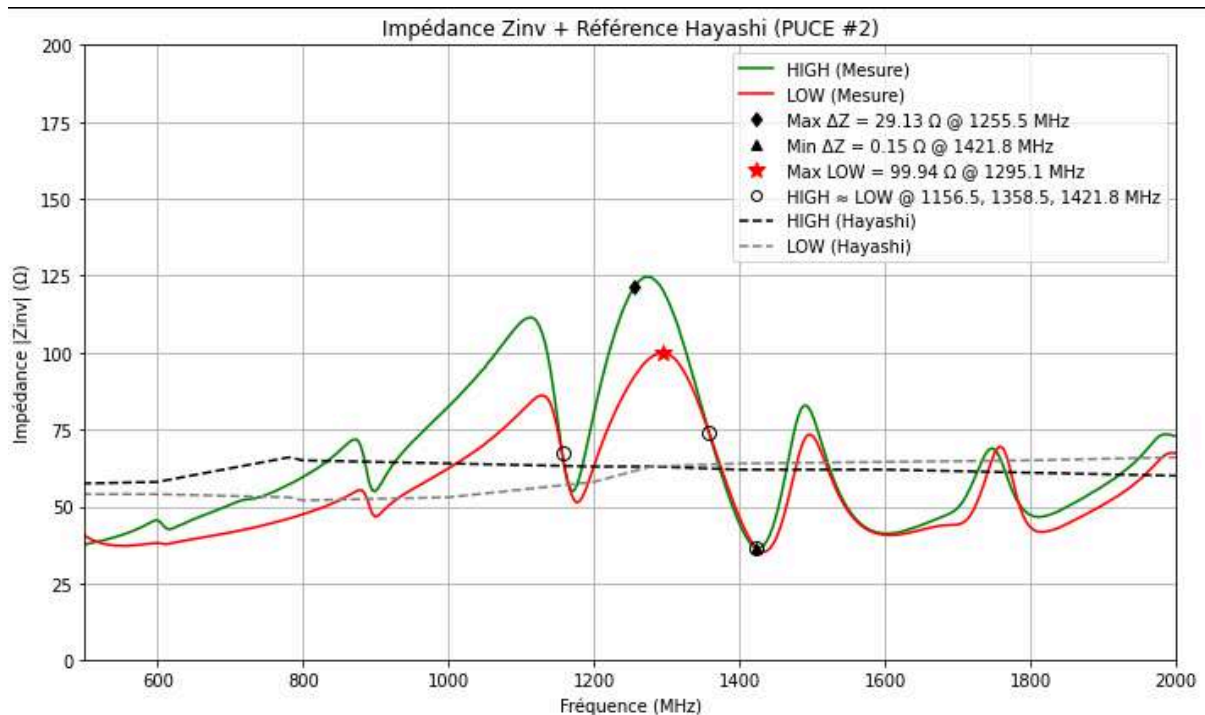


Pour 3721.4 MHz (autre min diff impedance)



**PUCE #2 : 74HCT : bufferisé (transition plus abrupte et non analogique)**

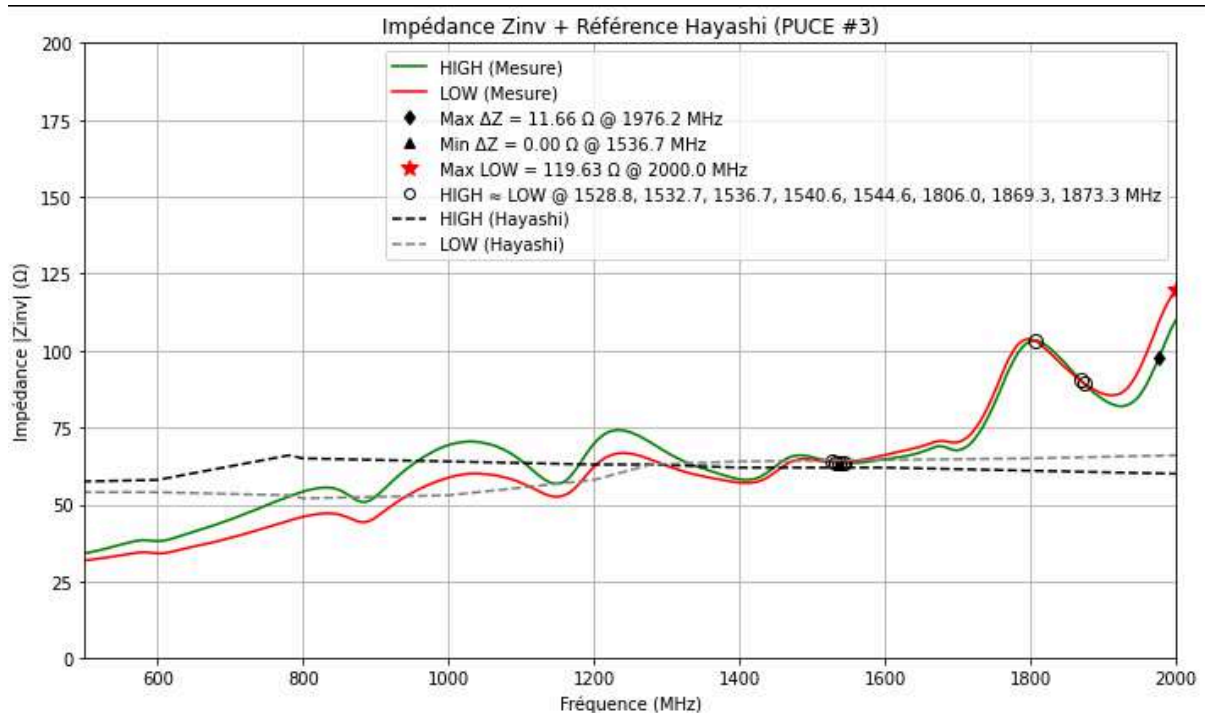
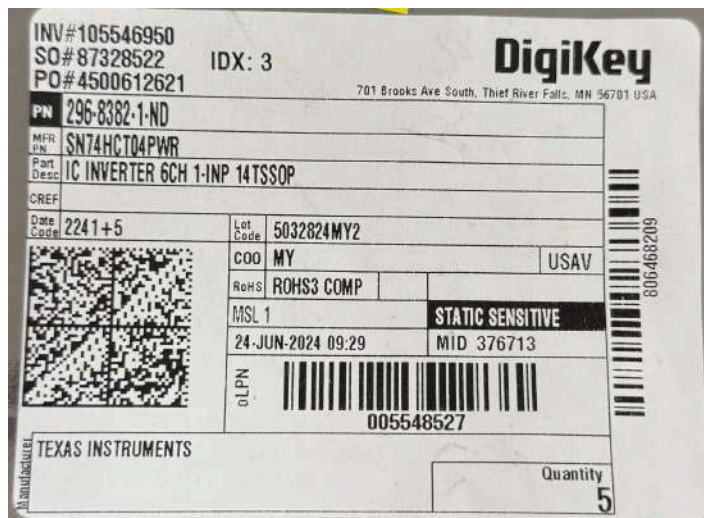
Test de l'impédance en fonction de la fréquence sur un autre inverseur (HCT)



Remarque : Un inverseur non bufferisé (comme le 74HCU04) fonctionne de manière plus analogique, ce qui permet d'observer finement les variations d'impédance entre les états logiques HIGH et LOW. À l'inverse, un inverseur bufferisé (comme le 74HCT04) intègre des étages de gain internes qui saturent rapidement la sortie, rendant les transitions très franches mais masquant toute variation subtile dans la mesure de l'impédance en fonction de l'inverseur

BOUAMAMA. O

PUCE #3 : SN74HCT04PWR : Bufferisé



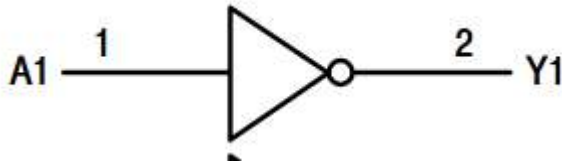
Remarque : même remarque que la puce #2

### Explication :

#### Non bufferisé

Un seul étage CMOS (transistors P et N complémentaires).

- L'impédance de sortie dépend plus finement de l'état logique appliqué à l'entrée.
- Sensible aux variations de charge, température, etc.

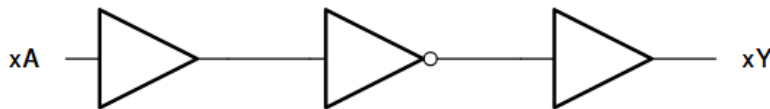


Un seul étage

### Bufferisé

Plusieurs étages d'inversion (2 ou plus) → **"bufferisé"**.

- La sortie est plus franche (rail-to-rail), indépendante de la charge.
- Meilleure immunité au bruit.
- L'impédance de sortie est plus stable, donc moins influencée par l'état logique en entrée.
- Les étages supplémentaires standardisent le signal.



### **Functional Block Diagram**

- Le premier inverseur fait le travail logique (inversion).
- Le second inverseur restaure et stabilise le signal.
- Le troisième agit comme buffer pour augmenter la capacité en courant et stabiliser les temps de transition.

Un inverseur non bufferisé (comme le HCU04) a une impédance qui varie fortement selon l'état logique (HIGH ou LOW), car la transition se fait directement au niveau du transistor CMOS de base.

C'est ce changement d'impédance qui est exploitable par une attaque Echo TEMPEST.

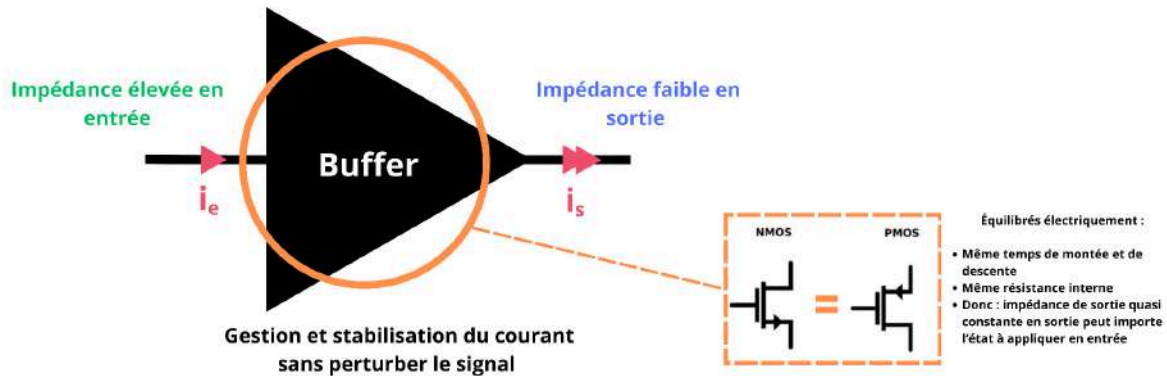
Mais un bufferisé ajouté :

- des transistors supplémentaires,
- une sortie amplifiée et protégée,
- une stabilisation des fronts.



Résultat : les états HIGH et LOW ont une impédance de sortie similaire, donc moins de contraste entre les deux états.

En réalité, quand on bufferisé on ajoute un étage d'amplification à gain de 1 avec pour entrée une impédance élevée permettant de gérer les faibles courants sans perturber le signal et permet de fournir, en sortie, un courant idéal afin de piloter ayant une impédance d'entrée plus faible.



Pourquoi l'impédance des HIGH et LOW dans le cas bufferisé on des courbes relativement similaire :

En fait, dans un inverseur bufferisé, les transistors de sortie (PMOS et NMOS) sont dimensionnés de manière symétrique et contrôlés par des étages internes qui régulent précisément leur activation. Cela permet à la sortie de fournir un signal robuste, que ce soit à l'état HIGH ou LOW, avec une capacité de courant importante et bien stabilisée. En conséquence, l'impédance vue en sortie reste pratiquement identique quel que soit l'état logique, ce qui explique pourquoi les courbes HIGH et LOW se superposent lors des mesures.

Source : <https://rajeev2007.github.io/VLSI/0072460539cmos.pdf> (voir chapitre 5)

Où peut-on les trouver :

Les inverseurs non-bufferisés sont souvent utilisés dans des circuits analogiques, oscillateurs RC, ou applications sensibles où l'impédance de sortie varie volontairement.

Les inverseurs bufferisés sont faits pour du traitement logique standard, avec des sorties à faible impédance constante, pour conduire facilement des charges.

Lien qui explique que les buffer permettent de stabiliser le signal : <https://www.y-ic.fr/blog/A-Complete-Guide-to-Buffer-Gates-in-Digital-Electronics.html> avec la citation :

*“Les tampons peuvent sembler des composants simples, mais leur impact sur la stabilité du circuit et la clarté du signal est substantiel. Des conceptions de base à deux investisseurs aux*

*configurations de collecteur ouvert et totem, les tampons jouent un rôle sérieux dans le renforcement des niveaux de logique et la prévention de la dégradation du signal.”*

## Etude électronique et fréquentiel d'un clavier

### Fabricant du pcb : Fabricant du PCB :

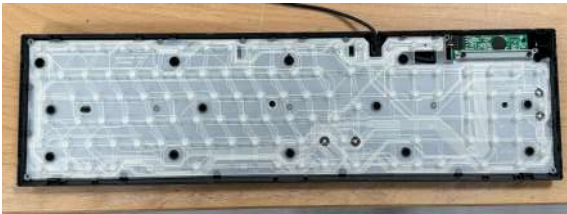
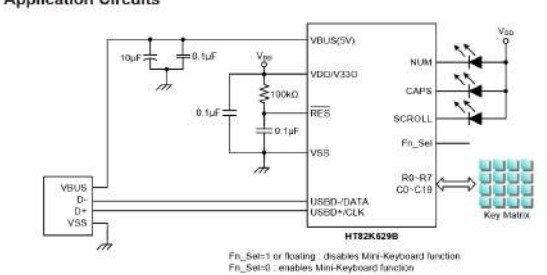
Guangdong Hetong Technology Co Ltd  
Third Road, PuXin Industrial Zone, Shipai Town, DongGuan, Guangdong 523330,  
China

### Puce :

Potentielle Datasheet : Puce HOLTEK HT82K629B

<https://www.holtek.com/webapi/116711/HT82K629Bv110.pdf>

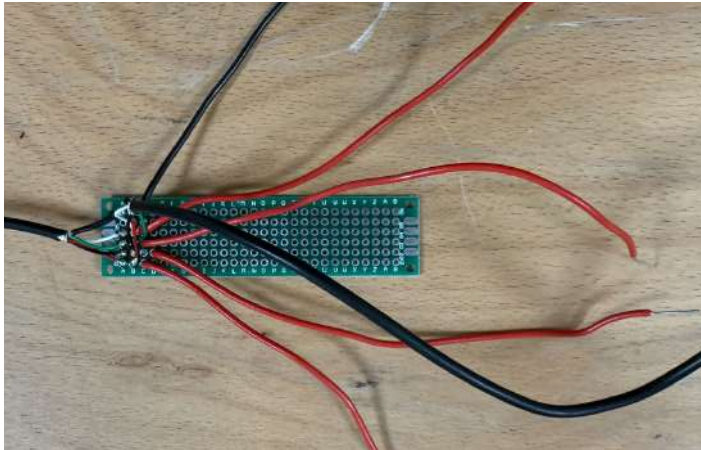
### Composition d'un clavier :

	<p><b>Application Circuits</b></p>  <p>HT82K629B</p> <p>Fn_Set=1 or floating : disables Mini-Keyboard function Fn_Set=0 : enables Mini-Keyboard function</p>
Intérieur d'un clavier physique (Dell)	Application circuits (Dell)

## Fonctionnement d'un clavier

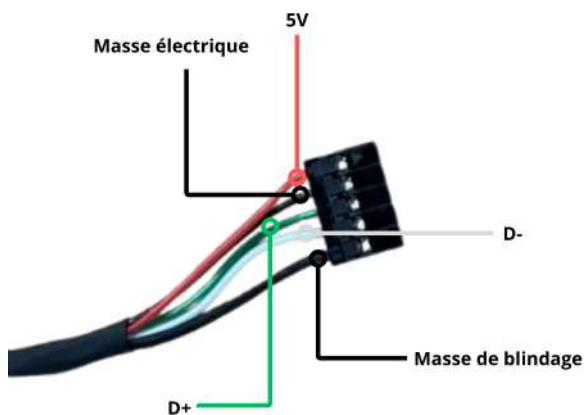
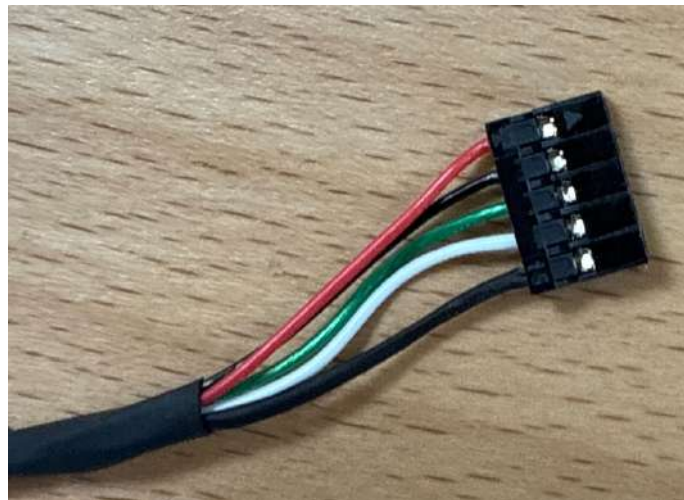
La routine de balayage matriciel des touches (scanline routine)

Ajout d'un trojan pour observer les trames envoyées

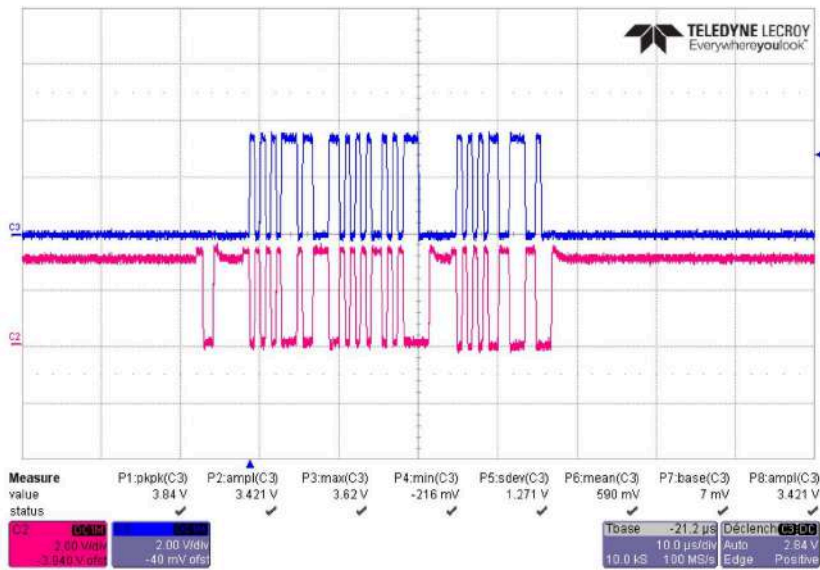


### Test de continuité :

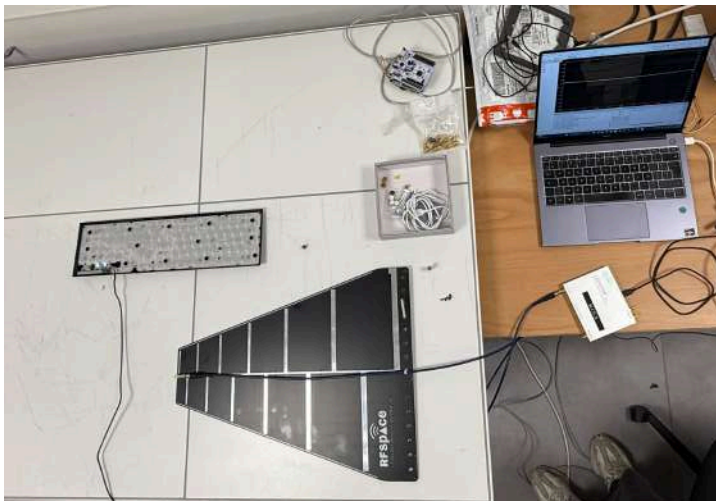
Le test de continuité m'a permis d'identifier entre les deux masses présentent laquelle faisant office de masse électrique et laquelle servait au blindage et de tresse métallique protégeant les signaux d' interférence électromagnétique. A savoir que l'embout métallique se branchant dans le pc fait office de blindage.



Visualisation de D<sup>+</sup> et D<sup>-</sup> (différentiel)



Test en réel avec vna et usrp sur un clavier dans l'espoir d'identifier les pertes à l'aide de log périodique







Test à l'usrp sur l'inverser en envoyant et réceptionnant le signal sur les fréquences delta max impédance et delta min

