THOMSON TMF & ALCATEL ATR 42x / 921x MB

Rétro-ingénierie à partir des firmwares officiels

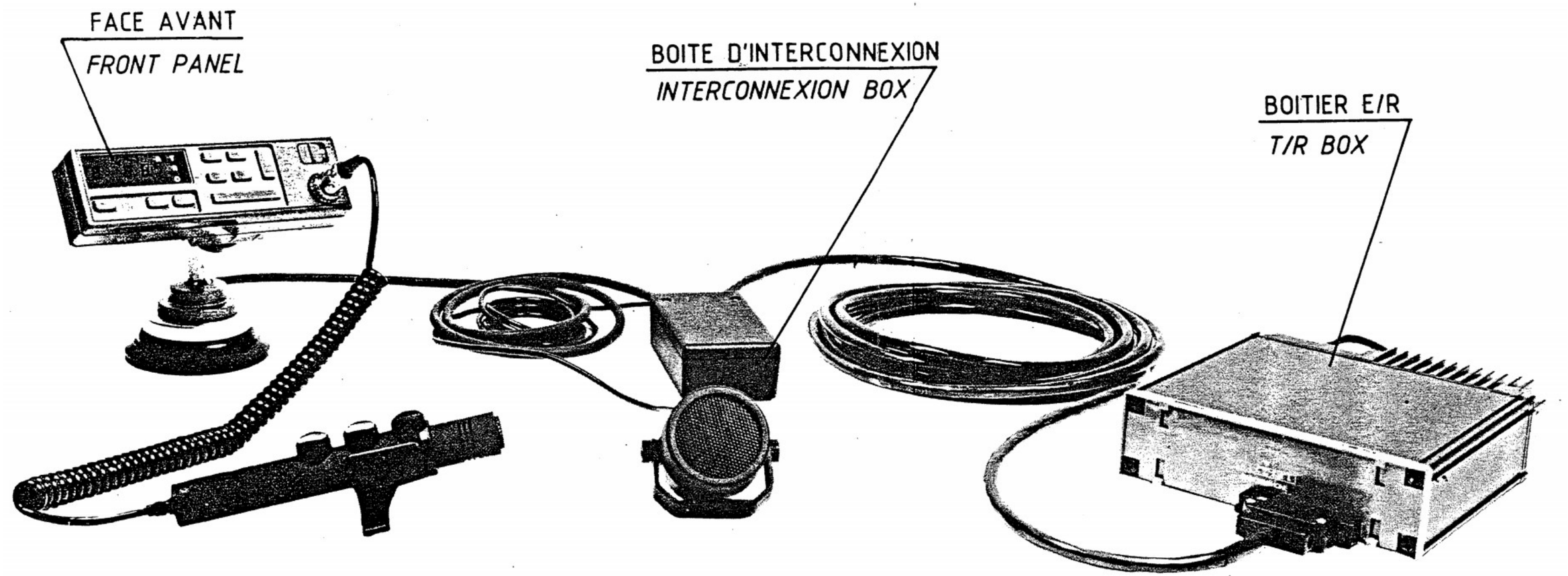


Illustration du manuel 9210 MB DGC-SC2-SC10-SC20

Table des matières

1 Introduction

Ce document regroupe les informations glanées sur Internet et le résultat de mes relevés de signaux.

15/09/2019 : Je constate, avec un peu de retard, que certains signaux sont mal décodés sur les captures d'écran, notamment les sorties des extenseurs de port. Je vais essayer de mettre à jour toutes les captures d'écran concernées.

L'objectif de cette étude est de proposer une réponse alternative à la transformation de ces postes destinés initialement à un usage professionnel, en tirant profit de toutes leurs fonctionnalités, et en y ajoutant la souplesse d'utilisation des postes radioamateur. La rétro-ingénierie est par conséquent la seule solution, puisque aucun document technique détaillé ou code source n'a été rendu publique.
J'ai regroupé en fin de ce document les adresses des sites qui ont rendu cette étude possible, ainsi que les fichiers et documents qui m'ont été transmis ensuite par d'autres passionnés.

Les protocoles de communication avec les divers périphériques seront donc détaillés autant que possible et illustrés par les captures d'écran de l'analyseur logique.

Les schémas utilisés pour mener à bien cette analyse ont été obtenus sur l'un de ces sites, et réarrangés pour améliorer nettement leur lisibilité. Ils sont disponibles ici.

Les informations ici fournies seront mises à jour au fur et à mesure de nouvelles découvertes ou de données complémentaires qui me parviendront. Vérifiez la disponibilité d'une révision plus récente en cliquant sur ce lien : vérifier maintenant.

Vous pouvez à ce titre me contacter à l'adresse e-mail suivante : blog@shibby.fr
Je suis particulièrement à la recherche du schéma électrique de la carte logique V3, ainsi que ceux des cartes radio des ATR/TMF 421 et 427 (9211 MB et 9217 MB).
N'hésitez pas non plus à me contacter si vous avez un de ces postes à céder, quelle que soit sa plage de fréquences, ou un équipement type face avant dont le modèle serait différent de ce qui est visible sur la photo en première page de ce document.

Ce document n'est encore qu'à l'état de brouillon. Pensez à vérifier la disponibilité d'une révision plus récente à l'aide du lien fourni ci-dessus.
Le texte surligné en jaune indique un résultat ou une affirmation nécessitant une analyse plus poussée afin de lever un doute, ou une section en cours d'édition/de modification.
Certains commentaires sont basés uniquement sur des infos fournies pas une ou deux personnes. Il est possible que ces informations soient erronées ou incomplètes. N'hésitez pas à me contacter si vous voyez des erreurs.

2 Glossaire

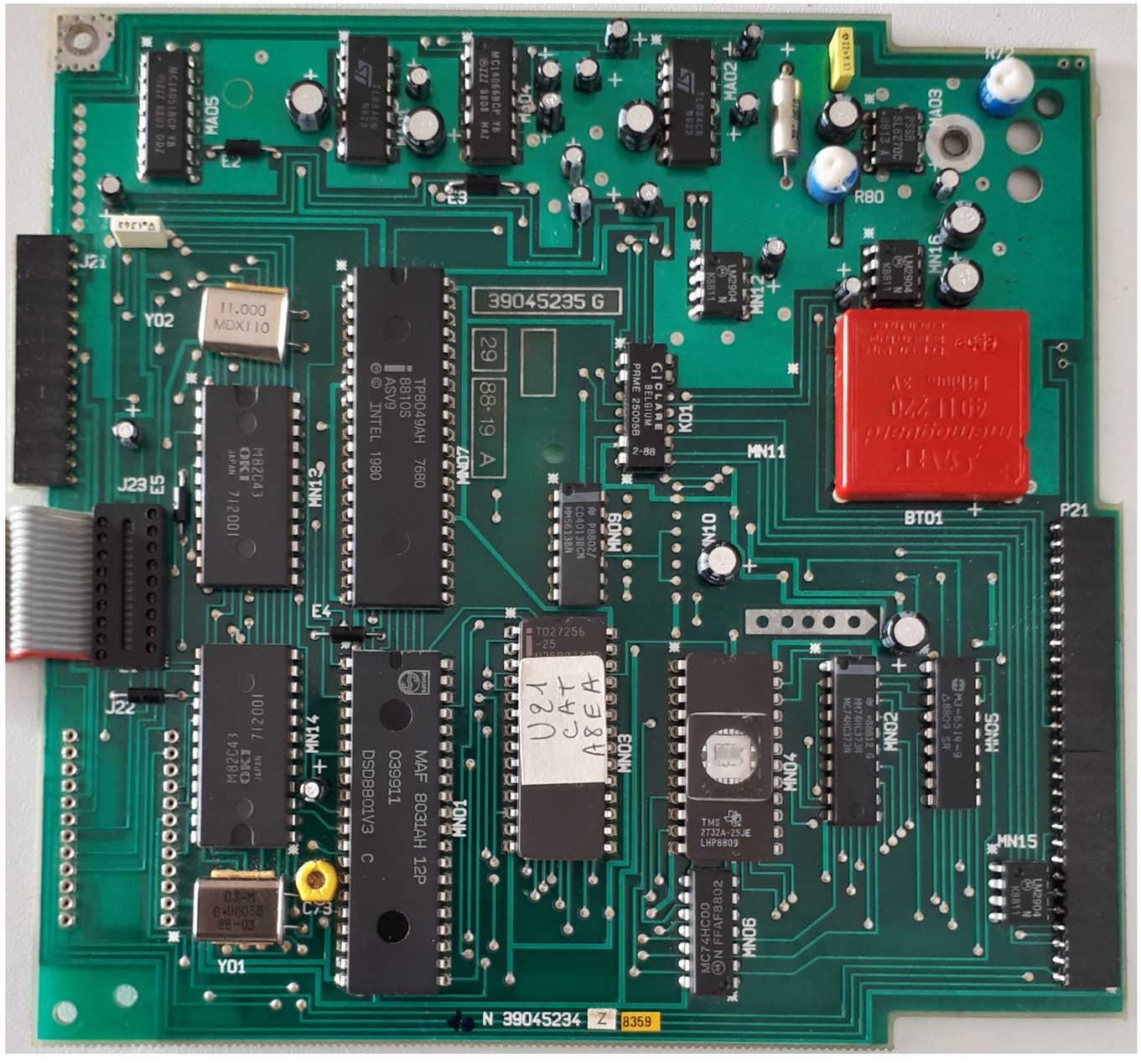
MAxx/Logique ou MNxx/Logique : Composant placé sur la carte logique
MAxx/Logique ou MNxx/HF : Composant placé sur la carte HF
HP : Haut-Parleur
µP : Microprocesseur
DP : Détection de Porteuse
AF : Audio Frequency / Fréquence Audio
ACK : ACKnowledgement / Acquittement
CER : Commande Émission/ Réception
OPE : Ordre de Passage en Émission
ETHF : Entrée de la Tête HF (préampli réception)

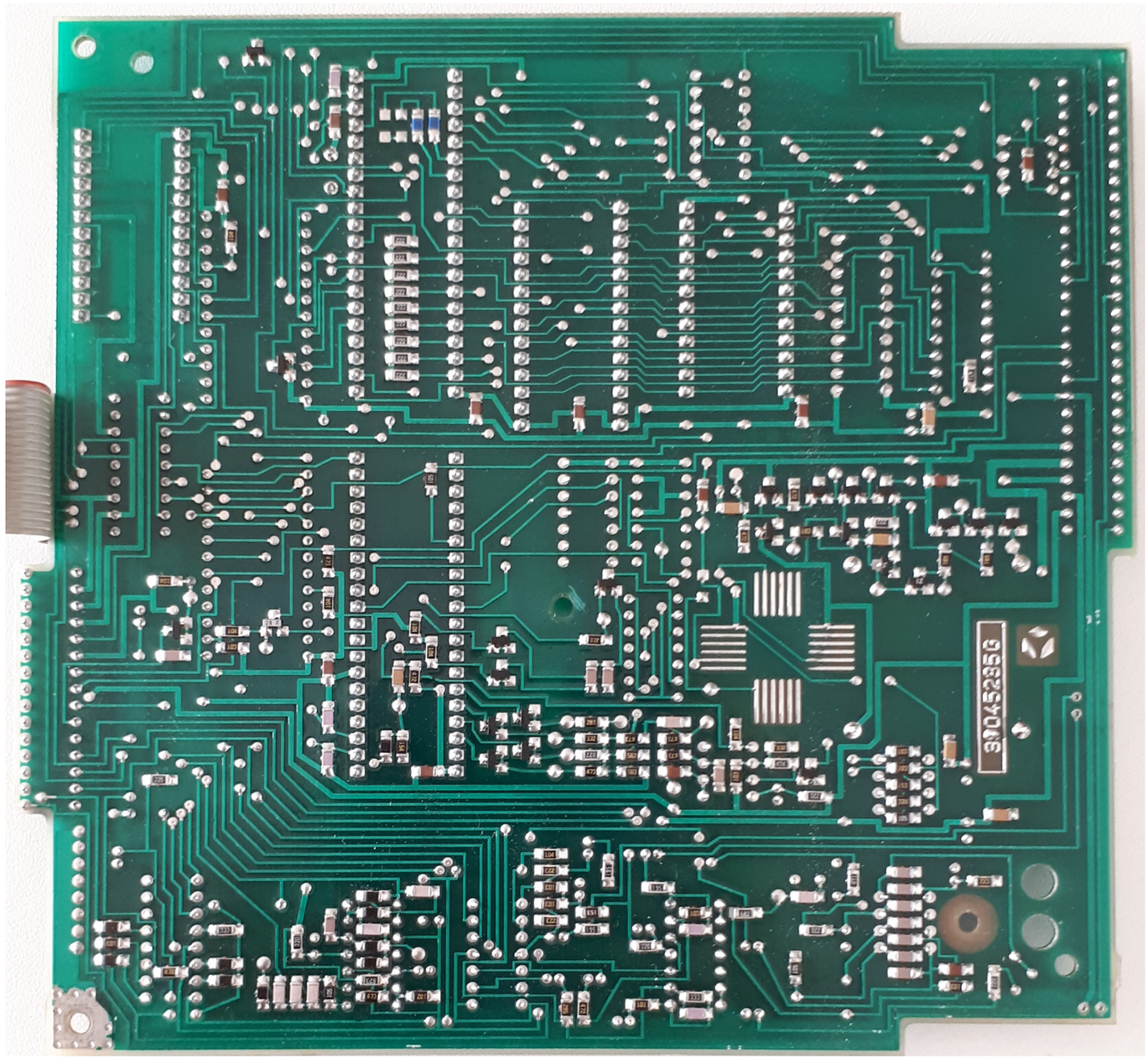
3 Points de réglage

R162 : Placée en sortie de la tête HF sur la carte radio 39 417 077 → Passée à 0R pour obtenir une sensibilité maximale

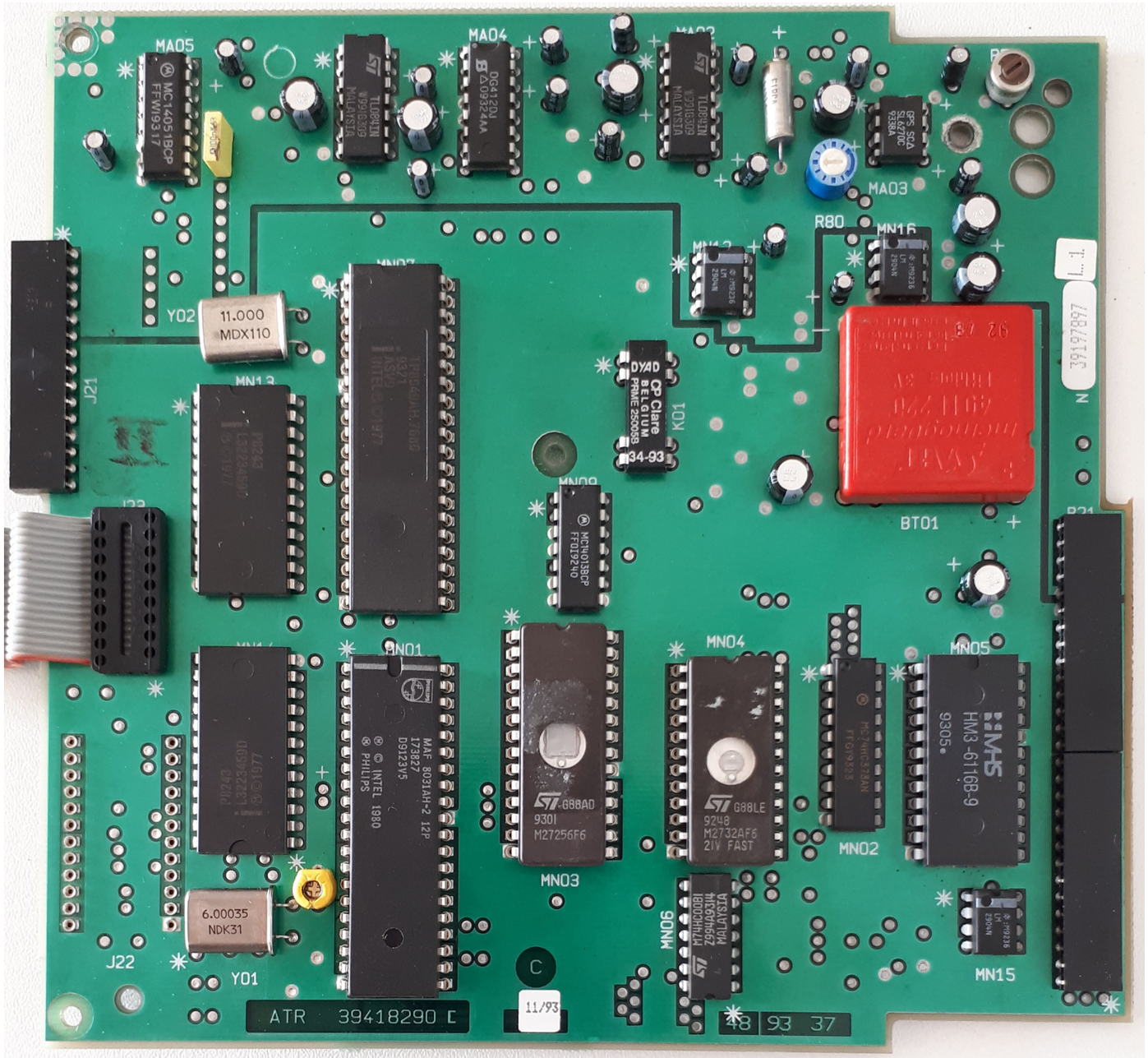
4 Identification des cartes logiques

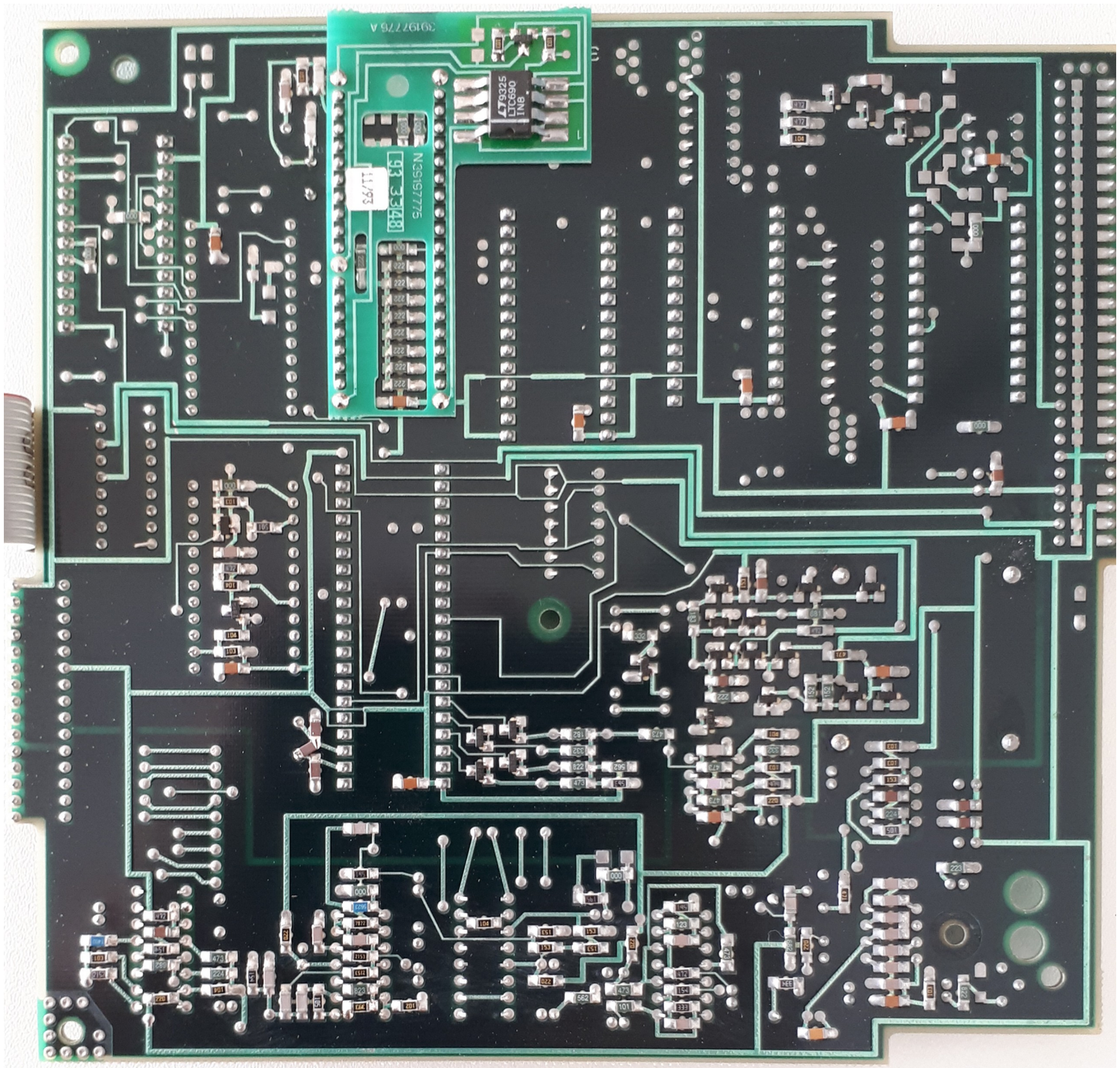
4.1 Première génération (cuivre 39 045 235)



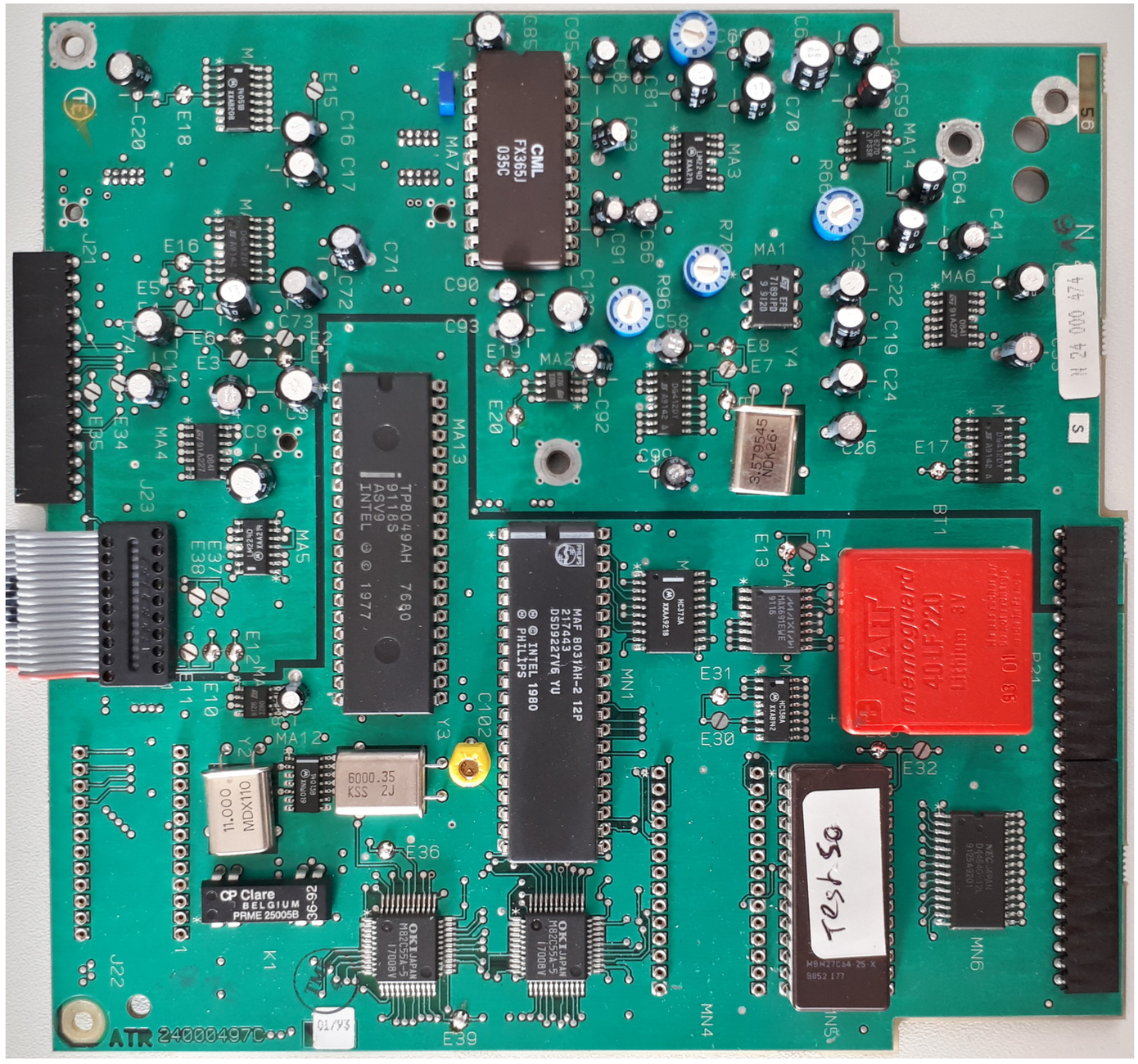

3904523SG

4.2 Deuxième génération (cuivre 39 418 290 avec circuit watchdog 39 197 776)

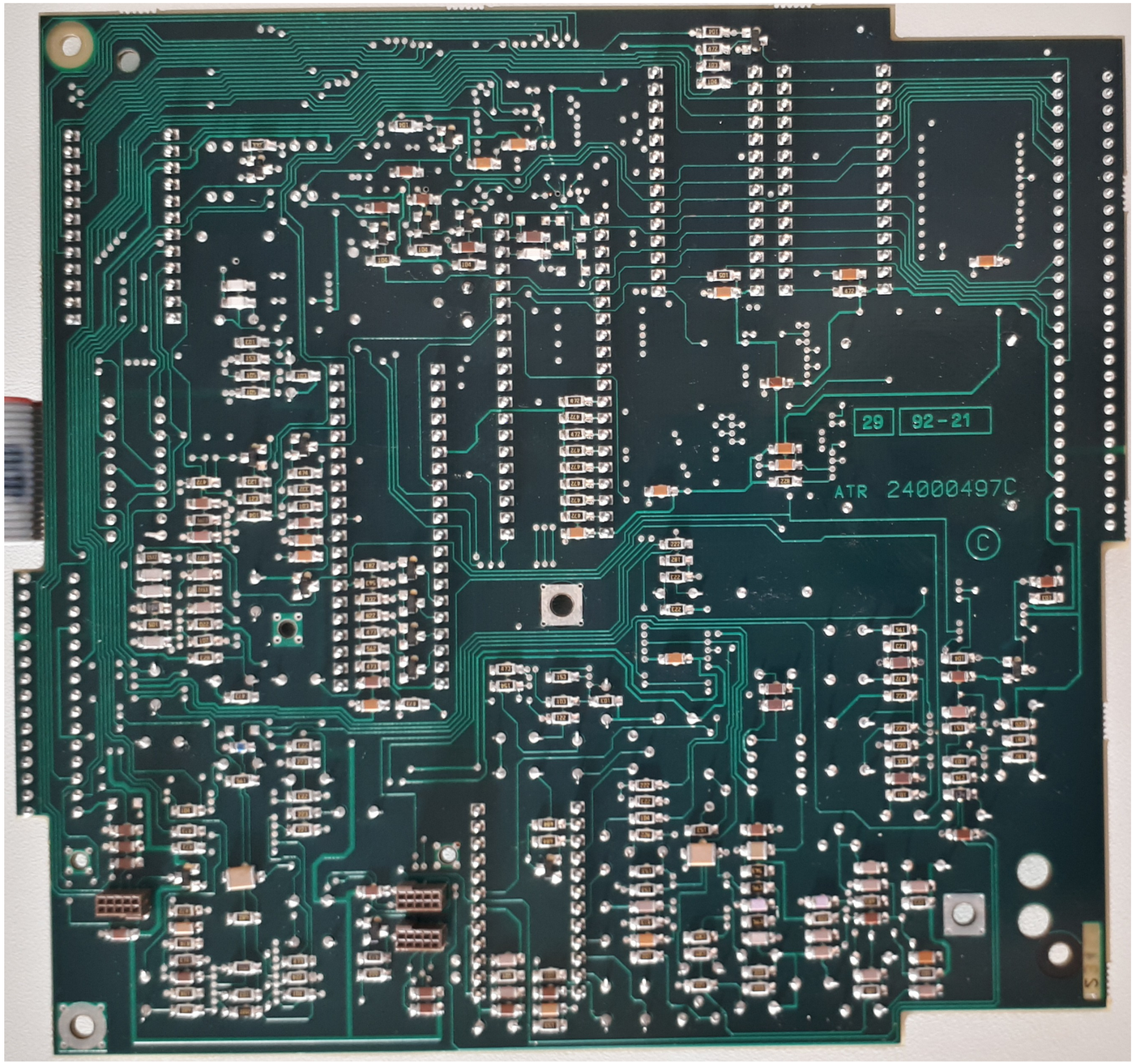



LT9325
LTC690
IN8
93 3348
11/93

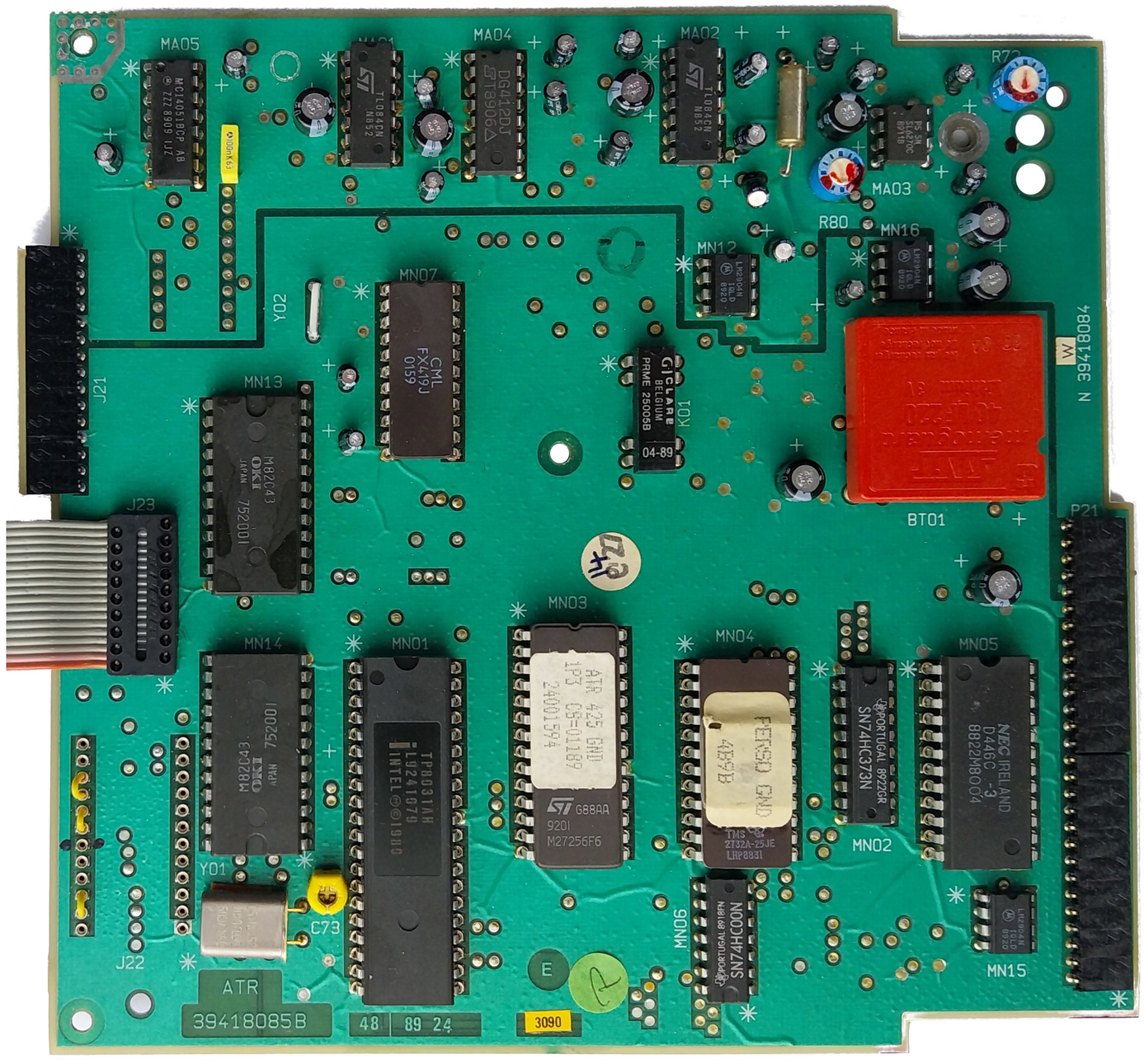
4.3 Troisième génération (cuivre 24 000 497) / Circuit logique universel (6 couches)



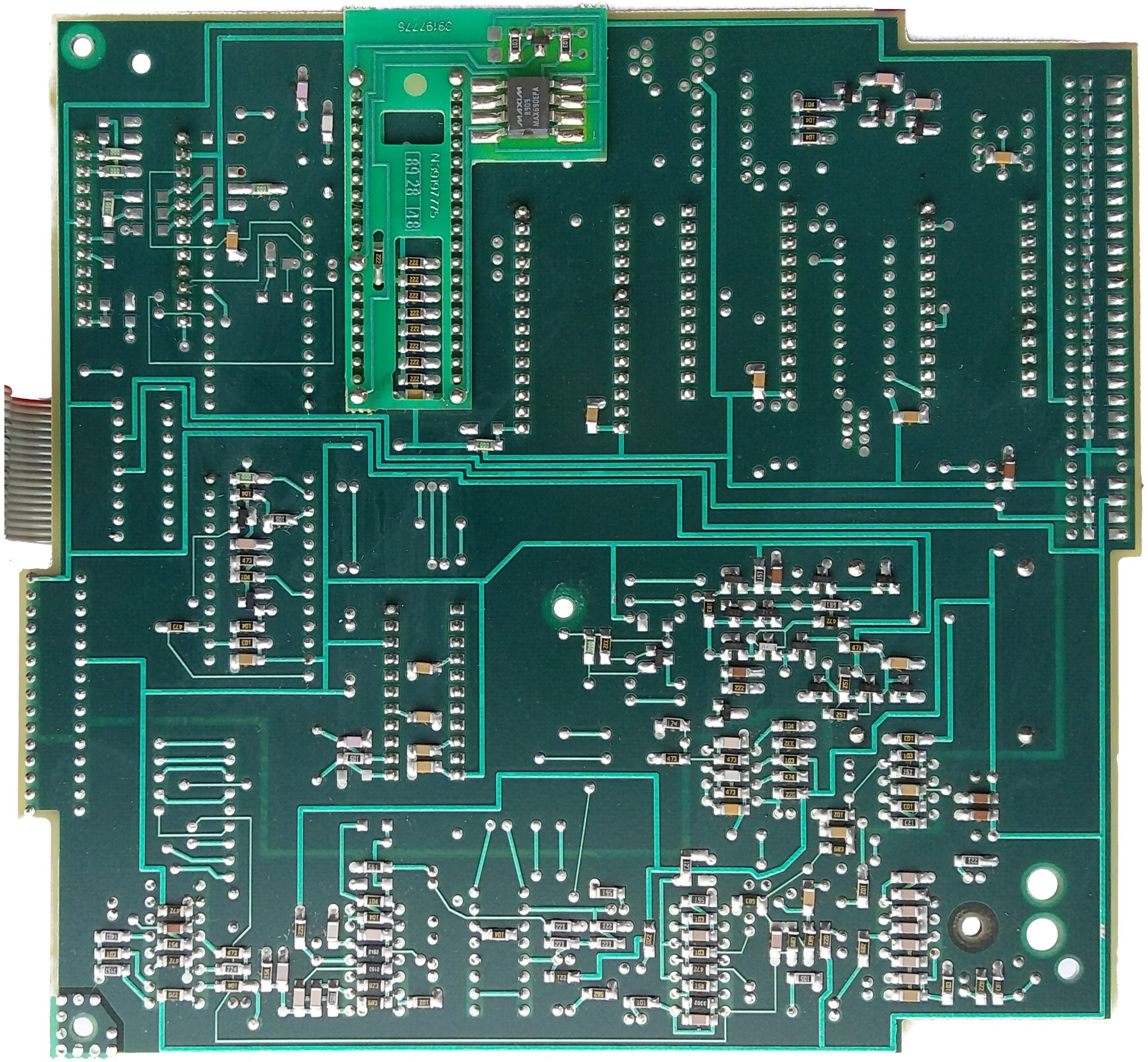
L'EPROM de gestion MN04 est absente sur cette photo.


29
92-21
ATR 24000497C

4.4 Carte signalisation numérique 6 couches (cuivre 39 418 085 avec circuit watchdog 39 197 776)



Les pontages sur J22 permettent de compenser l'absence du MICA.



5 Étude des différentes fonctions

5.1 Réglage du volume audio RX

Le réglage du volume audio du HP est assuré par le commutateur analogique MA05/logique (4051). Ce composant est piloté par 3 bits et permet donc 7 niveaux de réglage, obtenus en sélectionnant une résistance parmi 6. La septième combinaison binaire a pour fonction de rediriger la tonalité générée par le µP MN01/Logique vers le HP.

Table de vérité du commutateur analogique MA05/Logique :

BF1 (MA05-9)	**BF2 (MA05-10)**	**BF3 (MA05-11)**	**Effet**
L	L	L	Niveau audio HP 0 : mis en sourdine (muet)
L	L	H	Niveau audio HP 1 : le moins fort
L	H	L	Niveau audio HP 2
L	H	H	Niveau audio HP 3
H	L	L	Niveau audio HP 4
H	L	H	Niveau audio HP 5
H	H	L	Niveau audio HP 6 : le plus fort
H	H	H	Audio du générateur de tonalité aiguillé vers le HP

C’est aussi MA05/Logique qui permet l’ouverture du HP lorsqu’un signal est reçu. Le µP MN01/Logique est informé de la détection d’une porteuse lorsque le signal DP, en provenance de MA02-7/HF, passe au niveau haut. C’est à ce moment-là que MN01/logique pilote MA05/Logique pour diffuser le signal démodulé dans HP avec le niveau audio défini par l’utilisateur.
Le seuil du squelch, lui, est défini en dur par le réglage de la résistance variable R29/HF (proche de MA01/HF)

5.2 Aiguillage audio RX MA04/Logique

Le signal démodulé, avant réglage du volume et amplification, est appliqué simultanément sur les entrées 1 et 4 de MN04/Logique.

- Le signal présent sur MA04-1/Logique est commuté par BBF1 (Blocage BF1 en provenance de MN13-17/Logique) sur MA04-13/Logique. En sortie, sur MA04-2/Logique, ce signal audio est filtré et envoyé sur la BF RX de l’organe d’exploitation (signal BFREC sur le schéma).
- Le signal présent sur MA04/4/Logique est commuté par BBF2 (Blocage BF2 en provenance de MN13-18/Logique) sur MA04-5/Logique. En sortie, sur MA04-3/Logique, ce signal audio est filtré et envoyé sur la BF RX ligne téléphonique (signal BFRXLT sur le schéma).

Les signaux à émettre sont sélectionnés en fonction de la source : microphone ou ligne téléphonique :

- Le signal BF Emission Ligne Téléphonique (BFELT) présent sur MA04-11/Logique est commuté par BBF3 (Blocage BF3 en provenance de MN13-19/Logique) sur MA04-12/Logique. En sortie, sur MA04-10/Logique, ce signal audio est envoyé sur l’ampli à CAG MA03-4/Logique.
- Le signal BF micro de l’organe d’exploitation (EBFE) présent sur MA04-8/Logique est commuté par BLM (BLocage Microphone en provenance de MN13-4/Logique) sur MA04-6/Logique. En sortie, sur MA04-9/Logique, ce signal audio est envoyé sur l’ampli à CAG MA03-4/Logique.

Ces deux derniers signaux sont appliqués sur MA03-4/Logique par l'intermédiaire de R72 qui permet de définir l'excursion maximale.

Signal de commande (broches 5, 6, 12, 13)	Signal en entrée	Signal en sortie
L	X	Hi Z
H	L	L
H	H	H

5.3 Codeur/Décodeur 5-tons

Le composant utilisé pour le codage et décodage 5-tons est un microcontrôleur de la famille 8049, dont le logiciel embarqué est programmé lors de la fabrication du composant. Cette technique appelée Mask ROM empêche toute relecture du code par les méthodes conventionnelles et accessibles aux électroniciens lambda. La référence constructeur du composant programmé, présent sur tous les postes dont je dispose, est **TP8049AH 7680**. Ceci étant dit, la documentation de personnalisation DIGICOM V3.2 évoque deux références de microcontrôleurs, selon le format 5-tons utilisé :

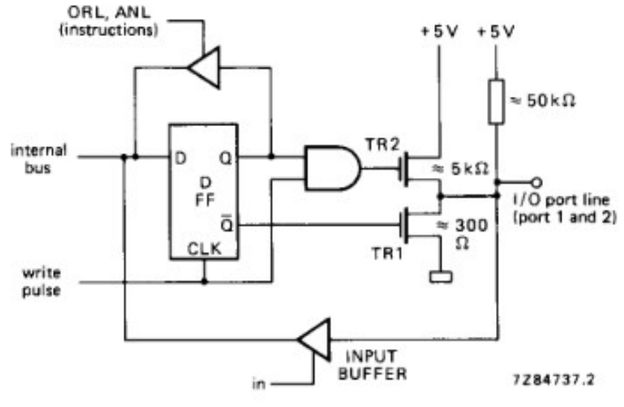
- Un microcontrôleur capable de gérer le CCIR et ZVEI2 ;
- Un microcontrôleur capable de gérer le ZVEI1 et ZVEI1.

MN07/Logique est l'esclave du processeur MN01/Logique.

Le bus de communication s'articule autour des signaux suivants :
ACKM = ACK maître (MN01/Logique) ;
ACKE = ACK esclave (MN07/Logique) ;
DATA = Voie série bidirectionnelle ;
RSTMP2 = Entrée reset de MN07/Logique (ReSeT MicroProcesseur 2).
À l'état de repos, tous ces signaux sont à l'état haut.

Avant de détailler le protocole, il faut noter ceci concernant le signal bidirectionnel DATA :

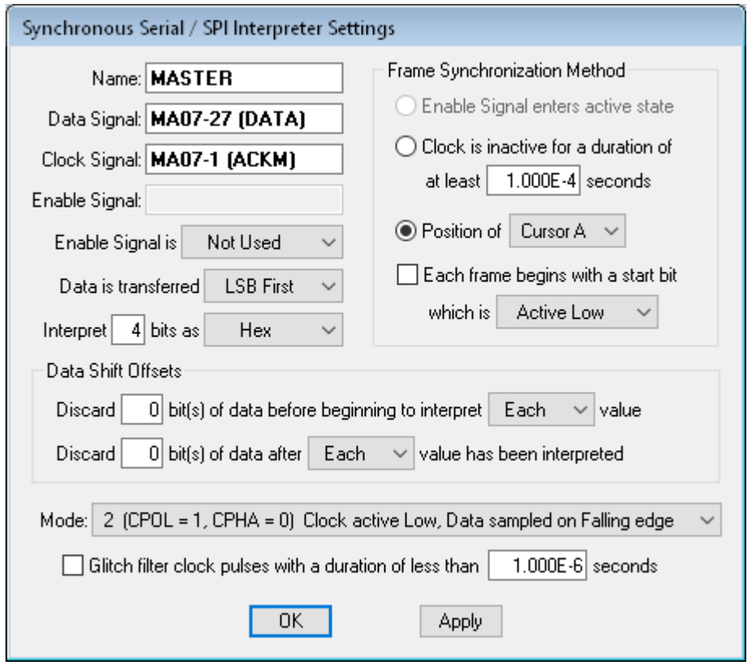
- Côté maître, ce signal est relié à la broche 4 du microcontrôleur 8031AH, correspondant au port 1 bit 3, qui est de type « collecteur ouvert » avec une résistance interne de tirage au niveau haut ;
- Côté esclave, ce signal est relié à la broche 27 du microprocesseur 8049, correspondant au port 1 bit 0 (LSB) qui est bidirectionnel mais de type « Push-Pull » :



Source : documentation technique du MAB8049H

- Un état où le maître force DATA à 0, alors que l'esclave le force à 1, serait destructeur pour l'électronique interne des deux composants.

L'interprétation du dialogue peut être effectuée avec le paramétrage de décodeur suivant :



Le débit observé est de l'ordre de 50kbps.

5.3.1 Protocole de dialogue utilisé pour une transaction

Dialogue Maître → Esclave

1. Le maître effectue une réinitialisation de l'esclave en générant une impulsion à 0V pendant 10µs
   1.1. Cette durée est largement supérieure au délai minimal pour effectuer un reset d'un µC 8049 ;
   1.2. Cette action permet de s'assurer que, quelles que soient les conditions, l'esclave libère le signal DATA en paramétrant son port 1, bit 0, en entrée.
2. Le maître fixe l'état du signal DATA selon le bit qu'il s'apprête à transmettre (LSB en premier) ;
3. Le maître initie le début de la transaction en positionnant son signal ACKM à 0 ;
   3.1. Le front descendant d'ACKM sert à valider la valeur du bit transmis à l'esclave.
4. L'esclave acquitte ce changement d'état en passant à son tour son ACKE à 0 ;
5. Le maître change l'état de son signal ACKM à 1 ;
6. L'esclave change l'état de son signal ACKE à 1 ;
7. Les étapes 2 à 6 sont répétées tant que le maître doit transmettre des données : toujours une suite de deux quartets (commande / valeur?).
8. Chaque nouvelle émission de couple de quartets par le maître débute à partir de l'étape 1.

La commande autorisant l'esclave à indiquer périodiquement le résultat de son analyse de fréquence est 0x20.

Dialogue Esclave → Maître

L'esclave ne prend la main sur le signal DATA qu'après y avoir été autorisé par le maître.

1 L'esclave fixe la valeur de DATA (LSB en premier) en même temps qu'il initie la transaction en positionnant son signal ACKE à 0 ;
2 Le maître acquitte ce changement d'état en passant à son tour son ACKM à 0 ;
  2.1 On observe un temps de réponse du maître au premier bit reçu relativement long comparé à la durée de transmission des bits suivants. Cela s'explique par les nombreuses tâches qu'exécute en parallèle le maître.
3 L'esclave change l'état de son signal ACKE à 1 ;
4 Le maître change l'état de son signal ACKM à 1 ;
5 Les étapes 1 à 4 sont répétées tant que l'esclave n'a pas terminé de transmettre son quartet.

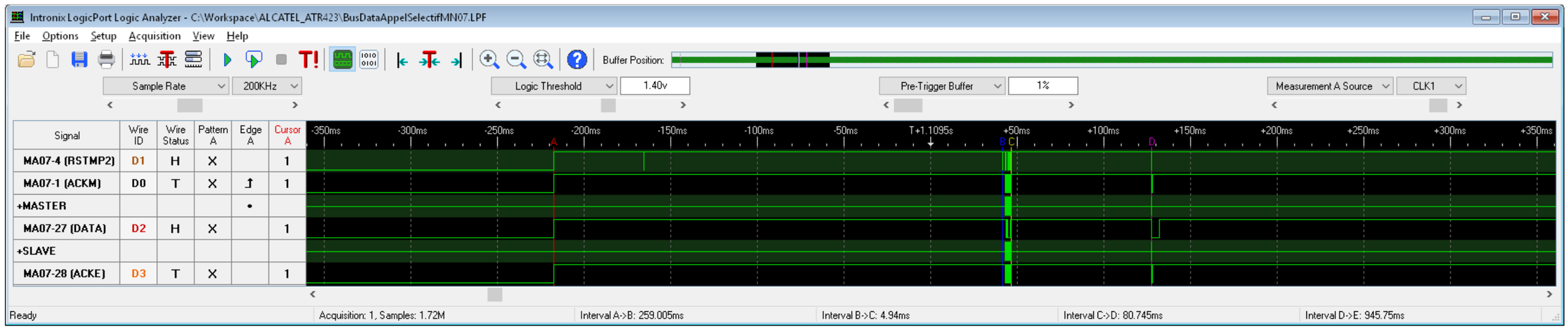
Le maître doit soit :
- Gérer la réception par polling, et donc détecter avec suffisamment de retard le front descendant sur ACKE pour ne pas décoder l'état de DATA qui change en même temps qu'ACKE ;
- Gérer la lecteur par interruption en ajoutant un léger délai avant de lire l'état logique de DATA, afin d'éviter une erreur en cas de désynchronisation ente ACKE et DATA côté esclave).

5.3.2 Chronogrammes

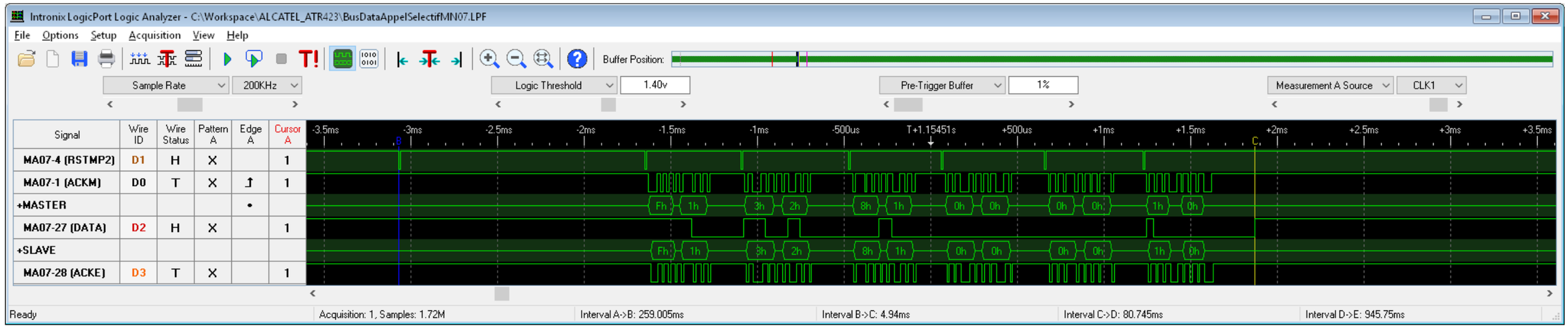
Lors de cette étude du protocole, le poste était configuré pour le standard 5-tons CCIR.

Initialisation du codeur/décodeur 5-tond MN07/Logique

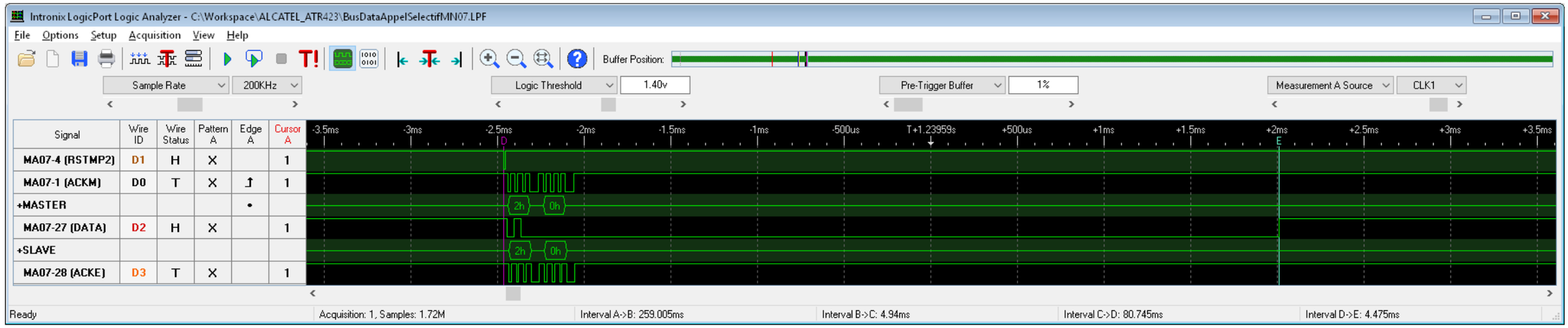
Au démarrage du poste, MN01/Logique communique avec MN07/logique. Pour définir la norme 5-tons ? :



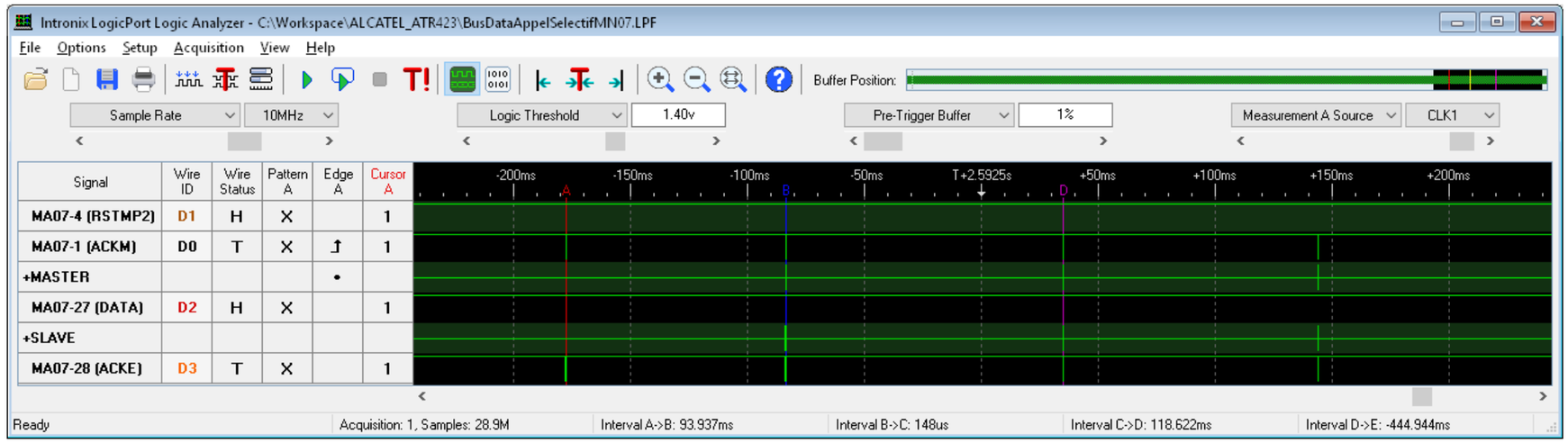
Zoom sur la première séquence de données (entre les curseurs B et C) :



Zoom sur la seconde séquence de données (entre les curseurs D et E) :



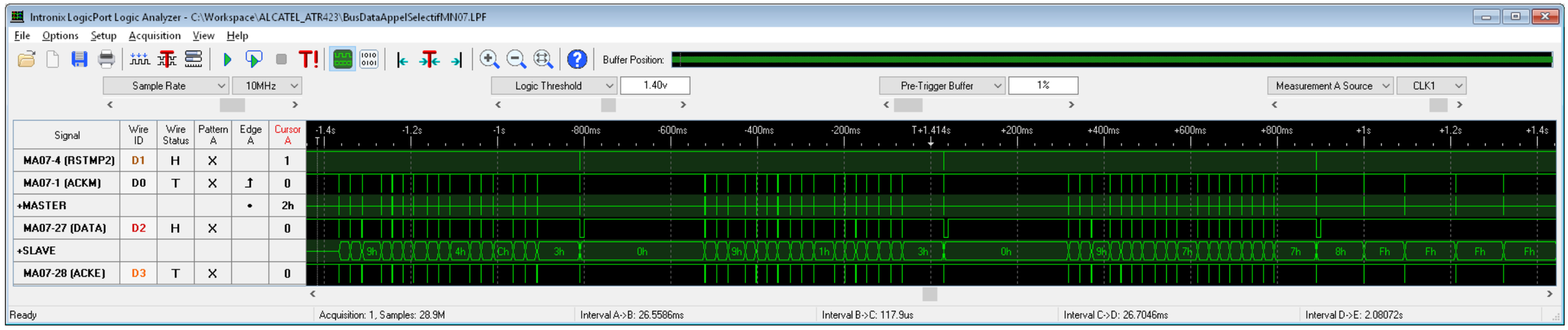
À l'état de repos, MN07/Logique transmet à intervalles quasi réguliers le contenu de son buffer de décodage, soit "F" :



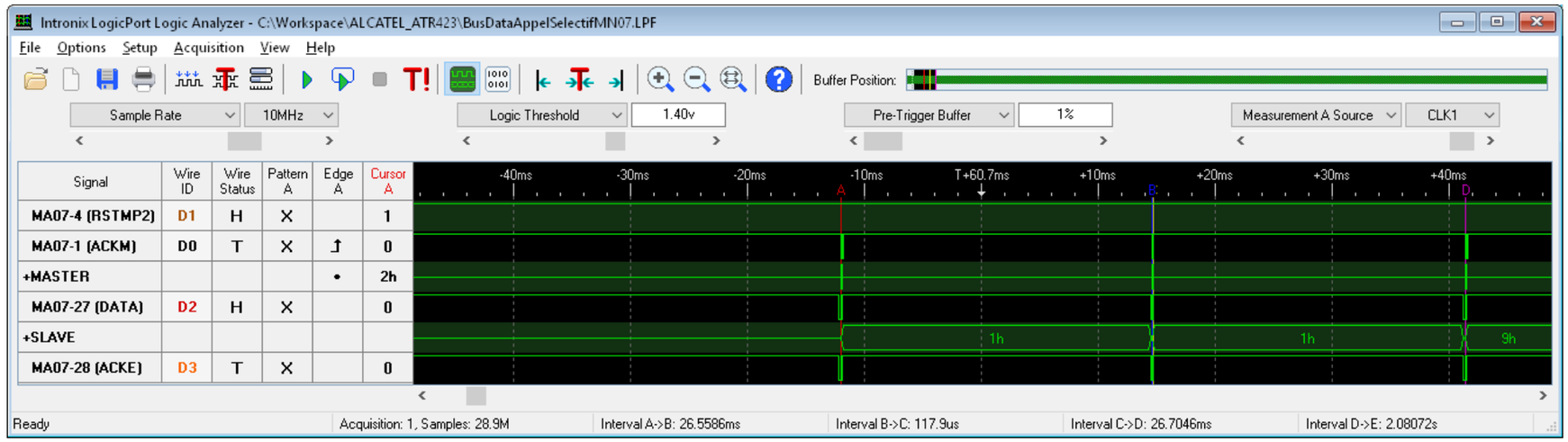
Dans cet exemple, le premier intervalle A->B est de 94ms, puis C->D de 119ms.

Réception de séquences 5-tons

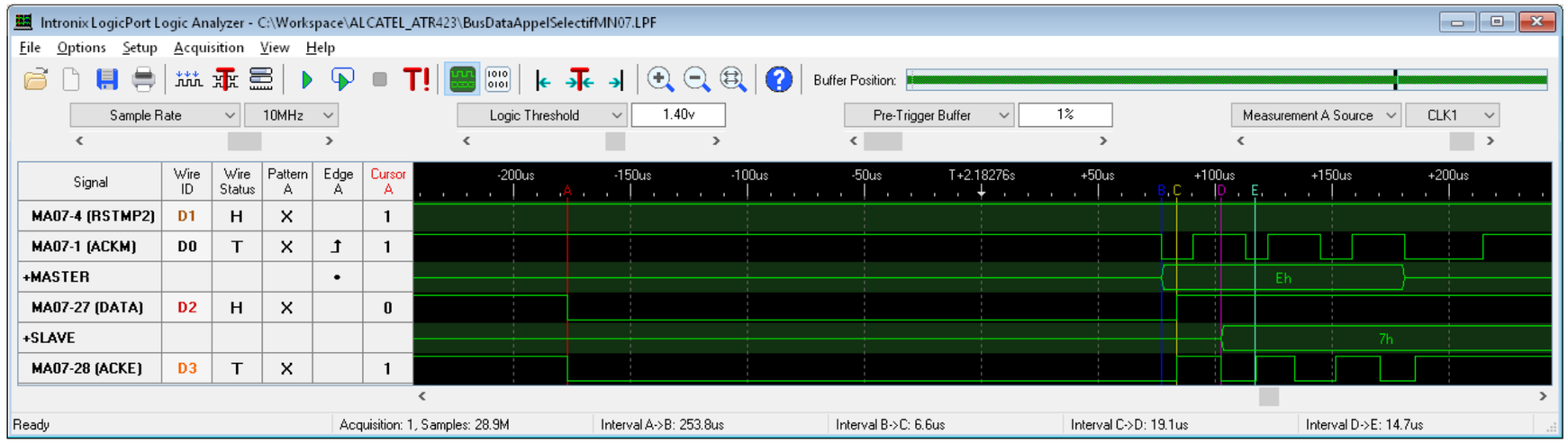
Vue générale du dialogue, lors d'une réception complète de 3 séquences 5-tons suivies de l'état de repos de MN07 :



Pendant le décodage de tonalités, l'intervalle entre chaque transmission de données passe à 26ms environs :

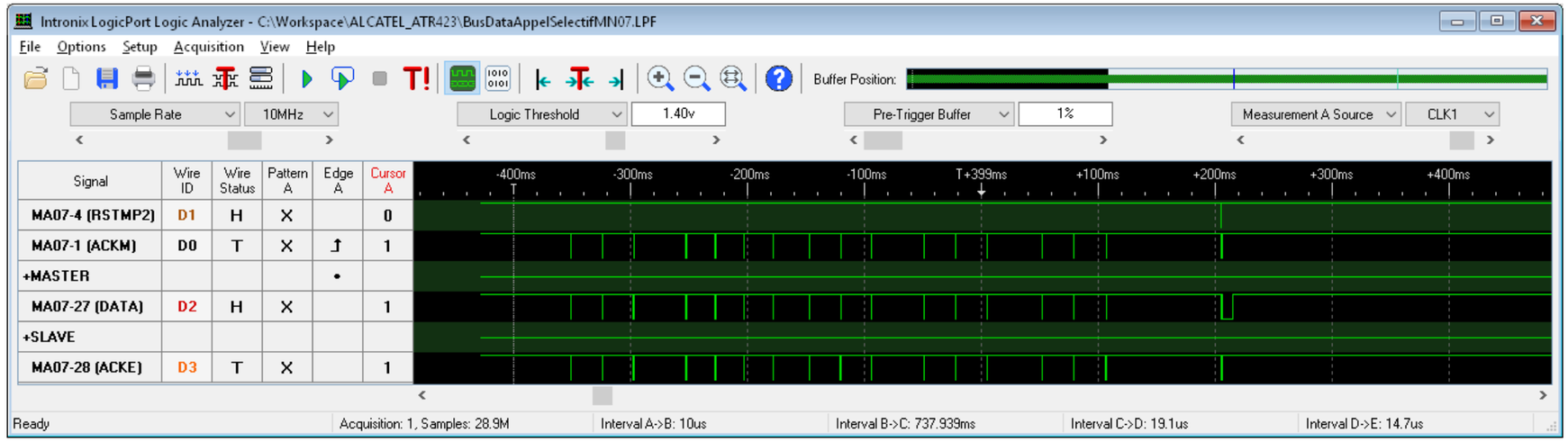


Ici l'esclave indique qu'il a reçu une tonalité correspondant au chiffre 7 par exemple (interpréteur "SLAVE") :

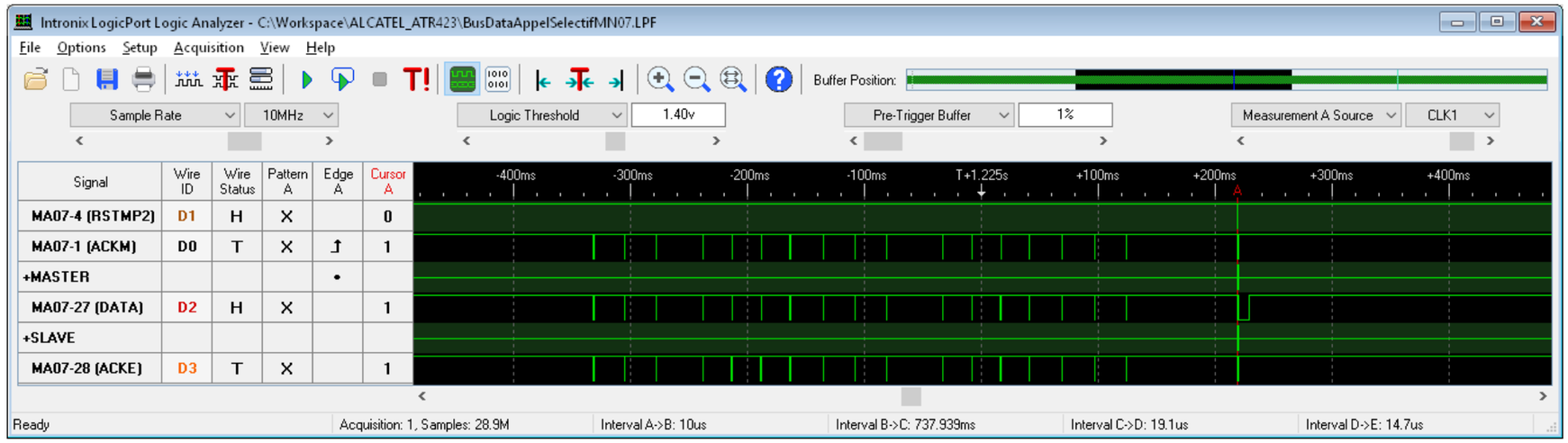


Il se peut qu'il y ait un loupé dans le décodage, l'esclave n'envoie alors rien. On peut donc retrouver un nombre de quartets différent lors du décodage d'une séquence 5-tons :

Ici 16 quartets transmis :



Et ici 17 quartets :

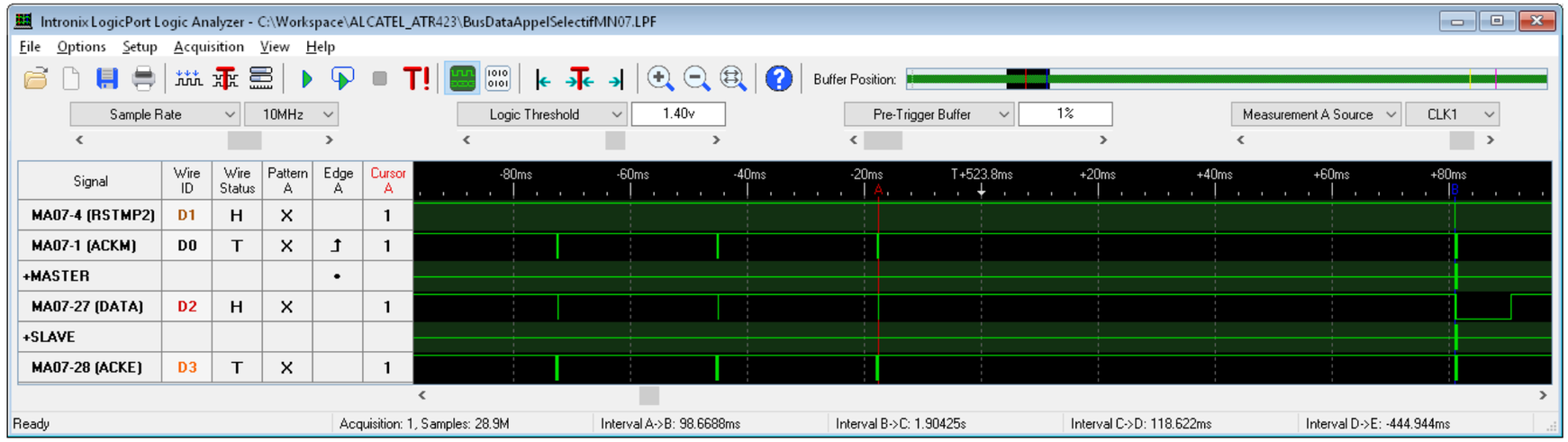


Le nombre de quartets dépasse largement le nombre de tonalités contenues dans la séquence 5-tons, puisque MN07/Logique envoie régulièrement la valeur hexa de la tonalité décodée. On détecte la tonalité suivante quand la valeur décodée est différente de la précédente,avec au moins deux décodages identiques successifs.
L'atout de ces envois réguliers est la gestion d'erreurs de décodage, car on peut ainsi :

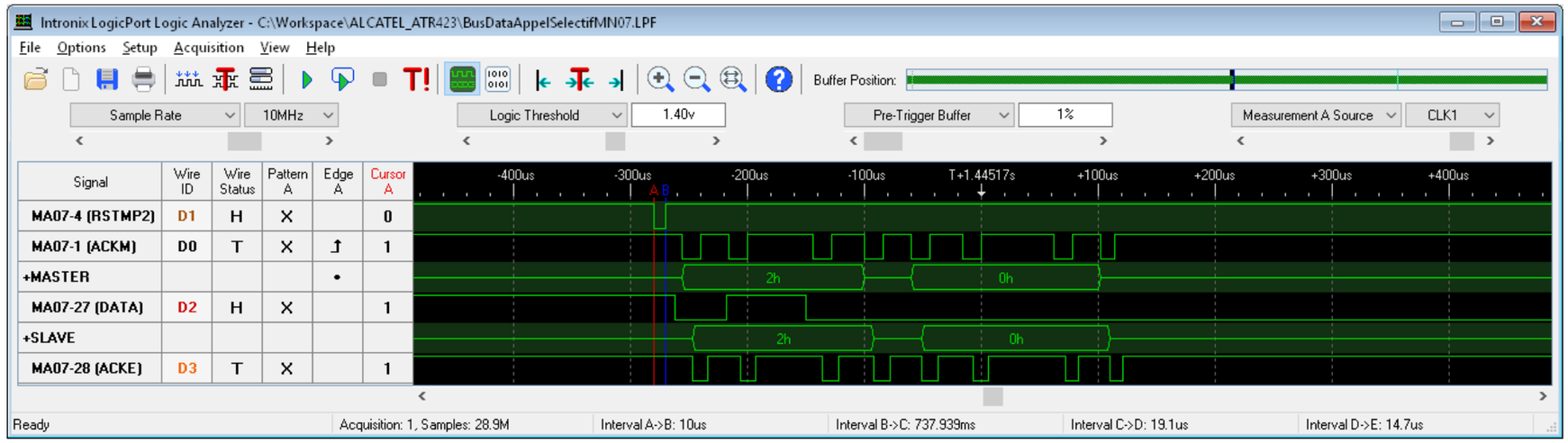
- Considérer qu'une tonalité n'a pas pu être décodée correctement quand on n'a pas 2 fois la même valeur transmise par MN07/Logique ;
- Stocker chaque valeur décodée transmise par MN07/Logique dans une liste et effectuer une gestion d'erreur par détection des décodages parasites dont la valeur n'apparaît qu'une fois.

À la fin du décodage, au bout de 100ms d'inactivité sur le bus de données de la part de MN07/Logique, MN01/Logique force le signal RSTMP2 à 0 pendant 10µs pour redémarrer MN07/Logique.

Timeout de 100ms :



Reset de 10µs :

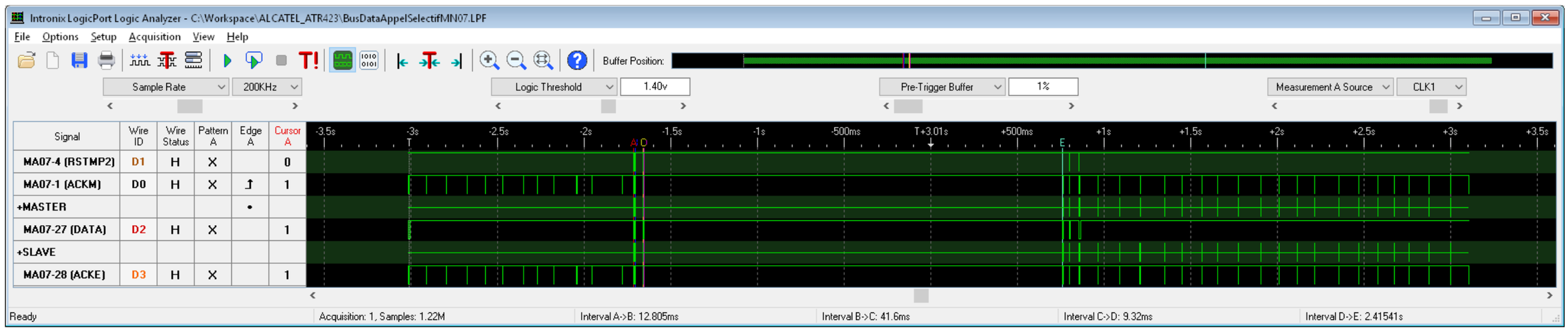


MN01/Logique reparamètre MN07/Logique avec la valeur 20 (réception) et MN07/Logique reprend les envois périodiques du contenu de son buffer.

5.3.3 Émission de séquences 5-tons

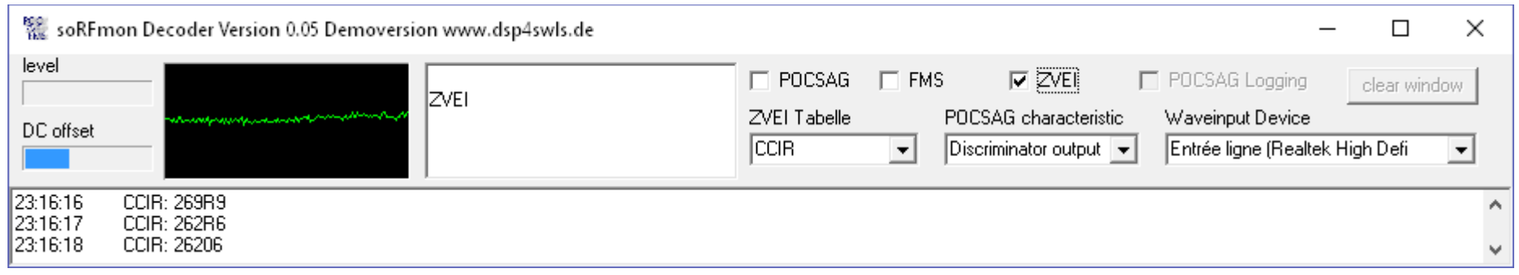
La BF « appel sélectif » générée par MN07/Logique est mélangé à la BF à émettre sur MA03-7/Logique. Les signaux BFELT et EBFE doivent donc impérativement être laissés en haute impédance en sortie de MA04/Logique afin de ne pas interférer avec le signal d'appel sélectif lors de son émission.

Vue d'ensemble de la communication lors de l'utilisation de MN07/Logique pour l'émission :

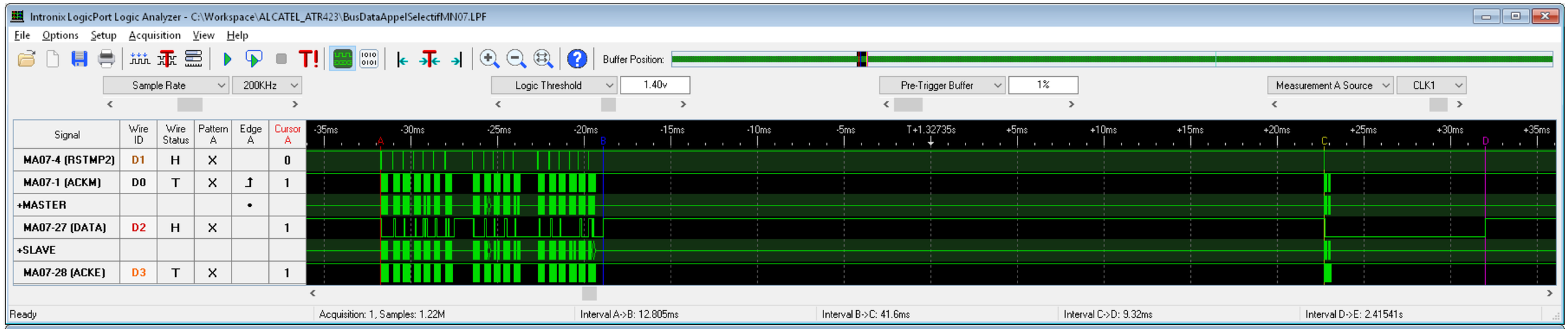


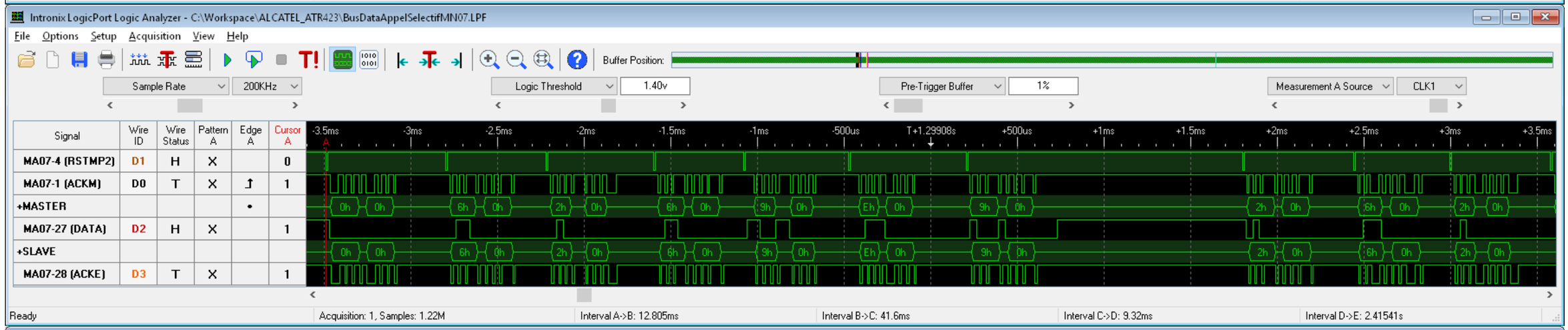
MN07/Logique est à l'état de repos avant le curseur A, puis il est configuré pour émettre les séquences 5-tons entre les curseurs A et D. La confirmation de fin d'émission apparaît au curseur E.
Détail de la configuration entre les curseurs A et D :

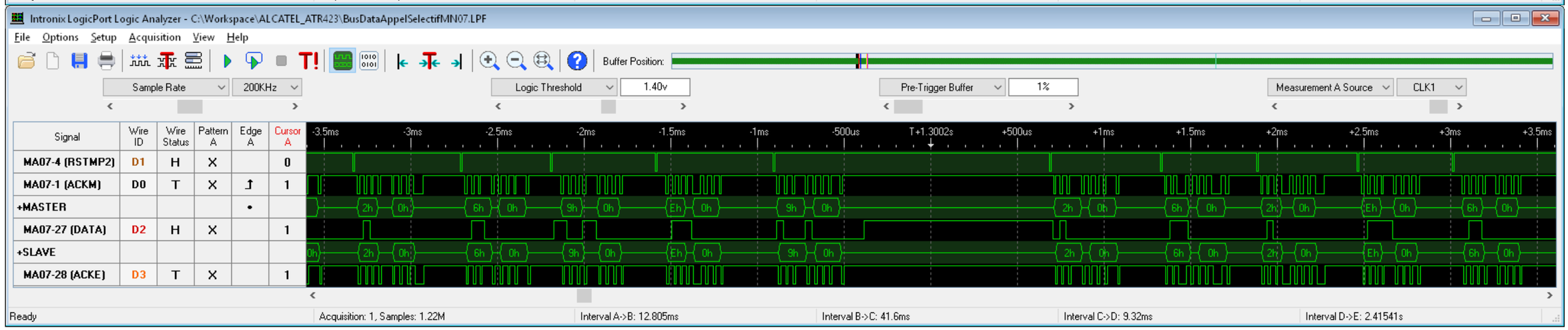
Les codes à transmettre sont, dans l'ordre :

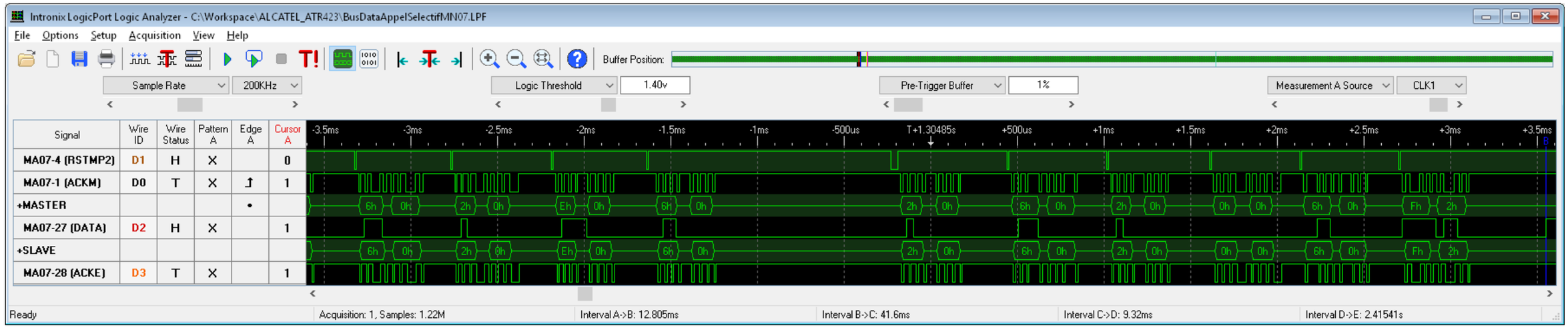


Le « R » inclus dans le décodage ci-dessus représente le caractère « E » utilisé pour la répétition dans le standard CCIR.


Intronix LogicPort Logic Analyzer - C:\Workspace\ALCATEL_ATR423\BusDataAppelSelectifMN07.LPF
File Options Setup Acquisition View Help
Buffer Position:
Sample Rate 200KHz
Logic Threshold 1.40v
Pre-Trigger Buffer 1%
Measurement A Source CLK1
Signal Wire ID Wire Status Pattern A Edge A Cursor A
MA07-4 (RSTMP2) D1 H X 0
MA07-1 (ACKM) D0 T X 1
+MASTER
MA07-27 (DATA) D2 H X 1
+SLAVE
MA07-28 (ACKE) D3 T X 1
-35ms -30ms -25ms -20ms -15ms -10ms -5ms T+1.32735s +5ms +10ms +15ms +20ms +25ms +30ms +35ms
A B C D
Ready
Acquisition: 1, Samples: 1.22M
Interval A->B: 12.805ms
Interval B->C: 41.6ms
Interval C->D: 9.32ms
Interval D->E: 2.41541s

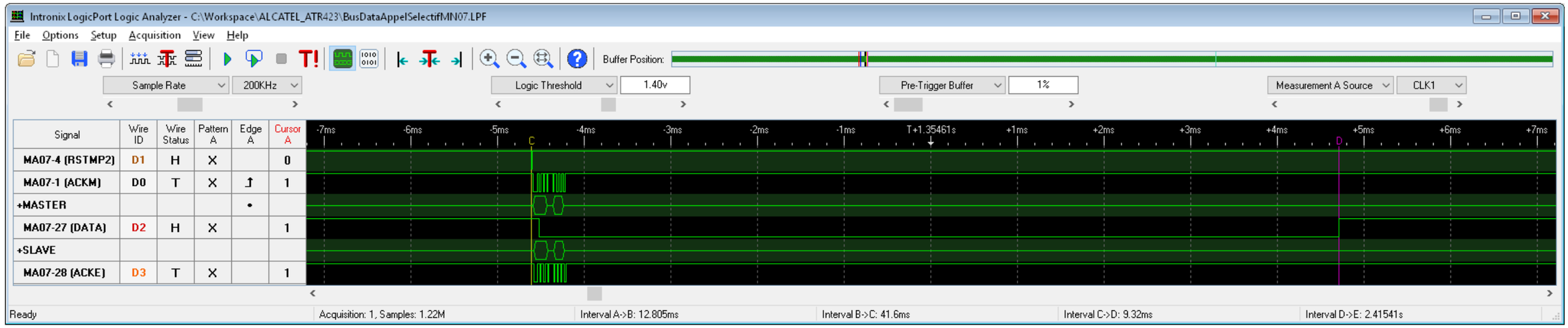

Intronix LogicPort Logic Analyzer - C:\Workspace\ALCATEL_ATR423\BusDataAppelSelectifMN07.LPF
File Options Setup Acquisition View Help
Buffer Position:
Sample Rate 200KHz
Logic Threshold 1.40v
Pre-Trigger Buffer 1%
Measurement A Source CLK1
Signal Wire ID Wire Status Pattern A Edge A Cursor A
MA07-4 (RSTMP2) D1 H X 0
MA07-1 (ACKM) D0 T X 1
+MASTER
MA07-27 (DATA) D2 H X 1
+SLAVE
MA07-28 (ACKE) D3 T X 1
-3.5ms -3ms -2.5ms -2ms -1.5ms -1ms -500us T+1.29908s +500us +1ms +1.5ms +2ms +2.5ms +3ms +3.5ms
A
0h 0h 6h 0h 2h 0h 6h 0h 9h 0h Eh 0h 9h 0h 2h 0h 6h 0h 2h 0h
Ready
Acquisition: 1, Samples: 1.22M
Interval A->B: 12.805ms
Interval B->C: 41.6ms
Interval C->D: 9.32ms
Interval D->E: 2.41541s

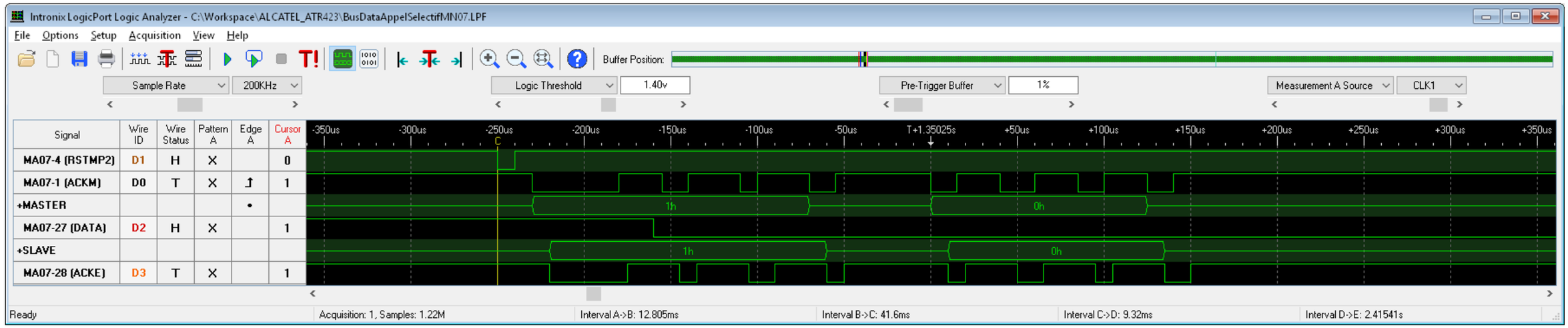

Intronix LogicPort Logic Analyzer - C:\Workspace\ALCATEL_ATR423\BusDataAppelSelectifMN07.LPF
File Options Setup Acquisition View Help
Buffer Position:
Sample Rate 200KHz
Logic Threshold 1.40v
Pre-Trigger Buffer 1%
Measurement A Source CLK1
Signal Wire ID Wire Status Pattern A Edge A Cursor A
MA07-4 (RSTMP2) D1 H X 0
MA07-1 (ACKM) D0 T X 1
+MASTER
MA07-27 (DATA) D2 H X 1
+SLAVE
MA07-28 (ACKE) D3 T X 1
-3.5ms -3ms -2.5ms -2ms -1.5ms -1ms -500us T+1.3002s +500us +1ms +1.5ms +2ms +2.5ms +3ms +3.5ms
0h 2h 0h 6h 0h 9h 0h Eh 0h 9h 0h 2h 0h 6h 0h 2h 0h Eh 0h 6h 0h
Ready
Acquisition: 1, Samples: 1.22M
Interval A->B: 12.805ms
Interval B->C: 41.6ms
Interval C->D: 9.32ms
Interval D->E: 2.41541s



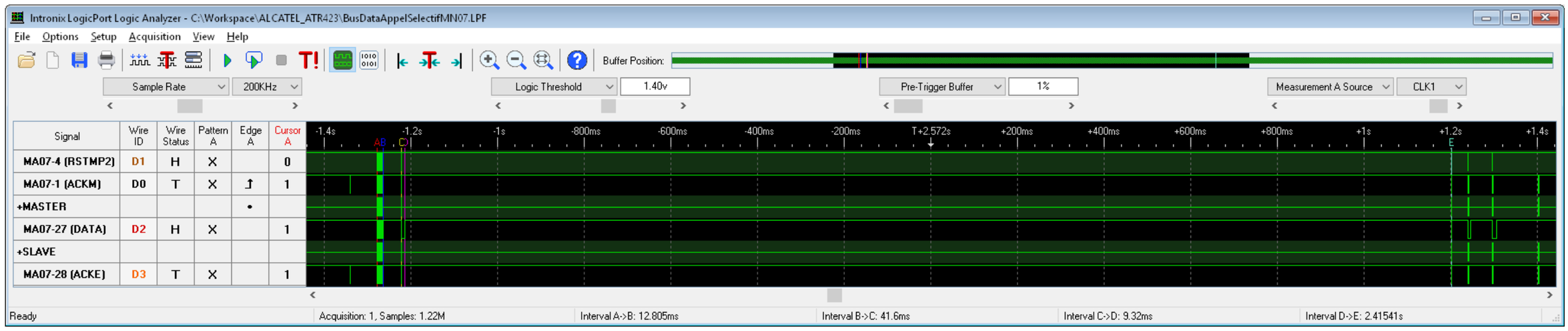
Soit pour résumer :
00h 60h 20h 60h 90h E0h 90h 20h 60h 20h E0h 60h 20h 60h 20h 00h 60h F2h

S'ensuit un temps d'inactivité de 41,6ms puis la transmission suivante (à partir du curseur C) :

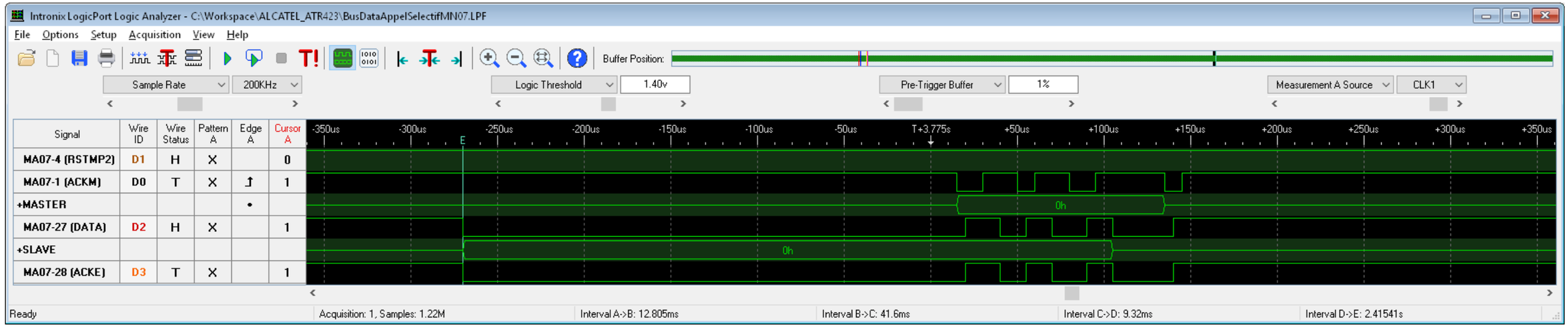




10h valide la transmission des tonalités via l'aiguillage sur la BF TX, pendant 2,4s (entre les curseurs D et E) :

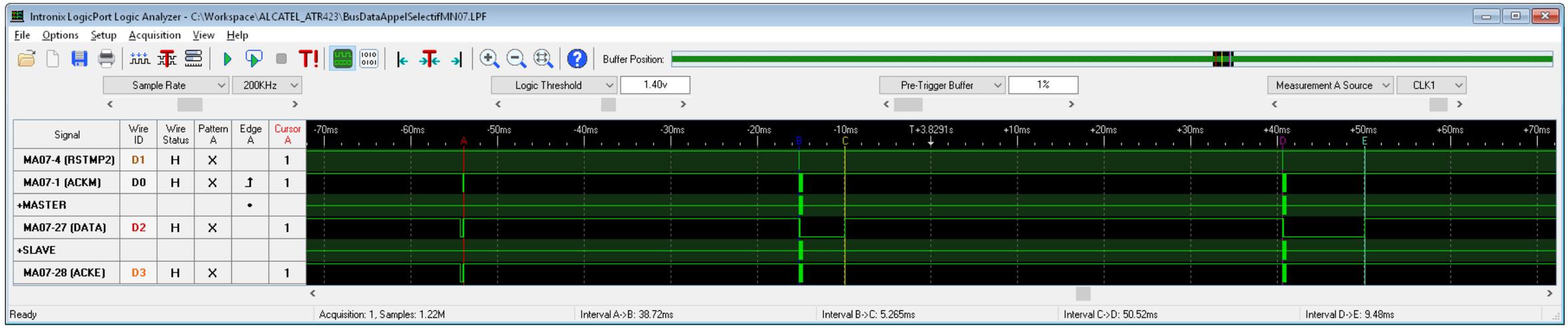


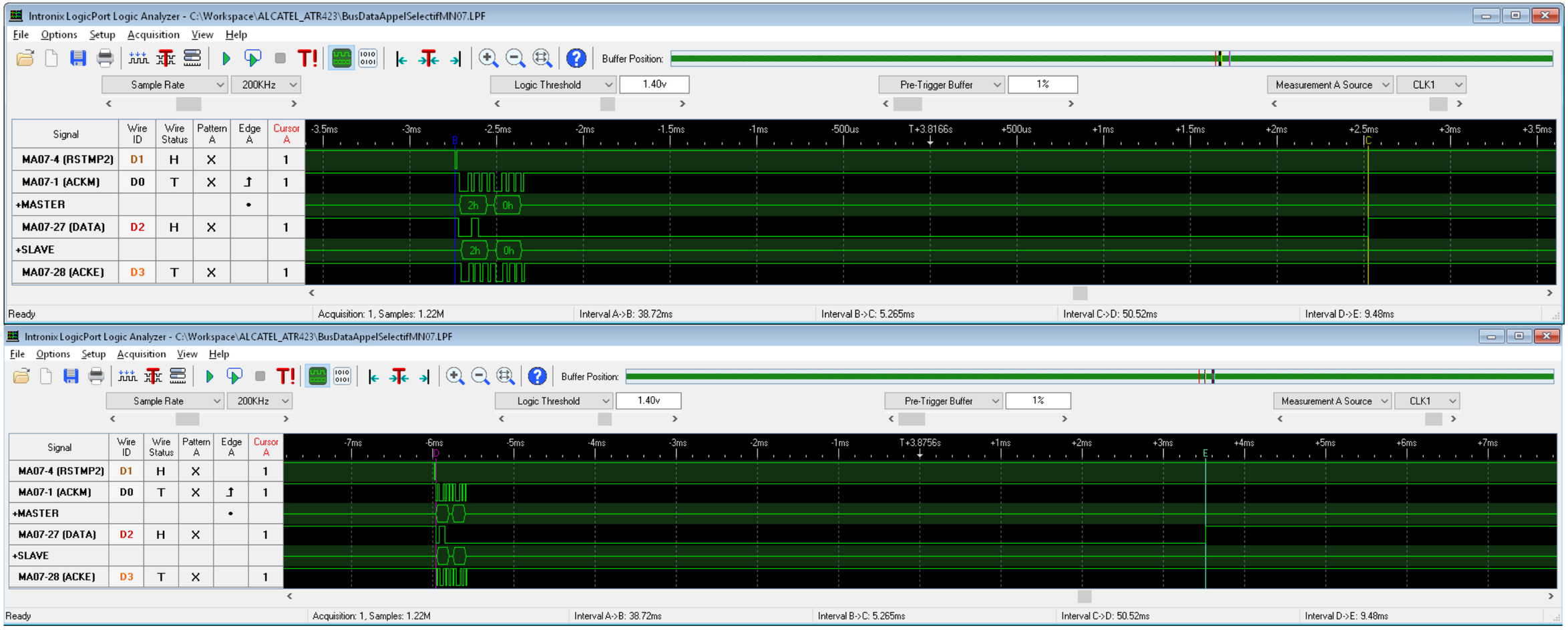
Suivie du quartet 0h, indiquant la fin d'envoi des séquences de tonalités ?:



Les positions des curseurs A à E ont été redéfinies ci-dessous afin de mesurer les temporisations des échanges suivants .

Après la fin d'émission, MN01/Logique attend 39ms (entre les curseurs A et B) et force RSTMP2 à 0, toujours pendant 10ms, puis reparamètre MN07/Logique avec l'octet 20h. 50ms plus tard, MN01/Logique répète cette même séquence de reparamétrage :

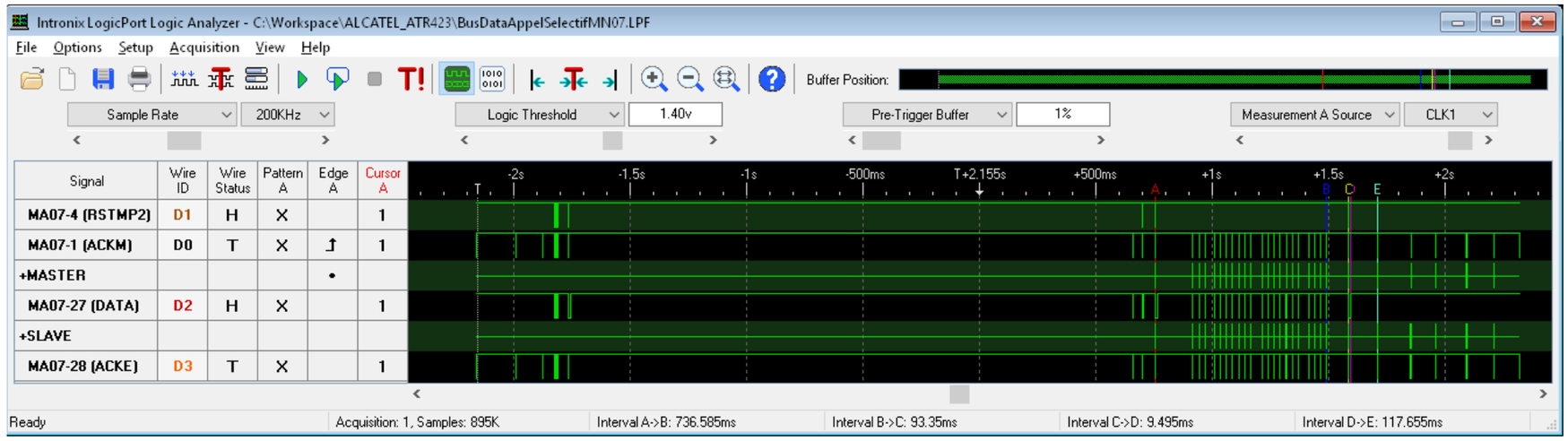




MN07/Logique reprend alors les envois périodiques de l'état de son buffer.
Dans cet exemple, le poste distant n'a pas répondu.

Les positions des curseurs A à E ont été redéfinies ci-dessous afin de mesurer les temporisations des échanges suivants .

Autre exemple, en cas de réponse du poste appelé :
MN07/Logique retourne la séquence reçue entre les curseurs A et B, puis est réinitialisé par MN01/Logique entre les curseurs C et D, avant de renvoyer périodiquement l'état de son buffer à partir du curseur E.



Les tonalités de retour d'appel, émises par le poste appelé (permettant de confirmer la bonne réception de l'appel), ne sont pas décodées par MN07/Logique.

5.3.4 Récapitulatif des commandes maître → esclave

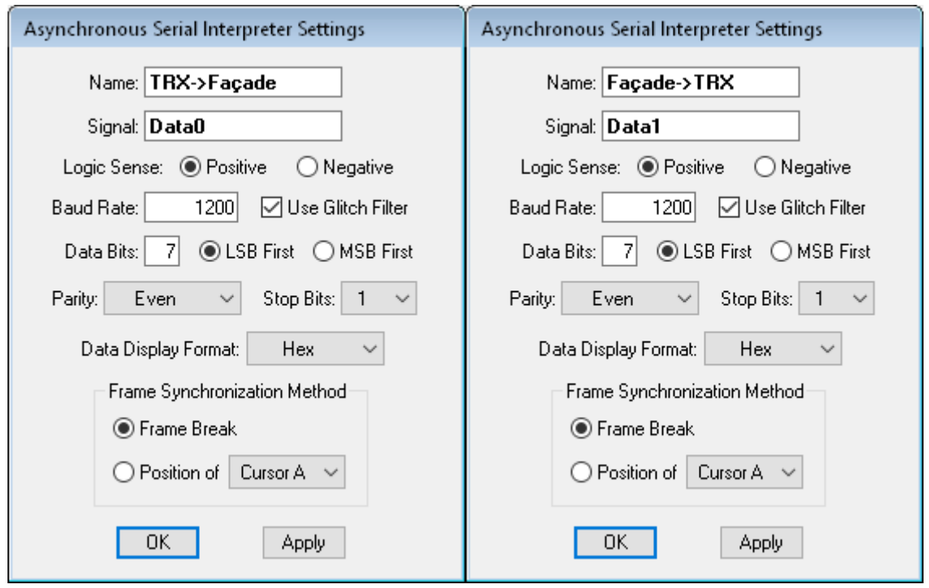
Cette liste est alimentée au fur et à mesure que les commandes sont découvertes par rétro-ingénierie :

- 0x10 : ordre de passage en émission ;
- 0x20 : ordre de passage en réception

5.4 Organe d'exploitation

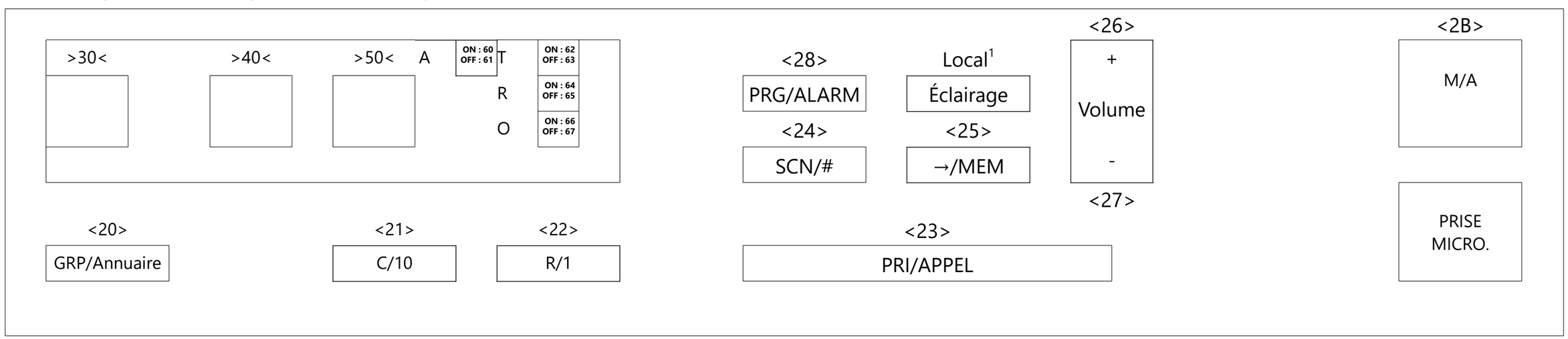
Il ne renferme aucune intelligence, à part la gestion des touches dont les codes et l'état sont transmis par une ligne UART vers le processeur de la radio, ainsi que de l'affichage (fluo + LEDs) reçu du processeur de la radio via une seconde ligne UART.

Le protocole de communication, dans un sens ou dans l'autre, est le suivant :



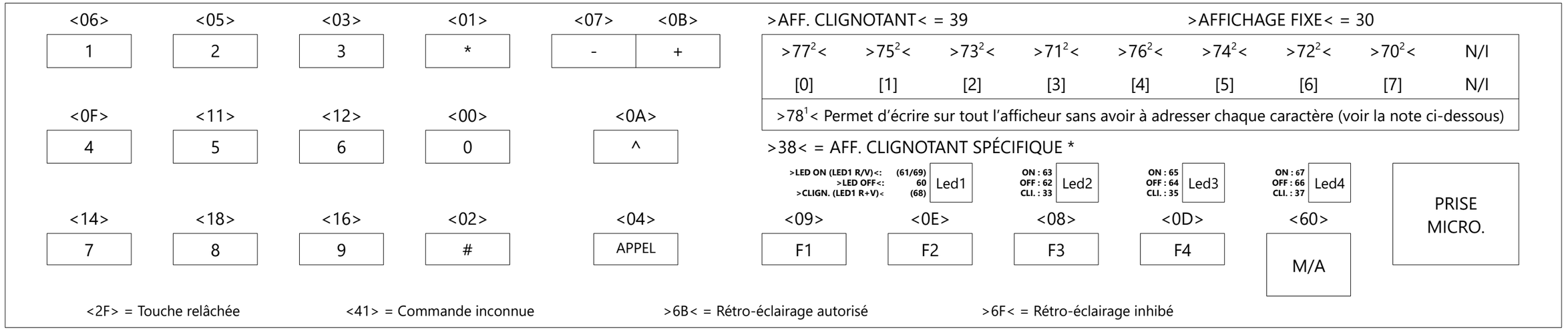
Une pause de 20ms est marquée entre chaque octet transmis du poste vers l'organe d'exploitation. Elle permet de laisser un temps de réponse à l'organe d'exploitation. Ex. : si un octet transmis à l'organe d'exploitation n'est pas correctement reçu, ce dernier répond 41h au poste.

5.4.1 Codage des E/S de l'organe d'exploitation type MINI / SC2 :



Note [1] : La touche n'émet aucune donnée. Elle est utilisée localement par l'organe d'exploitation pour alterner entre luminosité moyenne et élevée des afficheurs et LED.
Si l'organe d'exploitation ne reconnaît pas une donnée qui lui a été transmise, il répond 15.
Au démarrage du poste, si l'afficheur le plus à gauche indique « H », cela signale que l'organe d'exploitation n'a pas pu dialoguer avec la carte logique. Les causes peuvent être multiples : configuration définie pour une autre gamme d'organe d'exploitation, mauvais applicatif, erreur au démarrage de l'applicatif, etc.

5.4.2 Codage des E/S de l'organe d'exploitation type SC20



Note [1] : L'ordre dans lequel sont envoyés les caractères à l'afficheur n'est pas cohérent. Après avoir émis la commande 78, chacun des 8 caractère max. émis par la suite sera placé respectivement à l'emplacement suivant de l'affichage (en partant de la gauche) : 7, 3, 6, 2, 5, 1, 4 et 0. Voir un peu plus loin dans ce document avec la trame de données permettant d'afficher « NI 26;226 » à l'écran.

Note [2]: Lorsque l'envoi du caractère se fait sur une adresse spécifique de l'affichage, entre 70 et 77, seul cet emplacement de l'affichage prend la valeur transmise. Il l'y a pas d'incrémentation automatique du pointeur effectuée par l'organe d'exploitation, contrairement à ce qui est exécuté avec la commande 0x78. Pour une modification partielle de l'affichage, chaque caractère est précédé de l'adresse à laquelle il doit être affiché.

>53< : l'organe d'exploitation répond <33> ?
>6E< : l'organe d'exploitation répond <34> ?

* >38< = affiche les octets transmis juste après 38h de la manière suivante :
  - [0] reste inchangé et se met à clignoter
  - les octets transmis sont affichés à partir de [1]
  - [1] à [3] se mettent à clignoter
  - [4] reste inchangé et ne clignote pas, l'octet transmis à cette position est perdu
  - [5] est remplacé par l'octet transmis et ne clignote pas
  - [6] et [7] sont remplacés par les octets transmis et clignotent
* >31< = affiche les octets transmis juste après 31h de la manière suivante :
  - [0] reste inchangé et se met à clignoter
  - les octets transmis sont affichés à partir de [4]
  - [4] et [5] sont remplacés par les octets transmis et ne clignotent pas
  - [6] et [7] sont remplacés par les octets transmis et se mettent à clignoter
  - [0] reste inchangé et se met à clignoter
  - [1] à [3] sont remplacés par les octets transmis et se mettent à clignoter

5.4.3 Les touches, sens : <UART organe d'exploitation → poste>

Chaque appui sur une touche est signalé sur le bus UART par son identifiant indiqué ci-dessus entre les signes < et >.
Chaque touche relâchée est signalée par l'envoi sur le bus UART de son identifiant suivi par 2Fh.

5.4.4 Les LEDs , sens : >UART poste → organe d'exploitation<

Le pilotage des LEDs se fait en fonction de l'identifiant ON/OFF émis par le poste concernant chaque LED, indiqué ci-dessus entre les signes > et <.

5.4.5 L'affichage fluorescent, sens : >UART poste → organe d'exploitation<

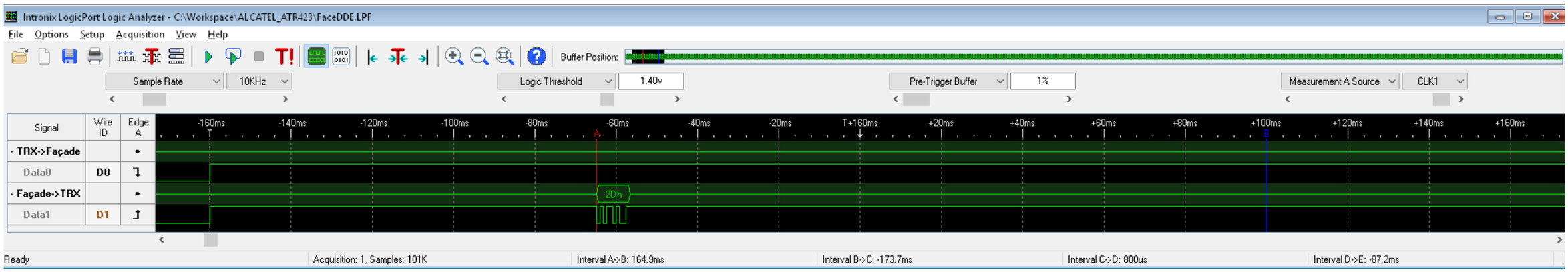
Le dernier caractère de l'afficheur, affiché N/I ci-dessus, n'est pas utilisable car non câblé dans l'organe d'exploitation.
L'affichage du texte se fait soit en ligne entière, soit par caractère :

- Ligne entière : Le poste envoie à l'organe d'exploitation le code 78h suivi des 8 caractères à afficher à la suite, de la position [0] à la position [7].
- Par caractère : Le poste envoie à l'organe d'exploitation le code correspondant à la position sur l'afficheur, (76) pour la position [4] et (71) pour la position [3] par exemple, suivie à chaque fois par le caractère à afficher .

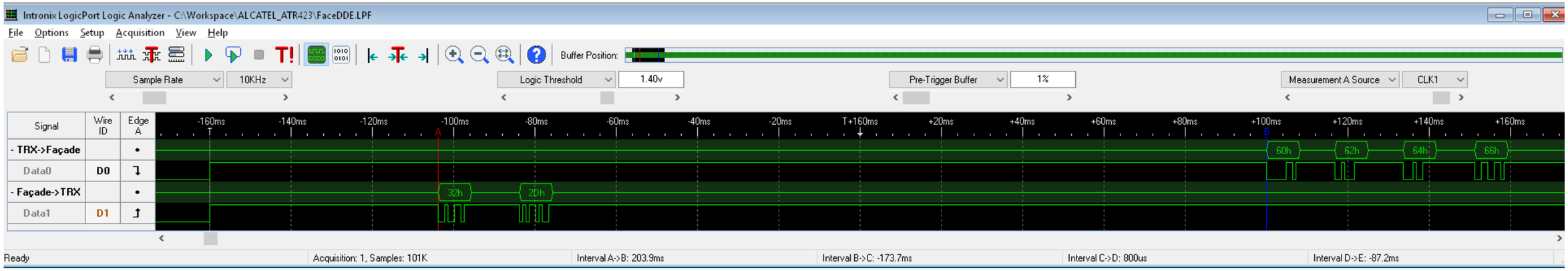
Le clignotement partiel des caractères est réalisé par une suite d'écritures sur l'afficheur, à intervalles réguliers. Le poste envoie à la façade un caractère vide pour faire disparaître le(s) caractère(s), patiente pendant la temporisation du clignotement, puis renvoie le(s) caractère(s) à rendre visible pendant cette phase du clignotement. Le poste envoie >39< pour effectuer un clignotement de l'affichage fluorescent entier, et >30< pour cesser le clignottement.

5.4.6 Mise sous tension du poste

Organe d'exploitation EDF :

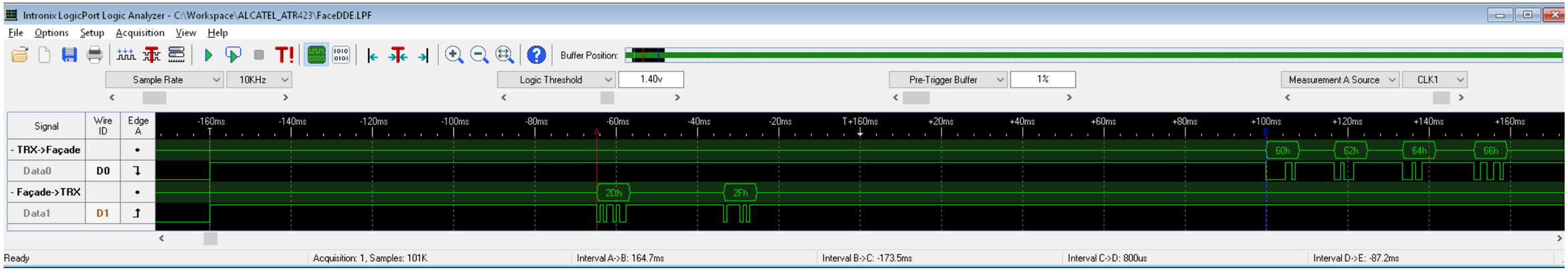


Organe d'exploitation DDE :

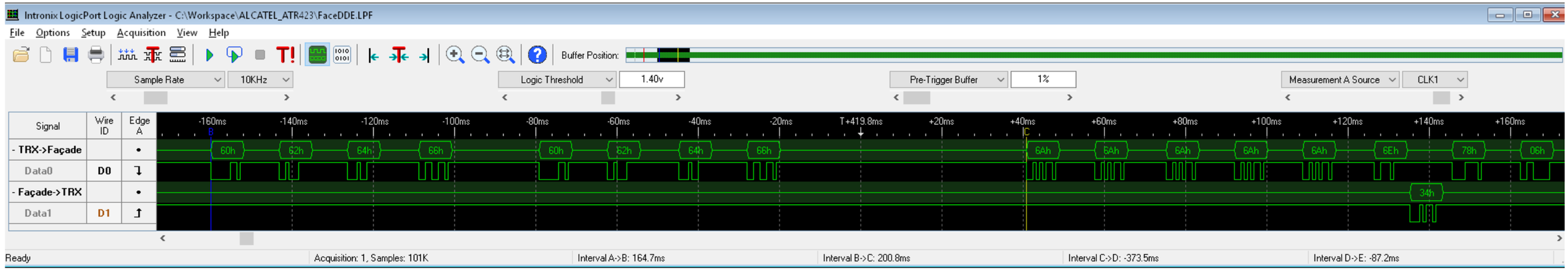


5.4.7 Allumage avec le bouton M/A de l'organe d'exploitation (EDF uniquement)

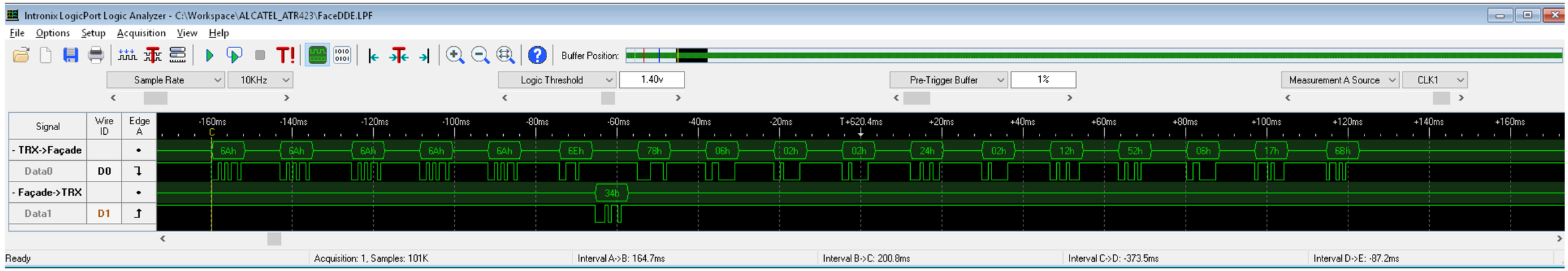
Appui sur le bouton, le code de la touche est remplacé par 2Dh :



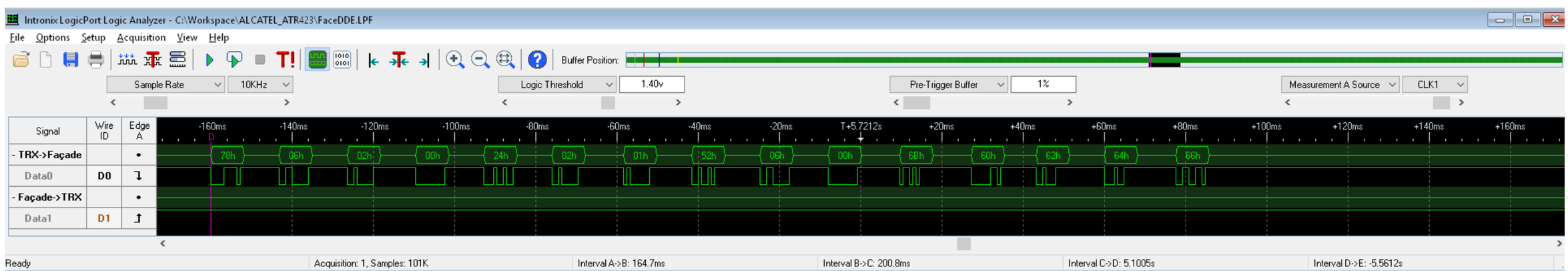
Au bout de 165ms environs, le poste envoie deux fois les identifiants d'extinction des 4 LEDs :



200ms plus tard, le poste envoie 5 fois 6Ah suivi de 6Eh. L'organe d'exploitation acquitte en envoyant à son tour 34h. Le poste lui envoie immédiatement les caractères à afficher « NI 26;226 » :



Cette capture met en évidence l'envoi désordonné des caractères à afficher à l'écran lorsque la commande 0x78 est utilisée. Les données sont envoyées dans cet ordre à l'afficheur : 622 2I;6N
5 secondes plus tard, le poste envoie à nouveau une nouvelle ligne complète à afficher « 01 26,206 » :



Enfin, 20 secondes plus tard, le poste envoie une nouvelle ligne ne contenant qu'un tiret en position [7] et inhibe le rétro-éclairage :

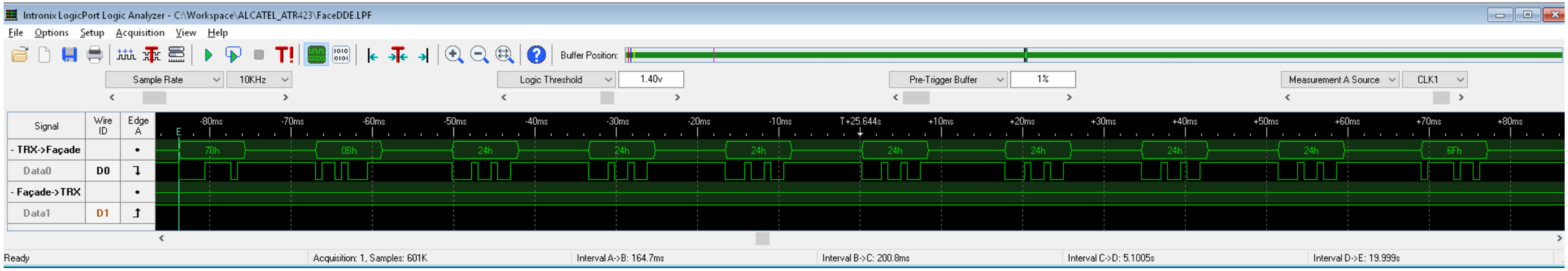


Table de caractères pour les organes d'exploitation type SC20 :

0	00h	6	06h	G	0Ch	I	12h	O	18h	U	1Eh	Espace	24h	<	2Ah			
1	01h	7	07h	D	0Dh	J	13h	P	19h	V	1Fh	B	25h	>	2Bh			
2	02h	8	08h	E	0Eh	K	14h	Q	1Ah	W	20h	Antenne	26h	/	2Ch			.	50h
3	03h	9	09h	r	0Fh	L	15h	R	1Bh	X	21h	F	27h	+	2Dh			,	51h
4	04h	A	0Ah	C	10h	M	16h	S	1Ch	Y	22h	*	28h	[	2Eh			;	52h
5	05h	–	0Bh	H	11h	N	17h	T	1Dh	Z	23h	=	29h	]	2Fh				

Pour effacer le point, la virgule, ou le point virgule, il suffit d'envoyer le caractère sans le précéder du code hexadécimal de ponctuation.

Table de caractères pour les organes d'exploitation type MINI / SC2 :

0	x0	6	x6	≡	xC
1	x1	7	x7	d	xD
2	x2	8	x8	r	xE
3	x3	9	x9	Éteint	xF
4	x4	P	xA		
5	x5	_	xB		

Remplacer x par l'adresse de l'afficheur. De la gauche vers la droite : 3y, 4y et 5y, avec y prenant pour valeur la donnée à afficher.

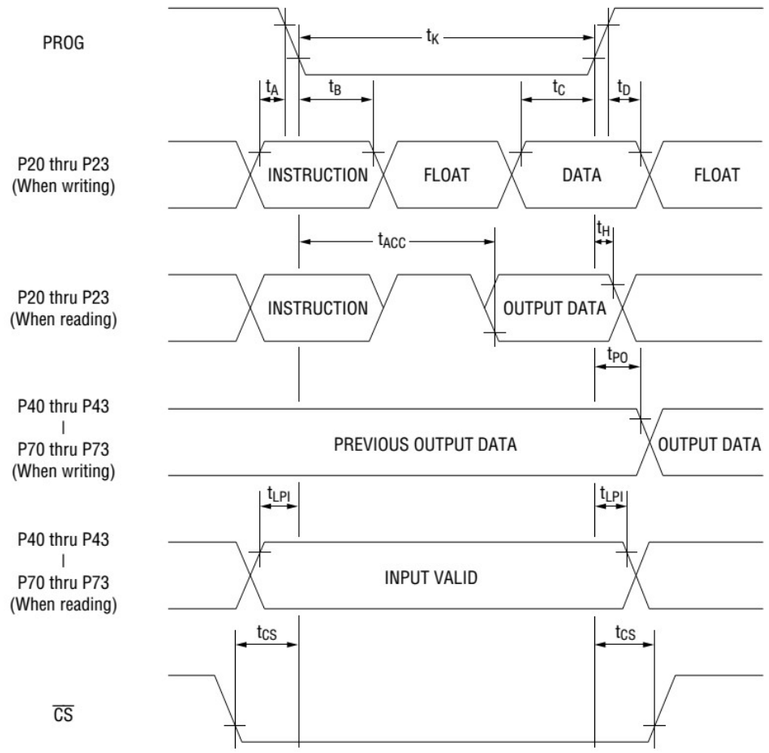
5.5 Les extenseurs de port MN13 et MN14

Les E/S disponibles sur MN01/Logique ne permettent pas d'assurer le pilotage des différents périphériques à elles seules, une grande partie étant déjà dédiée aux bus parallèles d'adresse et de donnée vers les EEPROM et la RAM. MN13/Logique et MN14/Logique, qui possèdent chacun 4 ports bidirectionnels de 4 bits, effectuent donc un aiguillage des signaux appliqués sur les E/S de leurs ports vers un 5e port bidirectionnel dédié à MN01/Logique, en fonction des commandes émises par ce dernier.

Le jeu de commandes est le suivant :

Instruction	Valeur binaire	P23	P22	Port	Valeur binaire	P21	P20
Lecture	0	0	0	Port 4	0	0	0
Écriture	1	0	1	Port 5	1	0	1
"OU" logique	2	1	0	Port 6	2	1	0
"ET" logique	3	1	1	Port 7	3	1	1

Les commandes sont transmises de la manière suivante :



Parameter	Symbol	Conditions	Min.	Max.	Unit
Port Control Setting Time (up to PROG Falling Edge.)	t_A	80pF LOAD	50	—	ns
Port Control Holding Time (up to PROG Falling Edge.)	t_B	20pF LOAD	60	—	ns
Output Data Setting Time	t_C	80pF LOAD	200	—	ns
Output Data Holding Time	t_D	20pF LOAD	20	—	ns
Input Data Holding Time	t_H	20pF LOAD	0	150	ns
PROG Pulse Width	t_K	—	700	—	ns
$\overline{CS}$ Valid Time (before and after PROG)	t_{CS}	—	50	—	ns
Output Data Valid Time (at Ports 4-7)	t_{PO}	100pF LOAD	—	700	ns
Input Data Holding Time (at Ports 4-7)	t_{LP1}	—	100	—	ns
Input Data Holding Time (from PROG Falling Edge)	t_{ACC}	80pF LOAD	—	650	ns

Les changements de direction des ports sont séparés par des périodes où les E/S du Port 2 sont flottantes (FLOAT). **Le respect des temps T_A, T_B, T_C et T_D est donc vital pour l'électronique des E/S de MN01/Logique et MN13/MN14/Logique.**

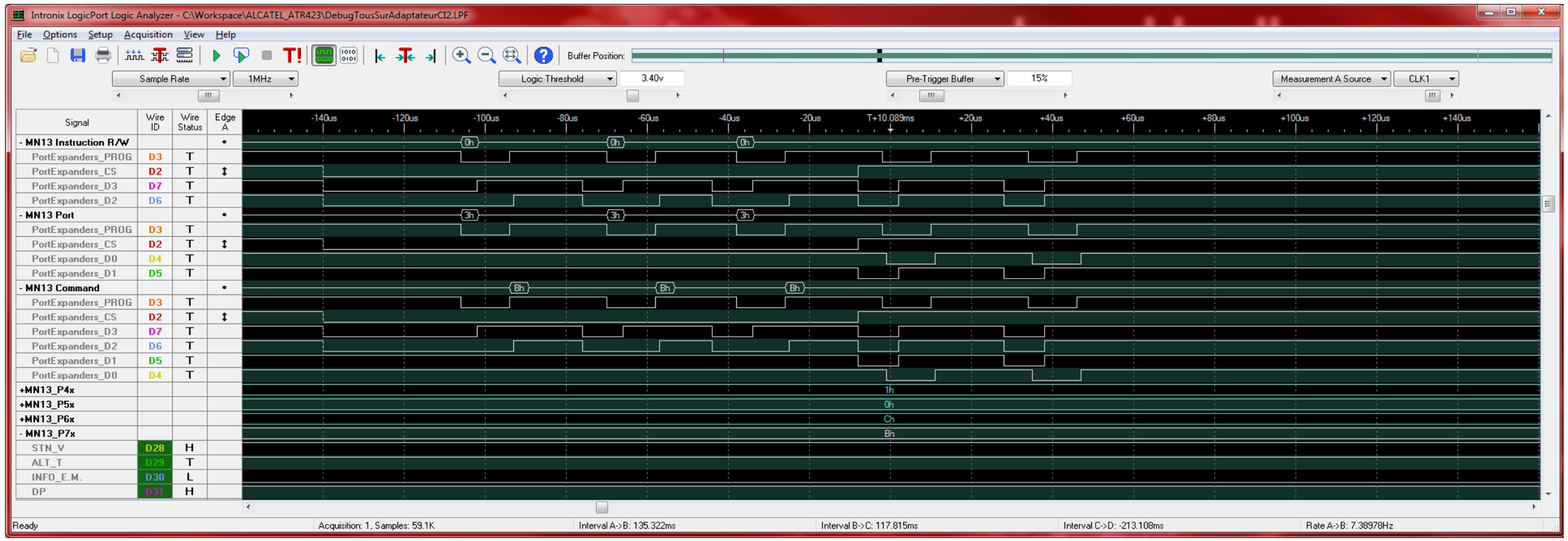
Rappel des E/S sur chaque extenseur de port :

	MN13 – Périphériques et signaux internes				MN14 – E/S accessoires et cartes option			
Bit	Port 4	Port 5	Port 6	Port 7	Port 4	Port 5	Port 6	Port 7
[LSB] 0	OPE [S]	(N/C)	TEST [?]	STN_V [E]	LBA	TCS_DEC	LBB	FX1
1	(N/C)	BF1 [S]	BBF3 [S]	ALT_T [E]	KLX	XEAS	VTCS	FX2
2	BLM [S]	BF2 [S]	BBF2 [S]	INFO EM [E]	RAS-DSR	XURG	XTCS	FX3
[MSB] 3	ENR [S]	BF3 [S]	BBF1 [S]	DP [E]	PAE	ACQ	ERTCS	FX4

Dans l'exemple suivant, MN01/Logique effectue vers MN13/Logique :

- 3 lectures du Port 7 ;
  → Lecture de Bh : DP = 1, INFO EM = 0, ALT_T = 1 et STN_V = 1 ⇒ 1011b = Bh
- un « OU » sur le Port 6 avec la valeur 8h ;
  →Mise à 1 de BBF1
- un « OU » sur le Port 6 avec la valeur 4h ;
  →Mise à 1 de BBF2
- une écriture sur le Port 5 avec la valeur Ch ;
  →Mise à 1 de BF3 et BF2, mise à 0 de BF1 ⇒ 1100b = Ch

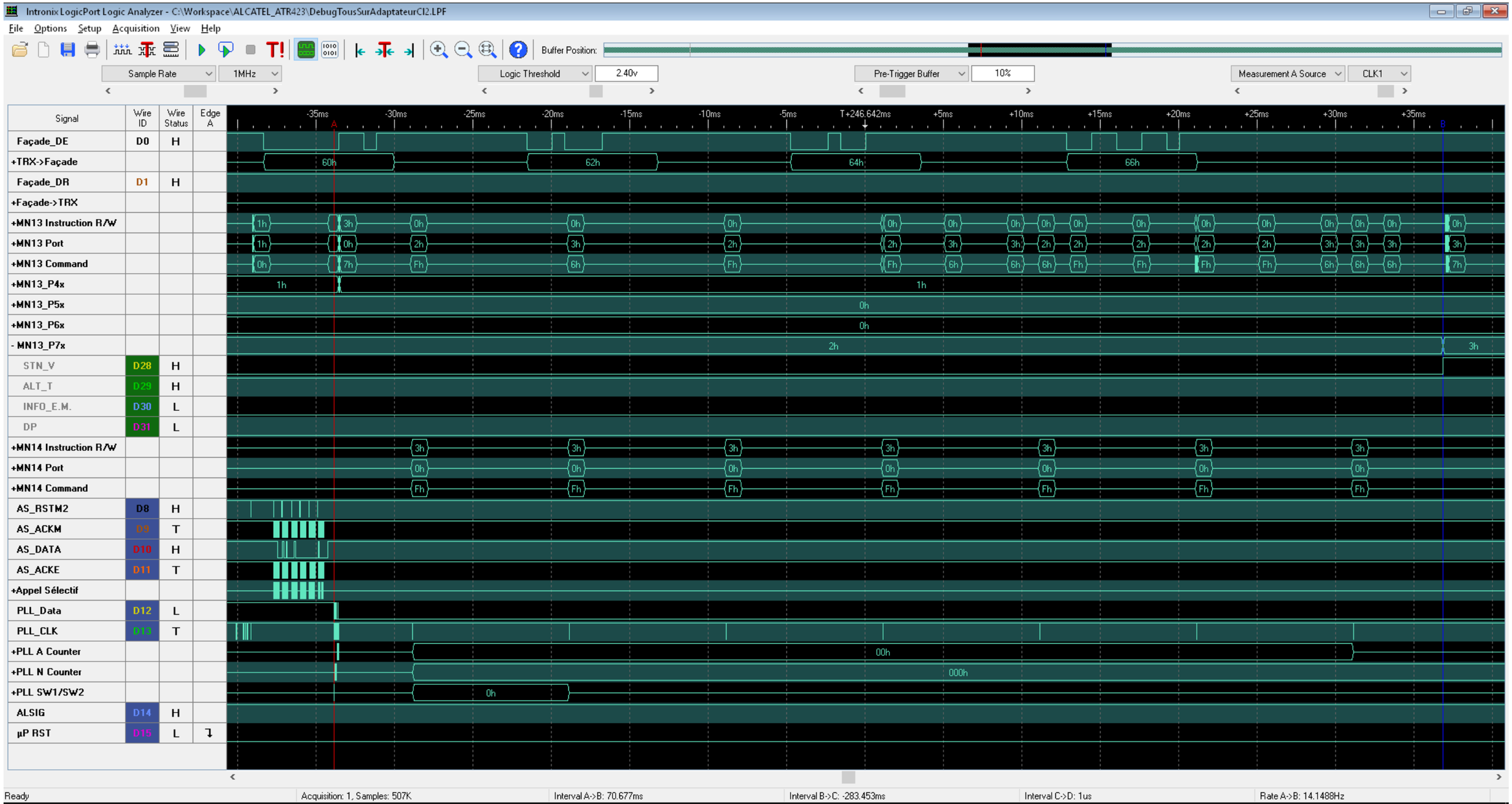
Volume HP mis à 3, voir le chapitre 5.1 Réglage du volume audio RX



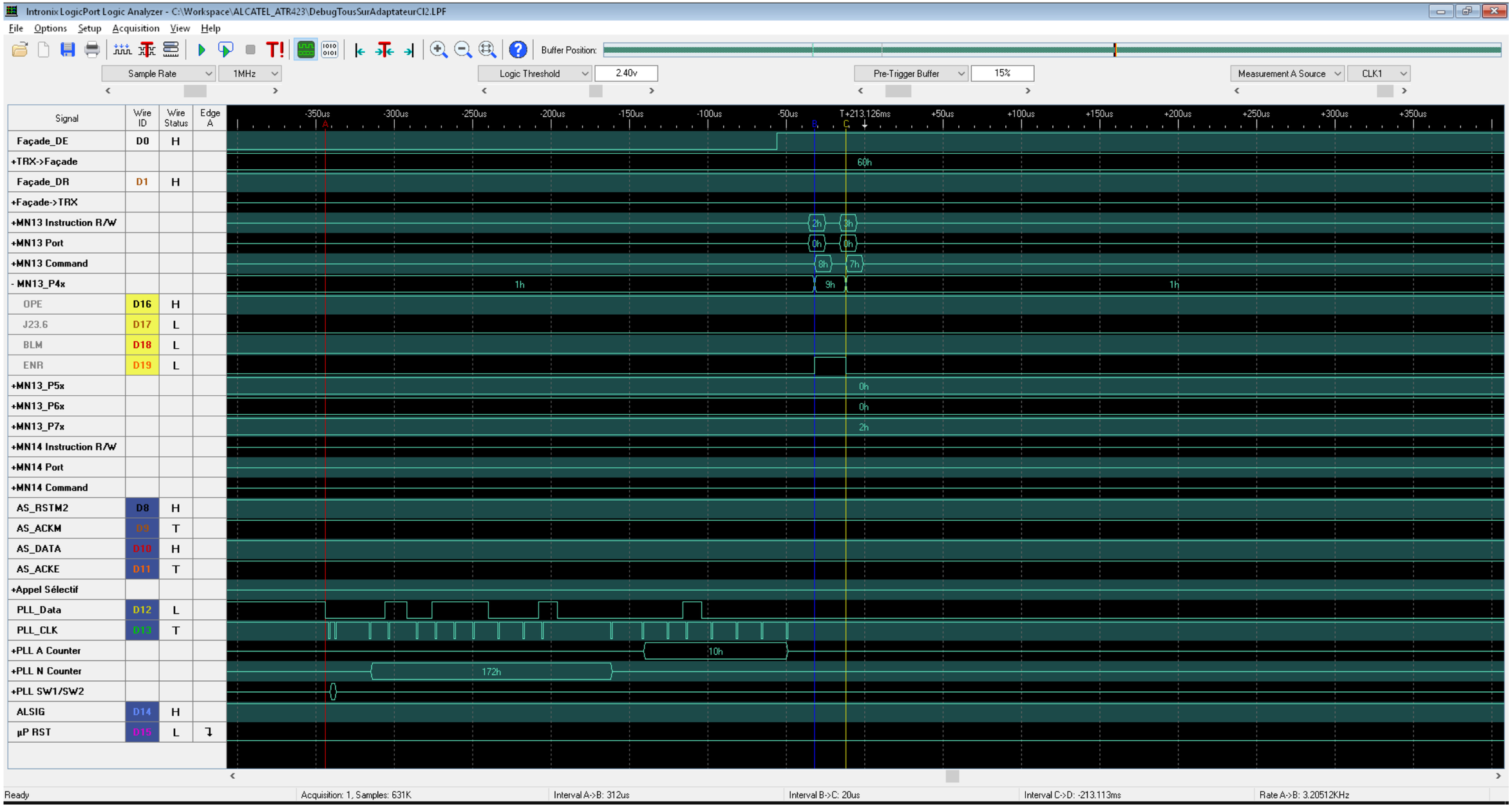
Voir le chapitre 5.7 Détection de porteuse & ouverture du HP pour l'explication détaillée de ces échanges entre MN01/Logique et MN13/logique.

5.6 PLL MN01/HF

L'analyse suivante est basée sur une carte radio équipée de la PLL MN01/HF référence MC145156P. Celles équipées d'un circuit imprimé en lieu et place de MN01, sur lequel est implanté une PLL référence MC145158-2 en boîtier PLCC, nécessitent une version d'EPROM de gestion et/ou de personnalisation adaptée(s) à cette spécificité matérielle car le dialogue avec ces deux références de PLL ne s'effectue pas de la même façon. Si il y a une incohérence logicielle et matérielle, le poste émet dans son haut-parleur une tonalité longue, suivie d'une pause courte, et ceci sans discontinuer, indiquant un problème avec la PLL. Une analyse du dialogue avec la PLL référence MC145158-2 sera réalisée ultérieurement.
Temps de verrouillage de la PLL au démarrage :



Le curseur A est positionné au début de la configuration de la PLL et le curseur B sur le signal fourni par cette dernière indiquant qu'elle est verrouillée : 71ms environs.
La lecture du port 7 de MN13/Logique indique 2h tant que STN_V est à 0 (PLL non verrouillée), puis 3h lorsque STN_V passe à 1.
Zoom sur le paramétrage de la PLL :



Les données sont transmises sur le signal PLL_Data et chaque bit est validé par PLL_CLK. À la fin de l'envoi des 19 bits, l'entrée de validation des données transmises de la PLL (ENR) est pilotée via l'extenseur de port MN13/Logique, sur le port P4.3.

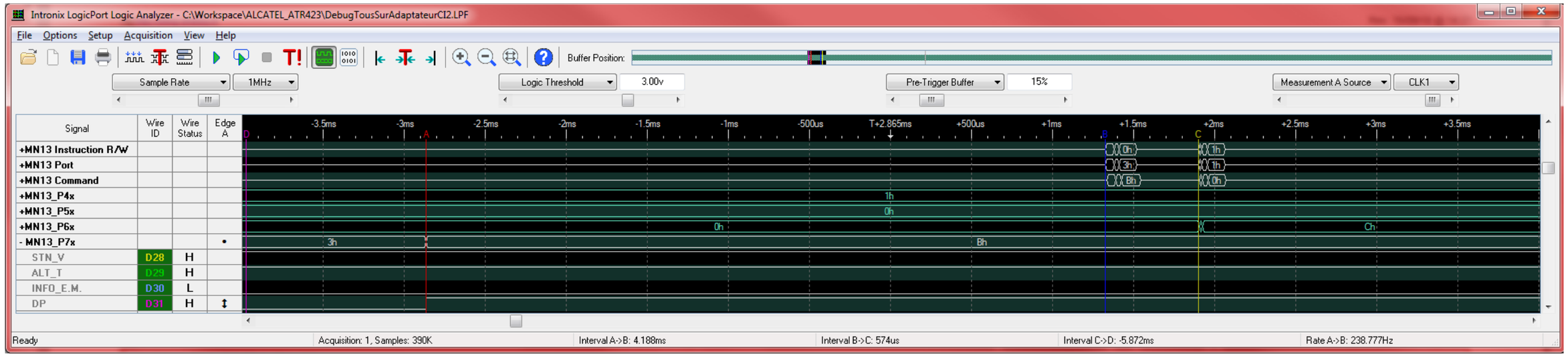
- - L'instruction 2h « OR » est envoyée au port 0h (Port4) avec pour valeur 0h : ceci met ENR à 1 ;
- - L'instruction 3h « AND » est ensuite envoyée au port 0h (Port4) avec pour valeur 7h : ceci met ENR à 0.

Mon tableau de décodage des données envoyées à la PLL est disponible ici. Ce fichier est à ouvrir de préférence avec LibreOffice.

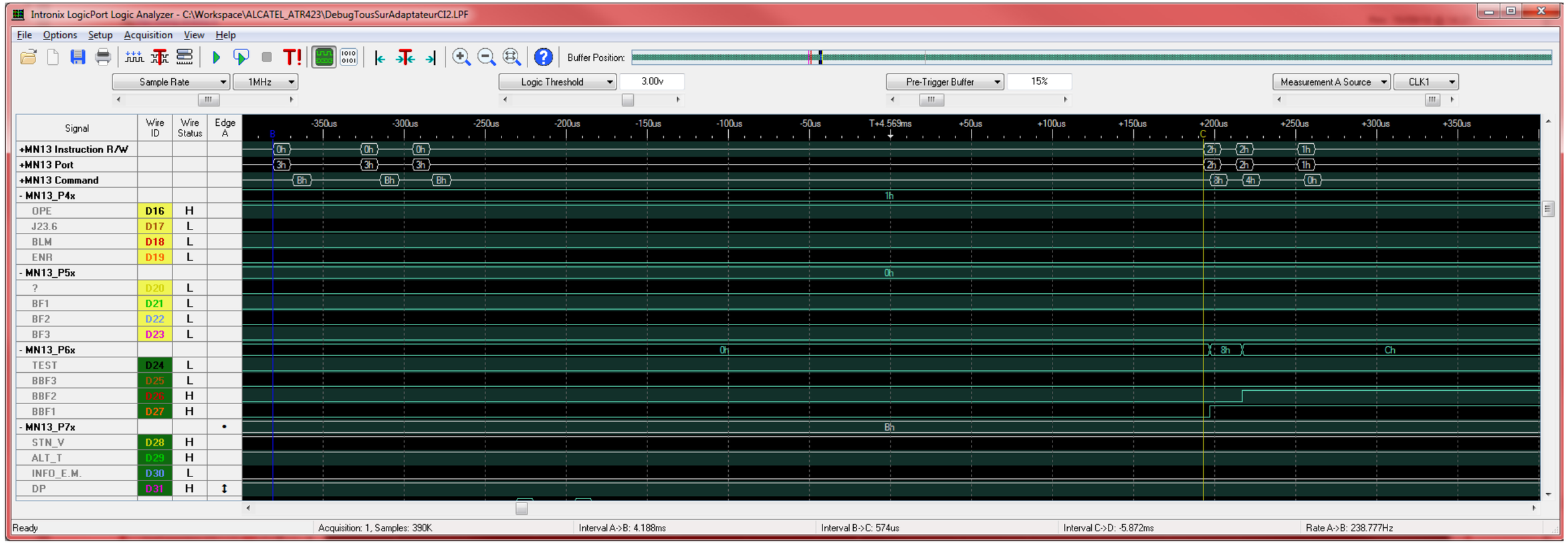
5.7 Détection de porteuse & ouverture du HP

MN01/Logique scrute périodiquement l'état du signal DP, par l'intermédiaire de l'extenseur de port MN13/Logique.
Ci-dessous :

- le curseur A est positionné au niveau du changement d'état de DP ;
- le curseur B est positionné au niveau de la lecture de l'état de DP, via MN13/Logique ;
- le curseur C est positionné au niveau des instructions de déblocage BF ligne téléphonique et HP.



Zoom sur le pilotage des voies BF et du volume :



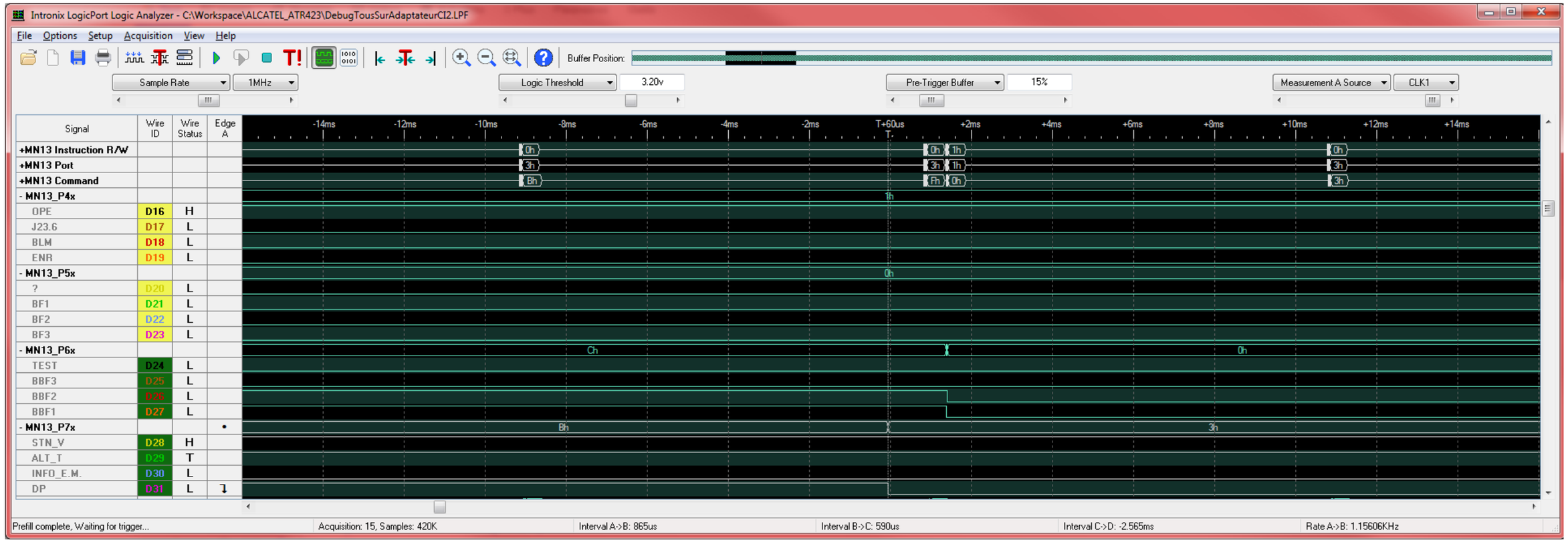
Le changement d'état de DP est donc détecté à partir du curseur B. Il s'agit d'une détection de porteuse (réception d'une émission).
MN01/Logique pilote MA04/Logique (CD4066 - Quadruple switch analogique) par l'intermédiaire de MN13/Logique afin de valider la BF RX :

- vers le HP → mise à 1 de BBF1 ;
- vers la ligne téléphonique (envoyé sur la broche 22 du connecteur SUBD25) → mise à 1 de BBF2.

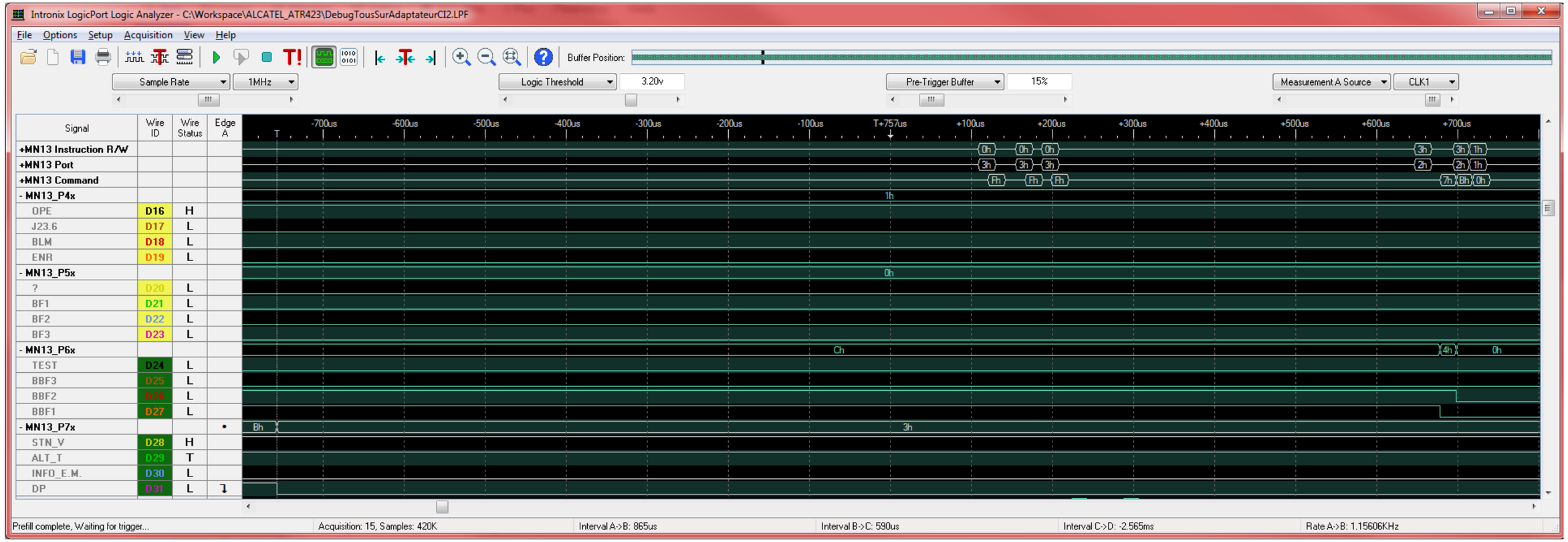
Puis MN01/Logique pilote MA05/Logique (CD4051 – Multiplexeur analogique 8 voies vers 1), toujours via MN13/Logique, afin de redéfinir le volume HP qui était jusqu'ici à 0, pour simuler l'effet de l'ouverture d'un squelch.

MN01/Logique effectue la séquence suivante à la fin de la détection de porteuse (fin de la réception de l'émission) :

- Blocage de la BF RX HP ;
- Blocage de la BR RX ligne téléphonique ;
- Mise en sourdine du HP (squelch fermé).


Intronix LogicPort Logic Analyzer - C:\Workspace\ALCATEL_ATR423\DebugTousSurAdaptateurCI2.LPF
File Options Setup Acquisition View Help
Buffer Position:
Sample Rate
1MHz
Logic Threshold
3.20v
Pre-Trigger Buffer
15%
Measurement A Source
CLK1
Signal
Wire ID
Wire Status
Edge A
+MN13 Instruction R/W
+MN13 Port
+MN13 Command
- MN13_P4x
OPE D16 H
J23.6 D17 L
BLM D18 L
ENR D19 L
- MN13_P5x
? D20 L
BF1 D21 L
BF2 D22 L
BF3 D23 L
- MN13_P6x
TEST D24 L
BBF3 D25 L
BBF2 D26 L
BBF1 D27 L
- MN13_P7x
STN_V D28 H
ALT_T D29 T
INFO_E.M. D30 L
DP D31 L
-14ms -12ms -10ms -8ms -6ms -4ms -2ms T+60us +2ms +4ms +6ms +8ms +10ms +12ms +14ms
Prefill complete, Waiting for trigger...
Acquisition: 15, Samples: 420K
Interval A->B: 865us
Interval B->C: 590us
Interval C->D: -2.565ms
Rate A->B: 1.15606KHz

Zoom sur la détection de disparition de la porteuse :



On constate que la routine de lecture du Port 7 comporte 3 lectures consécutives, quel que soit l'état de DP.

5.8 Passage en émission

Le signal ALT_T présent sur le Port7.1 de MN13/Logique est scruté par MN01/Logique afin de vérifier l'état :

- du PTT du microphone (signal « alternat » de l'organe d'exploitation) ;
- de la carte option (signal « ALT ») ;
- du connecteur accessoires DB25 (signal « ALT »).

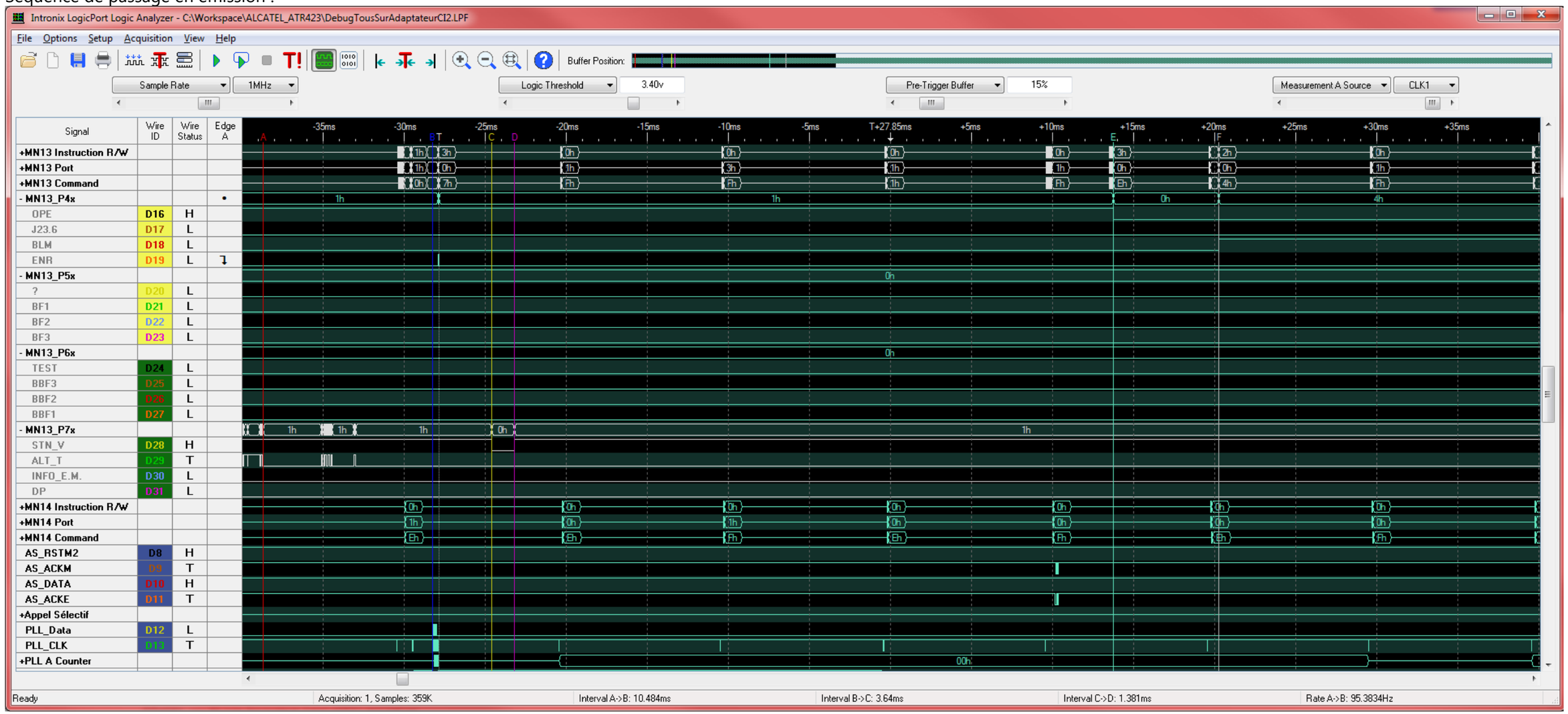
Ces trois signaux sont shuntés entre eux et reliés au Port7.1 de MN13/Logique via le strap « E5 » dans le cas ou le poste est dépourvu de carte option. Autrement c'est la carte option qui fournit l'information ALT_T à MN13/Logique.

MN01/Logique effectue les actions nécessaires au passage en émission du poste dès la mise à la masse de l'entrée ALT_T de MN13/Logique.

Le passage en émission côté carte radio est possible grâce à deux signaux : CER et OPE :

- CER est fourni par la PLL MN01/HF et permet de basculer entre les étages d'émission et ceux de réception ;
- OPE est fourni par MN01/Logique via MN13/Logique et pilote le circuit d'amplification.

Séquence de passage en émission :



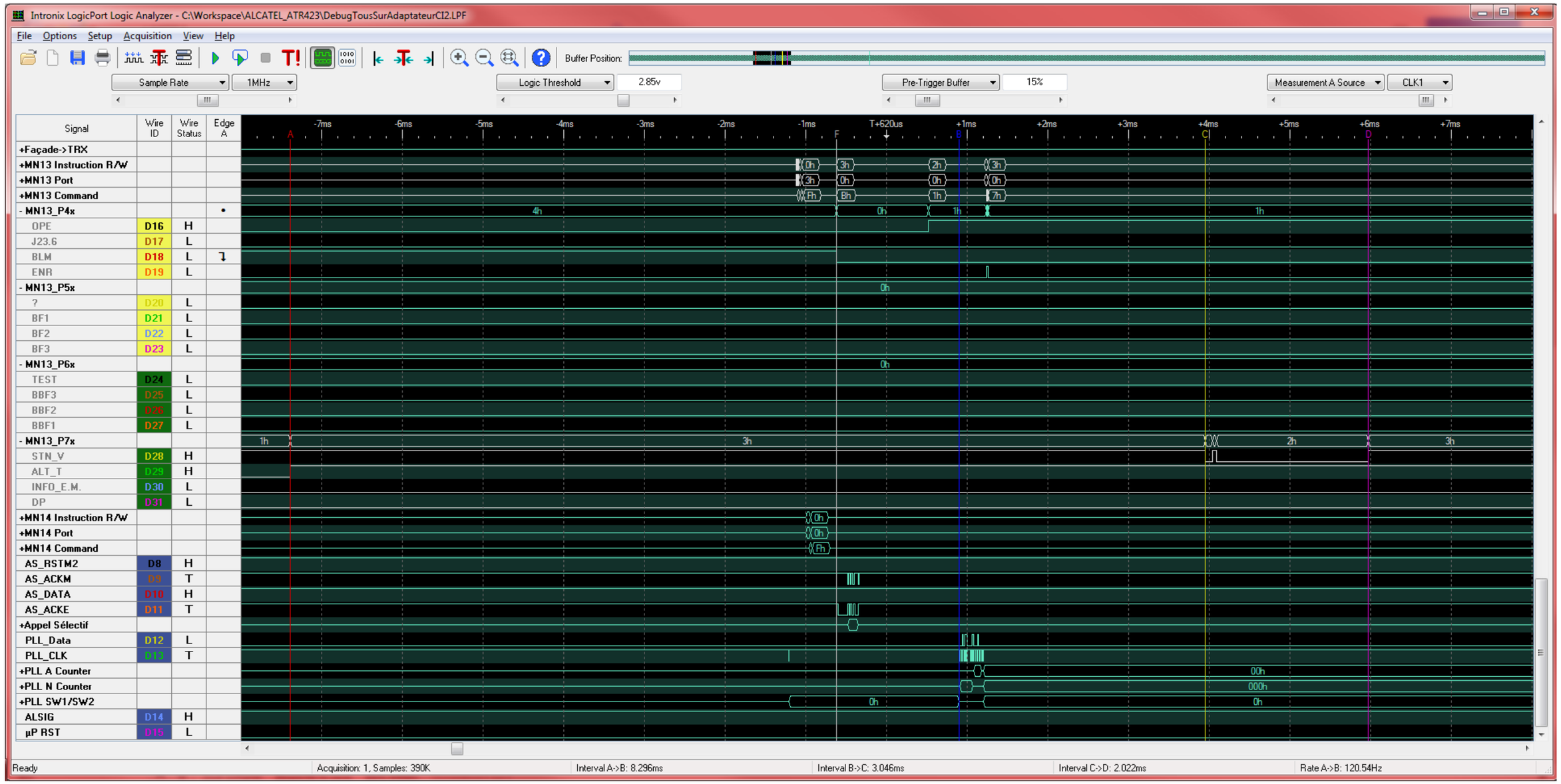
Position des marqueurs dans l'ordre chronologique :

- A = passage à 0 du signal « ALT_T » ;
- B = début de la trame de pilotage de la PLL : définition de la fréquence d'émission et mise à 1 du signal « CER ».
  La validation de l'ordre est transmise juste après l'envoi des 19 bits, avec une impulsion à 1 du signal « ENR » (voir le paragraphe traitant de la PLL) ;
- C à D = déverrouillage de la PLL, le temps du changement de fréquence (signal « STN_V ») ;
- E = pilotage du transistor de l'amplificateur via le signal OPE, permettant l'émission du signal ;
- F = déblocage du signal audio provenant du microphone (signal « BLM »), vers le VCO.

Les durées sont affichées en bas de la capture d'écran fournie ci-dessus.

5.9 Passage en réception

L'ordre d'exécution des actions est différent, mais le principe reste le même :



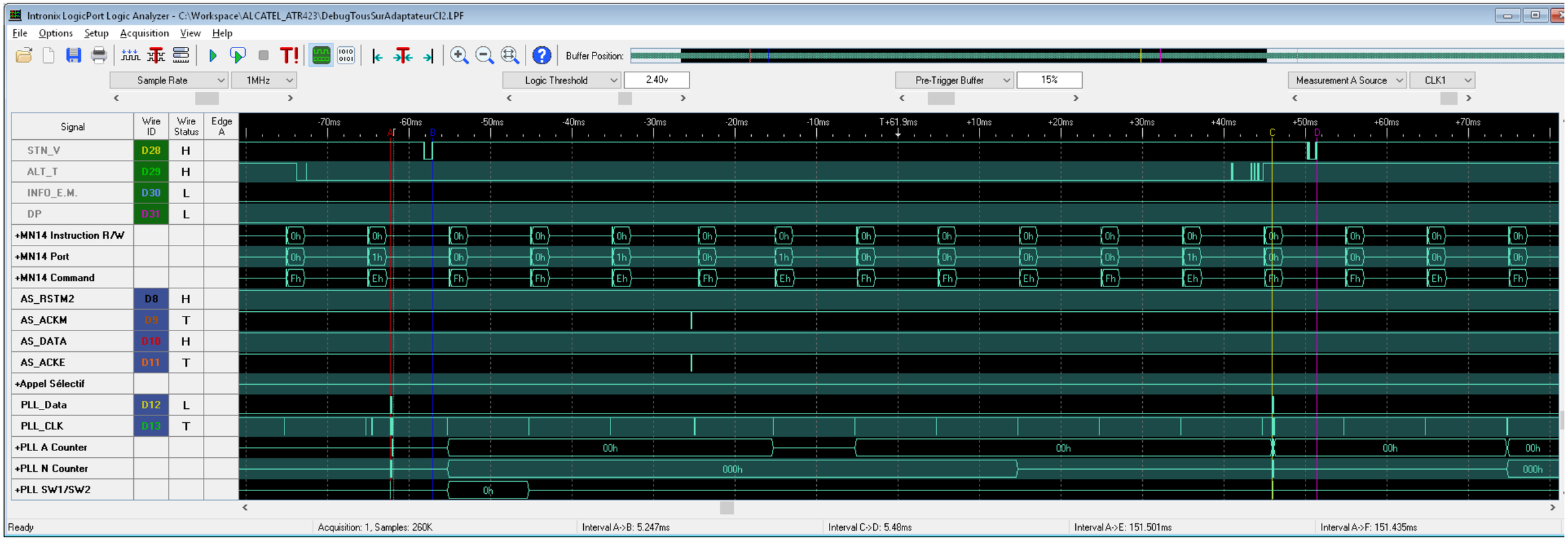
Position des marqueurs dans l'ordre chronologique :

- A = retour à 1 du signal « ALT_T » ;
- F = blocage du signal audio issu du microphone (signal « BLM ») ;

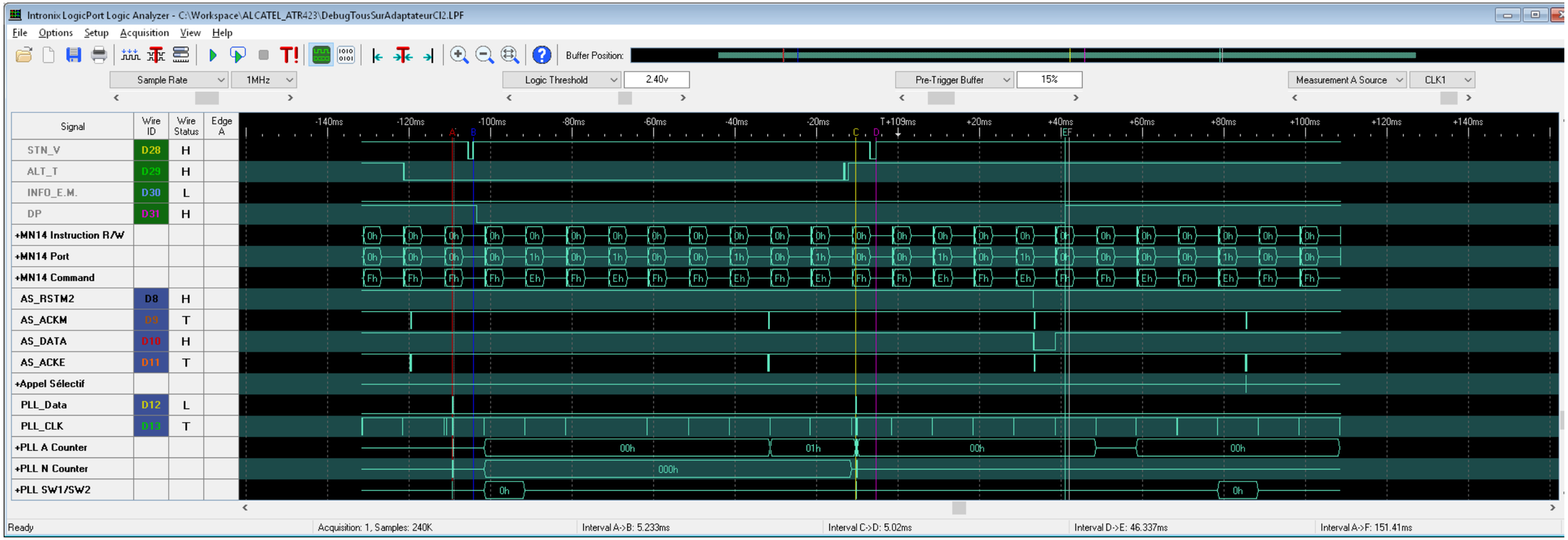
- E = arrêt de l'amplification du signal RF (signal « OPE ») ;
- B = pilotage de la PLL pour rebasculer en réception via le signal « CER » et passer sur la fréquence de réception ;
- C à D = Déverrouillage de la PLL le temps du changement de fréquence (signal « STN_V »).

Dans les deux cas :

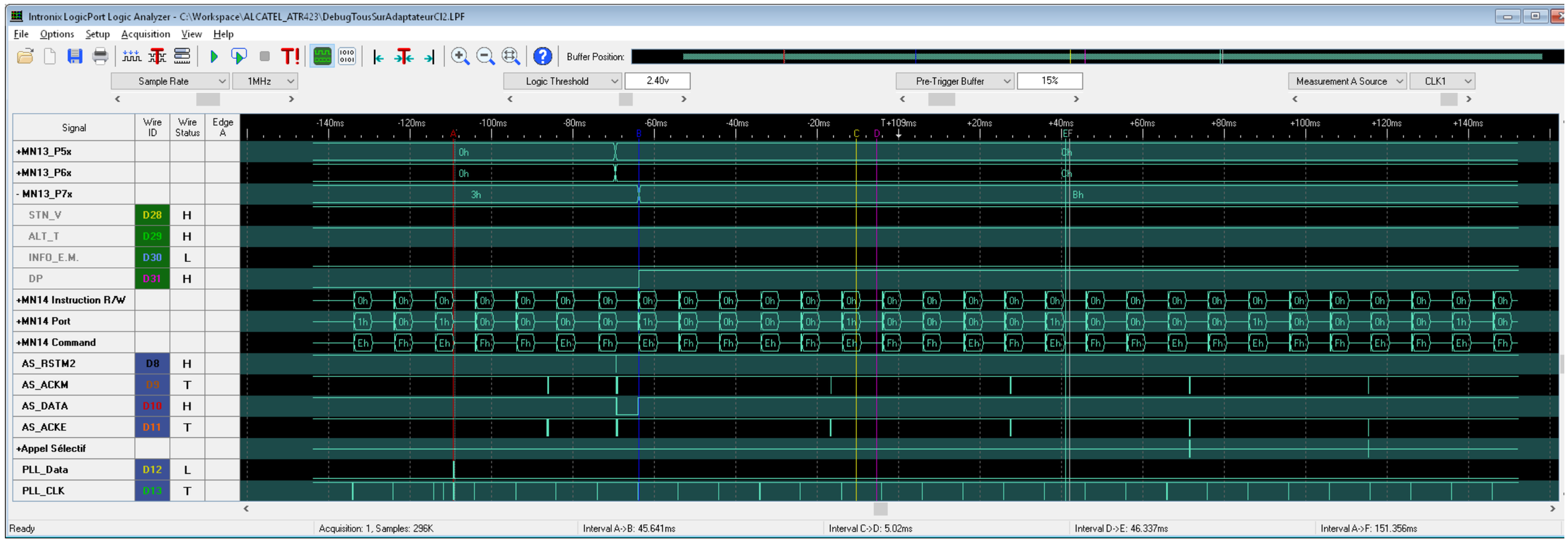
- le pilotage de la PLL est effectué lorsque l'amplification RF n'est pas validée ;
- le signal audio issu du microphone n'est validé qu'en dehors de toutes les séquences de pilotage des autres signaux ;
- le temps de verrouillage de la PLL sur la nouvelle fréquence, mesuré entre le début du premier bit transmis et le retour à un état stable du signal « STN_V », est inférieur à 5,5ms :



Délai de détection de porteuse après basculement émission vers réception du poste, avec le banc radio en émission permanente : inférieur à 50ms :



Délai de détection de porteuse après changement de canal, avec le banc radio en émission permanente : inférieur à 50ms :



On remarque dans ce cas que le signal « STN_V » n'indique pas de déverrouillage de la PLL. Ceci serait donc causé par le basculement TX/RX et RX/TX uniquement, ce qui permet d'accélérer sensiblement la vitesse du scan, bien que le temps de verrouillage soit 10 fois moindre que le temps de détection de porteuse après changement de fréquence. On peut espérer incrémenter de 20 pas par seconde.

6 Spécificités ATR 425 DIAMANT

Tant que ce message est visible, ce paragraphe doit être considéré comme un brouillon / pense-bête. Les infos sont complétées et/ou modifiées au fur et à mesure de l'avancement de l'étude.

6.1 Présentation

L'ATR 425 DIAMANT est une version spécifique, elle aussi, dédiée à la gendarmerie.
Ce poste était équipé notamment :

- D'une carte logique embarquant un modem FFSK 1200bauds (CML FX419J) ;
- D'une carte supplémentaire assurant la fonction de cryptophonie sur laquelle se trouve le MICA (Module Intégré de Cryptophonie Analogique).

L'intérêt principal de ce poste radio est la prise en charge de la fonction de cryptophonie apportée par le MICA, équipement quasi autonome, qui n'échange que des états avec la carte logique par l'intermédiaire de simples entrées / sorties TOR : Il n'y a pas de bus de données entre ces deux éléments.
Ce module se présente sous la forme de deux cartes électroniques gravées sur un support céramique, reliées entre elles par des broches périphériques. Les broches qui servent aux liaisons électriques avec la carte support sont soudées sur la carte se situant en-dessous de cet empilage, et sont décalées d'un demi pas par rapport aux broches d'interconnexion entre les deux cartes du MICA.
Selon les configurations, il est monté :

1. Sur une petite carte support époxy équipée de 3 micro connecteurs 10 contacts, qui permet de l'intégrer dans un portatif type ATR430 ou dans l'ATR420 utilisant la carte logique universelle. Référence 24 00 788 ;
2. Sur une grande carte support époxy équipée d'un connecteur 24 contacts sur nappe, intégrée sous la carte logique, et qui se relie sur le connecteur J22 de cette dernière. Référence 39 418 174.

Ses clés de chiffrement sont reprogrammées par l'intermédiaire d'un terminal baptisé CRY-106 (on rencontre aussi dans certains documents l'appellation CRY-106-2) connecté à cette occasion sur la prise accessoires à l'arrière du poste (DB25 mâle).
La liaison de données entre le CRY-106 et le MICA ne fait que transiter sur la carte logique. Le processeur de la carte logique n'intervient pas dans ce dialogue. Seul le MICA mémorise donc les clés de chiffrement.
À l'analyse du schéma, on voit que le bus de données utilisé est de type série sur un seul lien électrique (fil). Il s'apparente au 1-Wire pour l'interface physique. Le protocole, lui, est inconnu car le CRY-106 reste un appareil introuvable.
Le chiffrement effectué par le MICA est de type temporel : Le signal audio clair issu du microphone est appliqué en entrée du MICA, qui effectue un découpage en segments d'une durée définie (comprenez par là que je ne la connais pas), et chaque segment est découpé en sous segments qui sont mélangés selon l'une des clés de chiffrement. La restitution dans la transmission chiffrée est donc un ensemble de bouts de parole mélangés et incompréhensibles. Chaque sous segment est évidement d'une durée excessivement courte afin de s'assurer qu'aucune sonorité ne puisse être distinguée par l'écouteur ne disposant pas de la bonne clé de (dé)chiffrement.

Côté utilisateur émetteur, la sélection de la clé de chiffrement se fait depuis l'organe d'exploitation, avec une valeur comprise entre 1 et 4. Cette information est codée en binaire sur deux bits (CLE 0 et CLE 1) par le microcontrôleur de la carte logique à destination du MICA.
À l'appui sur le PTT, la carte logique émet la séquence FFSK initiale puis recopie l'état du PTT sur un signal dédié « PTT Traité » partagé avec le MICA, C'est vraisemblablement le « top départ » utilisé par le MICA pour cadencer son découpage du signal audio. Pour l'instant, la synchronisation des MICA récepteurs reste un mystère, car même si ce module utilisait un TCXO pour cadencer l'exécution des tâches de son propre microcontrôleur, ce n'est pas le cas du microcontrôleur de la carte logique. Le moindre délai causé par l'instabilité de l'horloge du microcontrôleur de la carte logique peut induire en erreur les postes à l'écoute. Il n'y a par ailleurs aucune information type « top synchro » fournie au MICA par un récepteur → Le PTT n'est pas impliqué dans ce cas. L'étude de cette partie est rendue compliquée du fait de ne posséder qu'un seul ATR425 DIAMANT. Il faudra recourir à la génération d'une trame FFSK depuis un équipement tiers pour comprendre le mécanisme mis en œuvre côté récepteur.

6.2 Interconnexion sur J22 (carte 6 couches signalisation numérique)

Brochage supposé entre J22 de la carte logique et le MICA, en m'appuyant sur la doc officielle d'Alcatel :

J22 carte logique			MICA		Remarques
N°	SIGLE	Signal	Sens du signal	Broche MICA	
1	MASSE L	M sur le MICA		20	
2	5VL (+5V)				
3	INFO VC	VC sur le MICA LED « clé » Voyant Clair (0=allumé/1=éteint)	Sortie	16	Laisser en l'air sur la carte logique sans MICA, pas du pull-up ou pull-down, Sinon la touche CL/CR ne permet pas de sortir du mode CLAIR !
4	BFRNFND	BF Rx Non Filtrée Non Désaccentuée			
5	BFRNFNDT	BF Rx Non Filtrée Non Désaccentuée Traitée			
6	BFREC	BF Réception Écouteur			
7	INFO_RE_CL	REC_CHIFFRE sur le MICA (0=Clair/1Chiffré)	Sortie	2	
8	Cde C/D	CDECD sur le MICA Commande Clair Discret	Entrée	11	
9	NCLE0	N CLE 0	Entrée	3	
10	INFO C/D	I_C/D sur le MICA INFO Clair/Discret	Sortie	5	
11	DP	0=pas de porteuse / 1=réception porteuse			
12	NCLE1	N CLE 1	Entrée	4	
13	BFETCS	BF Émission TCS			En l'air car les ponts E15 et E16 sur la carte logique sont ouverts !
14	ALT	Alternat (0=TX / 1 = RX)			
15	BFRFT	BFRC sur MICA BF Réception Clair	Sortie	17	Relier ensemble si MICA absent
16	BFRFD	BFRD sur MICA BR Réception Discrèt	Entrée	18	
17	BFENP	BFEC sur le MICA = BF Émission Clair	Entrée	1	Relier ensemble si MICA absent
18	BFENPT	BFED sur le MICA = BF Émission Discret	Sortie	19	
19	VBC (+13.8V)	ALIM sur le MICA comprise entre 8 et 15,6V	Entrée	13	
20	Cde AIG	État logique sélection CL/CD (0=clair / 1 = Chiffré)			
21	EFF_CLE	Éffacement des CLÉs (0=fct normal / 1=Effacement des clés)	Entrée	14	
22	ALT_T	INFO_PEDALE sur le MICA (0=RX / 1=TX)	Entrée	15	Relier ensemble si MICA absent
23	ALT_SOFT	CDEM sur le MICA	Sortie	9	
24	CRY106	ICLE sur le MICA Injection des CLÉs	Entrée	12	
			Entrée	6	CDEALIM sur le MICA (0=fonctionnement normal/1=Conso<0,5mA)
			Entrée	7	DECOUPLAGE
			Entrée	8	RESET
			Sortie	10	+5V (alim régulée 20mA)

6.3 Fonctions trouvées par essai/erreur

A. **Suppression des clés de chiffrement**
   1. **N'effectuez JAMAIS cette action si votre MICA n'a pas déjà été réinitialisé ! La description de cette procédure est justement fournie pour vous éviter un geste regrettable.**
      a. **Dans le mode de fonctionnement courant du poste, appuyer sur la touche « flèche », puis #, puis CL/CR ;**
      b. **L'écran affiche CLE EFFA ;**
      c. **Fin de la crpytophonie sur votre poste :(**

B. Affichage de la version logicielle
   1. À la mise sous tension du poste avec le bouton marche/arrêt, celui-ci affiche un code sur 4 chiffres pendant 5 secondes.
   2. Appuyer sur le bouton APPEL. La version logicielle s'affiche à l'écran tant que le bouton n'est pas relâché.

C. Sélection de la clé de chiffrement
   1. Dans le mode de fonctionnement courant du poste, appuyer sur l'une des touches numériques entre 1 et 4, puis sur la touche « flèche », puis sur la touche CL/CR (fonction alternative « clé »).

D. Interrogation de la clé courante
   1. Dans le mode de fonctionnement courant du poste, appuyer sur la touche « flèche », puis sur la touche CL/CR (fonction alternative « clé »).

E. Modification de l'identifiant individuel
   1. À la mise sous tension du poste avec le bouton marche/arrêt, celui-ci affiche un code sur 4 chiffres pendant 5 secondes. Il s'agit de l'identifiant d'appel du poste.
      1. Il est décomposé en deux parties : Les milliers ainsi que les centaines correspondent au département, et les dizaines ainsi que les unités représentent le numéro du terminal radio.
   2. Pendant ces 5 secondes, il est possible de saisir un nouvel identifiant avec le pavé numérique :
      1. En cas d'erreur de saisie, la touche # conserve sa fonction d'effacement ;
      2. Une fois que le nouvel identifiant est saisi, appuyer sur la touche « flèche » : Un D apparaît sur le huitième caractère de l'afficheur
      3. Appuyer juste après sur la touche MODE (fonction alternative N.INDIV) : Un I apparaît sur le septième caractère de l'afficheur, qui indique alors ID.
   3. À l'issue de la dernière action sur le clavier, le délai de 5 secondes reprend son décompte puis le poste affiche l'écran d'accueil de l'applicatif (varie selon le mode de fonctionnement)
   4. La prise en compte du nouvel identifient peut alors être vérifiée en appuyant à nouveau sur les touches « flèche » puis MODE.
      1. Comme pour beaucoup d'autre affichages temporisés, il est possible de quitter l'affichage rapidement en appuyant sur la touche #.

C. Bascule Simplex / Duplex
   1. Mode Simplex
      a. Il existe deux sous-modes : Libre ou Sélectif
         1. Libre
            - Le poste fonctionne sans appel sélectif ;
            - La désactivation du squelch s'effectue avec la combinaison de touches « flèche » puis 8 (fonction alternative SQL) :
               - Si la sortie HP est validée (LED verte à côté du dessin de HP allumée), on doit entendre le souffle dans le haut-parleur ;
               - Si la sortie HP est invalidée, appuyer sur la combinaison de touches « flèche » puis 7 (fonction alternative HP).
               - Il n'est pas obligatoire d'ouvrir le squelch pour entendre son interlocuteur. Tant qu'on reste dans le mode Libre, la détection de porteuse ouvrira automatiquement le squelch.
            - Les modes CLair et CRypté sont utilisables ;
            - La sélection de la fréquence d'émission/réception se fait de deux façon :

- En choisissant une mémoire prédéfinie parmi les 9 sélectionnables, en appuyant sur l'une des touches de chiffre suivie par la touche *. L'afficheur indique le numéro de mémoire sélectionnée sur le premier caractère, suivi de **LIB** à la fin de l'écran. Ex. : **0 LIB** si la mémoire 0 est sélectionnée.
- En choisissant le canal affecté à la mémoire sélectionnée, par la combinaison de touches « flèche » puis * (fonction alternative PROG) :
  - L'afficheur indique alors le numéro de mémoire sur laquelle on se trouve, suivie par le numéro de canal sur 4 caractères[1], suivie par l'inscription CA (CAnal) :
    - On peut saisir avec le clavier le canal qui sera affectée à la mémoire, par exemple 0000 (40,800MHz sur mon poste), et on valide avec la combinaison de touches « flèche » puis * ;
    - L'afficheur indique alors le numéro de mémoire sur laquelle on se trouve, suivie par le numéro d'appel sélectif sur 4 caractères, suivi par l'inscription AS (Appel Sélectif) :
      - On peut saisir avec le clavier l'appel sélectif associé au canal et on valide avec la combinaison de touches « flèche » puis * ;
      - L'afficheur indique alors « SIMPLEX » pendant 10 secondes si le canal sélectionné est en simplex, ou « TEST RE » s'il s'agit d'un canal duplex. Un retour accéléré à l'écran est possible avec la touche #.
  - [1]*Note : L'affichage du canal est sur 4 caractères, mais seules les dizaines et unités servent à désigner le canal entre 0 et 99 (voir la table des canaux dans le paragraphe xxx). Les milliers et centaines servent à définir un code de groupe spécifique sur le canal. Exemple : le canal 9933 utilisera la fréquence de la présélection CA 0033 avec le code d'appel sélectif 9933.*
  -

2. Sélectif
   - Ce n'est pas encore étudié tant que le fonctionnement de l'appel sélectif n'est pas connu.

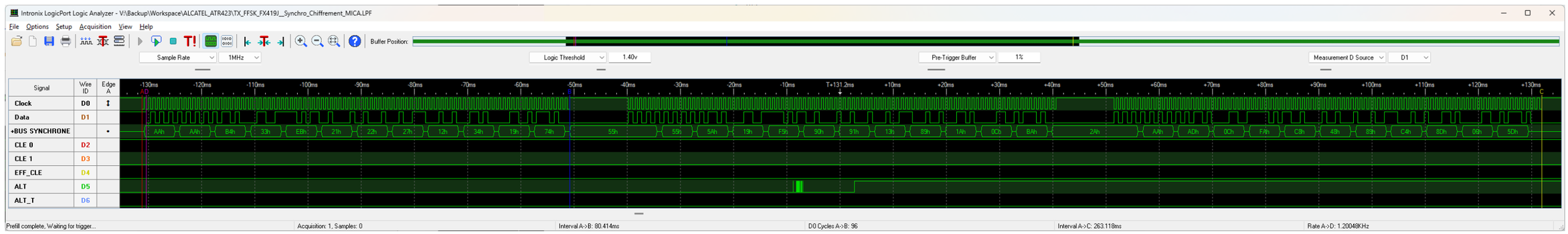
2. Mode duplex
   1. Ce n'est pas encore étudié tant que le fonctionnement de l'appel sélectif n'est pas connu.

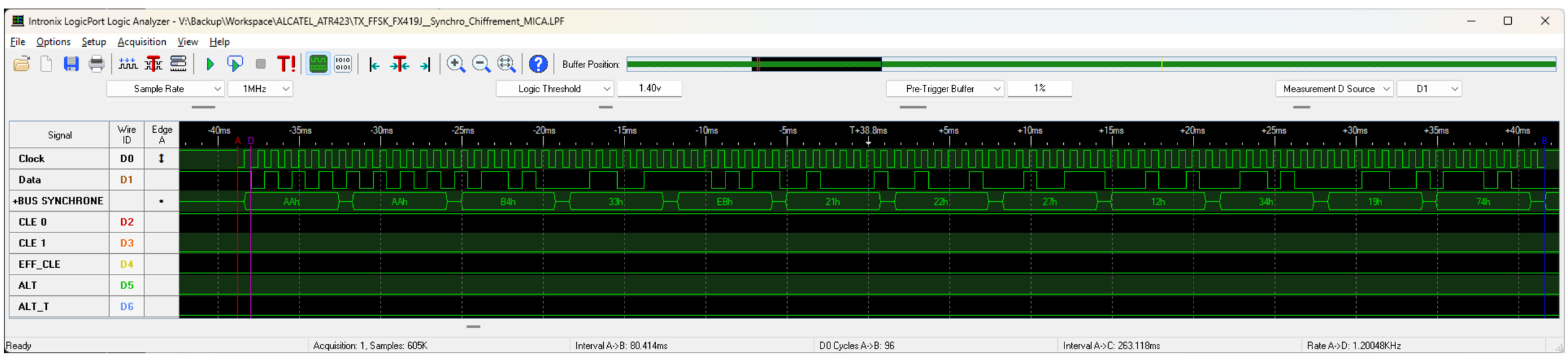
6.4 Signalisation FFSK

Les informations « numériques » échangées par les postes sont véhiculées par l'intermédiaire di modem FFSK FX419 de chez CML. Ce format de transmission offre beaucoup plus de possibilités en terme de codage que les formats habituels (5-tons, CTCSS, DTMF).

En mode « CRYPTE », la carte logique émet à chaque appui sur la pédale d'alternat, ainsi que de façon périodique (toutes les16 secondes) durant toute la prise de parole, une séquence FFSK 1200bps servant à rallier les postes à l'écoute de la fréquence dans la communication. La documentation d'Alcatel traitant du MICA évoque une synchronisation des récepteurs, mais l'absence de dialogue entre la carte logique et le MICA me fait plutôt penser à un abus de langage. Au mieux, l'information de clé sélectionnée sur le poste émetteur, elle aussi transmise dans la séquence FFSK de l'émission chiffrée, permet aux postes en écoute d'utiliser la bonne clé pour déchiffrer le message.
Ceci étant dit, la documentation utilisée comme source d'informations au sujet du MICA et de son fonctionnement fournit d'autres caractéristiques du signal FFSK qui ne sont pas cohérentes avec le fonctionnement observé sur l'ATR 425 DIAMANT. Face à la forte diversité d'applicatifs dont le fonctionnement est adapté à des clients spécifiques (DDE, 2 versions pour EDF, Gendarmerie, transports en commun, Pompiers, etc.), il n'est pas non plus inimaginable que le fonctionnement du MICA soit aussi différent d'une application à une autre, notamment pour assurer l'impossibilité d'utiliser un poste non DIAMANT bricolé pour écouter les communications chiffrées de ce réseau.
La signalisation FFSK est également utilisée pour la fonction d'appel sélectif (normal ou urgent) et l'enregistrement sur un relais.

Voici un exemple de séquence FFSK capturée sur les entrées du modem CML FX419J, émise en début de communication chiffrée :





On voit ici que la séquence de la transmission FFSK dure 263ms (mesure entre les marqueurs A et C). Elle comprend 3 trames de 80,4ms chacune (mesure entre les marqueurs A et B).
Une trame est composée de 96 bits (mesure entre les marqueurs A et B). Le débit binaire est fixé par le signal d'horloge visible sur la voie D0, soit 1200bps (mesure entre les marqueurs A et D).

Le décodeur utilisé sur l'analyseur logique est de type synchrone.

6.4.1 Contenu d'une trame

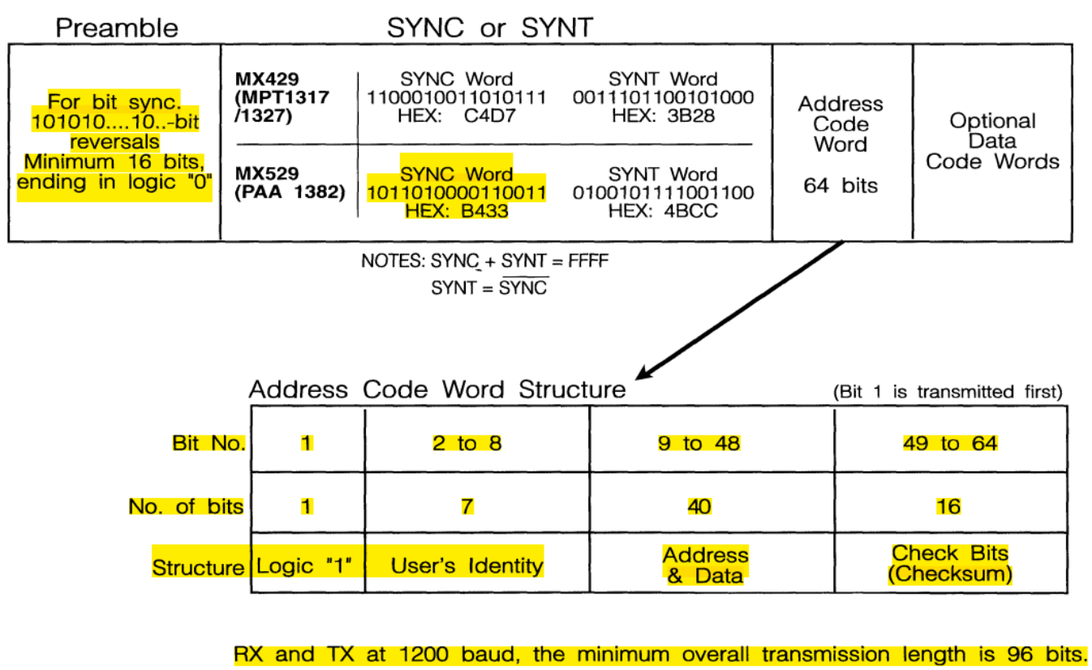
Les 2 premiers octets servent de préambule de trame. Il s'agit alternance de 1 et de 0 décodés sous la forme de 2 octets valant 0xAA chacun (0b10101010).
Les 2 octets suivants servent de synchro de trame et valent dans le cas présent toujours 0xB433. Cette entête est familière, car elle est semblable à celle utilisée par le standard PAA 1382. Ce n'est pas le seul point commun avec ce standard. J'y reviendrai un peu plus tard.
Les 6 octets suivants contiennent l'information à transmettre. Dans l'exemple visible sur la capture de trame ci-dessus, on pourra observer une indication du type de données émise, la clé de chiffrement utilisée s'il s'agit dune communication phonie, ainsi que l'identifiant de l'appelant ou de l'appelé.
Les 2 octets suivants contiennent le CRC de la trame, permettant de vérifier son intégrité. Le CRC reçu doit être identique à celui calculé localement par le poste récepteur à partir des 6 octets précédents.

Le contenu de chaque trame est invariable d'une émission à une autre tant qu'aucun paramètre n'est modifié. Il n'y a donc pas de code tournant.
Il faut garder à l'esprit qu'il s'agit d'une signalisation, et non d'une donnée fournissant aux autres équipements radio la clé de chiffrage. L'information véhiculée dans ces données FFSK n'est donc pas confidentielle.

On peut alors représenter le contenu de la trame sous cette forme, plus visuelle :

				1	**2 to 8**	**9 to 48**				**49 to 64**	
Préambule		**Synchro Trame**		**Type de trame**		**Code fixe ?**		**Info clé**	**Identifiant**		**CRC**	
AA	**AA**	**B4**	**33**	WW		*21*	*22*	XX	YY	ZZ	CC	CC

Comme mentionné précédemment dans ce sous-chapitre, le format de la trame n'est pas sans rappeler celui du standard PAA 1382, décrit comme indiqué ci-dessous dans la documentation du modem FFSK FX529 de chez MX-COM (ancien nom du FX529 de chez CML) :



Détail des champs de données

Type de trame	Commentaire
0xEA	Interrogation manuelle du relais (touche RE) ou périodique
0xEB	Appui PTT en mode chiffré ou appel sélectif (touche APPEL)
0xF0	Appel d'urgence (touche URG)

Info clé	Commentaire
0x00	Appel d'urgence (touche URG)
0x02	Appel sélectif (touche APPEL)
0x05	Interrogation manuelle d relais (touche RE) ou périodique
0x*n*7	Appui PTT en mode chiffré, avec *n* compris entre 1 et 4

Identifiant*	Commentaire
0x*YYZZ*	Identifiant individuel de l'émetteur si appui PTT ou appel urgent
0xYYZZ	Identifiant individuel de l'appelé (touche APPEL)
0xYYZZ	Identifiant canal (CA) en mode duplex

***** *L'identifiant est décomposé en deux éléments :*

- *Identifiant individuel :*
  - *YY = Code départemental ;*
  - *ZZ = Identifiant du terminal radio danse le département.*
- *Canal :*
  - *YY = Code du groupe ;*
  - *ZZ = Numéro du canal.*
    - *Les canaux ne sont codés que sur deux chiffres : unités et dizaines. La fréquence du canal ne change pas quel que soit le chiffre saisi dans les centaines et milliers de l'identifiant complet.*

Codage du CRC

Cette partie de l'analyse a été réalisée principalement avec l'aide de ChatGPT.
C'est ici que le rapprochement avec le standard PAA 1382 semble prendre fin. L'IA n'a pas trouvé de cohérence entre l'algorithme de calcul du CRC du standard PAA 1382 et le CRC décodé avec l'analyseur logique. Cela se confirme sur 80 trames uniques capturées avec l'analyseur logique.

Par déduction, en s'appuyant sur les 80 trames capturées, l'IA a recoupé les changements d'état des bits des 6 octets de données et leur influence sur le CRC capturé et à généré un algorithme spécifique au format de données FFSK de l'ATR 425 DIAMANT.
Afin de comprendre la notation de cet algorithme, il faut prendre en considération le nommage des bits de chaque octet qui a été retenu. Reprenons la représentation précédente, avec une ligne supplémentaire en bas du tableau :

				1	2 to 8							9 to														48	49 to 64															
Préambule		**Synchro Trame**		**Type de trame**								**Code fixe ?**														**Info clé**	**Identifiant**														**CRC**			
AA	**AA**	**B4**	**33**	WW								*21*								*22*						XX	YY							ZZ							CC			
			Bit →	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	*7*	*6*	*5*	*4*	***2***	*1*	*0*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*	*15*	*14*	*13*	*12*	*11*	*10*	*9*	*8*	*7*	*6*	*5*	*4*	*3*	*2*	*1*	*0*
			Octet →	*5*								*4*								***3***							*2*								*1*							*0*				*crc*															

La notation bit(B[3],2) représente le bit 2 de l'octet 3, mis en évidence et gras et en rouge ci-dessus.

Maintenant que tout est clair, voici les formules de calcul :

crc[0] = bit(B[0],0) ^ bit(B[3],2) ^ bit(B[4],4) ^ bit(B[4],0) ^ bit(B[5],6) ^ bit(B[5],3)
crc[1] = bit(B[0],4) ^ bit(B[4],5) ^ bit(B[4],1) ^ bit(B[5],7) ^ bit(B[5],4)
crc[2] = bit(B[0],7) ^ bit(B[0],4) ^ bit(B[3],4) ^ bit(B[4],6) ^ bit(B[4],2) ^ bit(B[4],0) ^ bit(B[5],5)
crc[3] = bit(B[0],7) ^ bit(B[0],4) ^ bit(B[3],5) ^ bit(B[4],7) ^ bit(B[4],3) ^ bit(B[4],1) ^ bit(B[5],6)
crc[4] = bit(B[0],0) ^ bit(B[3],4) ^ bit(B[3],2) ^ bit(B[4],5) ^ bit(B[4],3) ^ bit(B[4],2) ^ bit(B[4],0) ^ bit(B[5],7) ^ bit(B[5],6) ^ bit(B[5],2) ^ bit(B[5],0)
crc[5] = bit(B[3],5) ^ bit(B[3],4) ^ bit(B[3],2) ^ bit(B[4],6) ^ bit(B[4],4) ^ bit(B[4],3) ^ bit(B[4],1) ^ bit(B[4],0) ^ bit(B[5],7) ^ bit(B[5],3) ^ bit(B[5],1)
crc[6] = bit(B[0],7) ^ bit(B[0],4) ^ bit(B[0],0) ^ bit(B[3],5) ^ bit(B[3],4) ^ bit(B[3],2) ^ bit(B[4],7) ^ bit(B[4],3) ^ bit(B[4],2) ^ bit(B[4],1) ^ bit(B[5],6) ^ bit(B[5],4) ^ bit(B[5],0)
crc[7] = bit(B[0],4) ^ bit(B[0],0) ^ bit(B[3],6) ^ bit(B[3],5) ^ bit(B[4],4) ^ bit(B[4],3) ^ bit(B[4],2) ^ bit(B[5],7) ^ bit(B[5],5) ^ bit(B[5],1)
crc[8] = bit(B[0],7) ^ bit(B[0],4) ^ bit(B[3],6) ^ bit(B[3],2) ^ bit(B[4],7) ^ bit(B[4],6) ^ bit(B[4],5) ^ bit(B[4],3) ^ bit(B[5],7) ^ bit(B[5],6) ^ bit(B[5],1) ^ bit(B[5],0)
crc[9] = bit(B[0],4) ^ bit(B[3],6) ^ bit(B[3],4) ^ bit(B[4],5) ^ bit(B[4],4) ^ bit(B[4],3) ^ bit(B[4],0) ^ bit(B[5],6) ^ bit(B[5],2) ^ bit(B[5],0)
crc[10] = bit(B[0],7) ^ bit(B[3],6) ^ bit(B[3],5) ^ bit(B[3],2) ^ bit(B[4],6) ^ bit(B[4],3) ^ bit(B[4],1) ^ bit(B[4],0) ^ bit(B[5],7) ^ bit(B[5],6) ^ bit(B[5],3) ^ bit(B[5],2) ^ bit(B[5],1) ^ bit(B[5],0)
crc[11] = bit(B[0],4) ^ bit(B[0],0) ^ bit(B[3],2) ^ bit(B[4],7) ^ bit(B[4],5) ^ bit(B[4],3) ^ bit(B[4],2) ^ bit(B[4],1) ^ bit(B[5],7) ^ bit(B[5],6) ^ bit(B[5],4) ^ bit(B[5],3) ^ bit(B[5],1) ^ bit(B[5],0)
crc[12] = bit(B[0],7) ^ bit(B[0],4) ^ bit(B[4],6) ^ bit(B[4],4) ^ bit(B[4],3) ^ bit(B[4],2) ^ bit(B[4],0) ^ bit(B[5],7) ^ bit(B[5],5) ^ bit(B[5],4) ^ bit(B[5],2) ^ bit(B[5],1)
crc[13] = bit(B[0],4) ^ bit(B[0],0) ^ bit(B[3],6) ^ bit(B[4],7) ^ bit(B[4],1) ^ bit(B[5],5) ^ bit(B[5],3) ^ bit(B[5],0)
crc[14] = bit(B[0],4) ^ bit(B[0],0) ^ bit(B[3],2) ^ bit(B[4],2) ^ bit(B[5],6) ^ bit(B[5],4) ^ bit(B[5],1)
crc[15] = bit(B[0],7) ^ bit(B[0],0) ^ bit(B[4],3) ^ bit(B[5],7) ^ bit(B[5],5) ^ bit(B[5],2)

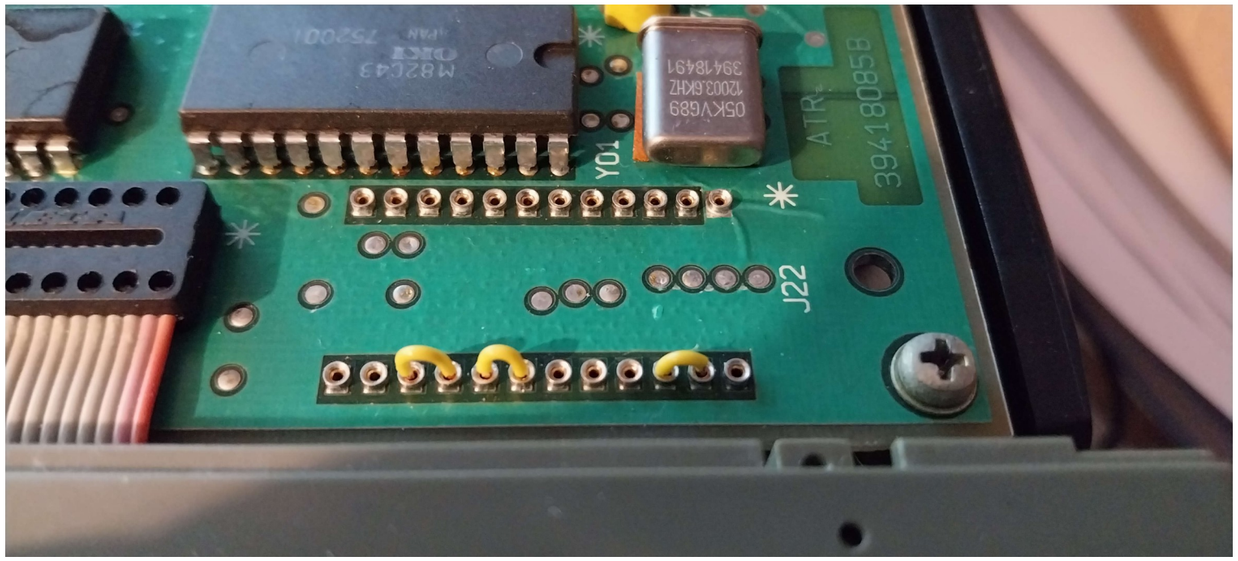
Le signe ^ représente l'opération « OU Exclusif » (XOR).

Un programme Python utilisant ces formules est mis à disposition sur mon dépôt GitHub : https://github.com/DevSHIBBY/paa1382_crc_decoder

Prochaine étape : Simuler un second poste avec une carte modem FFSK utilisant un FX529 de chez CML. Au moment où j'écris ces lignes, le PCB est en cours de fabrication chez PCBWay.

6.5 Utilisation sans MICA

Une modification simple à mettre en œuvre, sans utiliser le fer à souder et réversible rapidement, consiste à créer des ponts entre les les signaux normalement traités par le MICA sur le connecteur J22 de la carte logique :



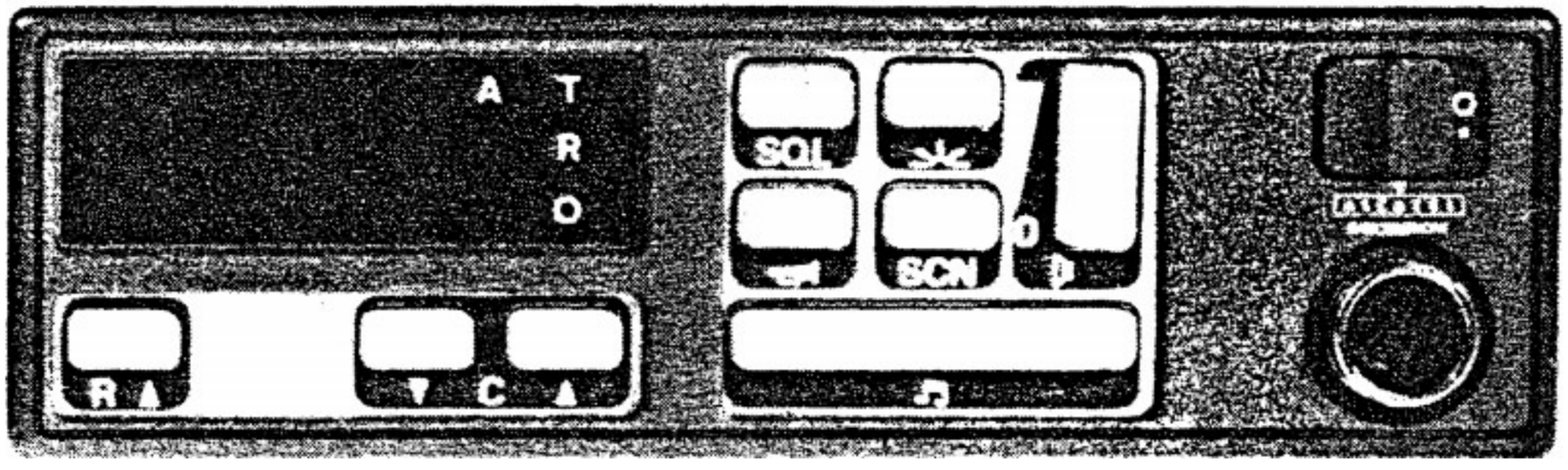
Cette configuration est applicable à la carte 6 couches avec signalisation numérique uniquement. Dans le doute, vérifiez la concordance du numéro de cuivre entre votre carte et celle prise en photo ci-dessus.

6.6 Utilisation avec MICA

En mode « CLAIR », les deux commutateurs analogiques DG412 de la carte support effectuent un rebouclage semblable à ceux visibles sur la photo ci-dessus.
En mode « CRYPTE », les signaux traversent le MICA. Par sécurité, afin de ne pas diffuser une information censée être chiffrée, aucun signal audio n'est émis si le MICA a ses clés effacées.

7 Annexe 1 – Différents équipements

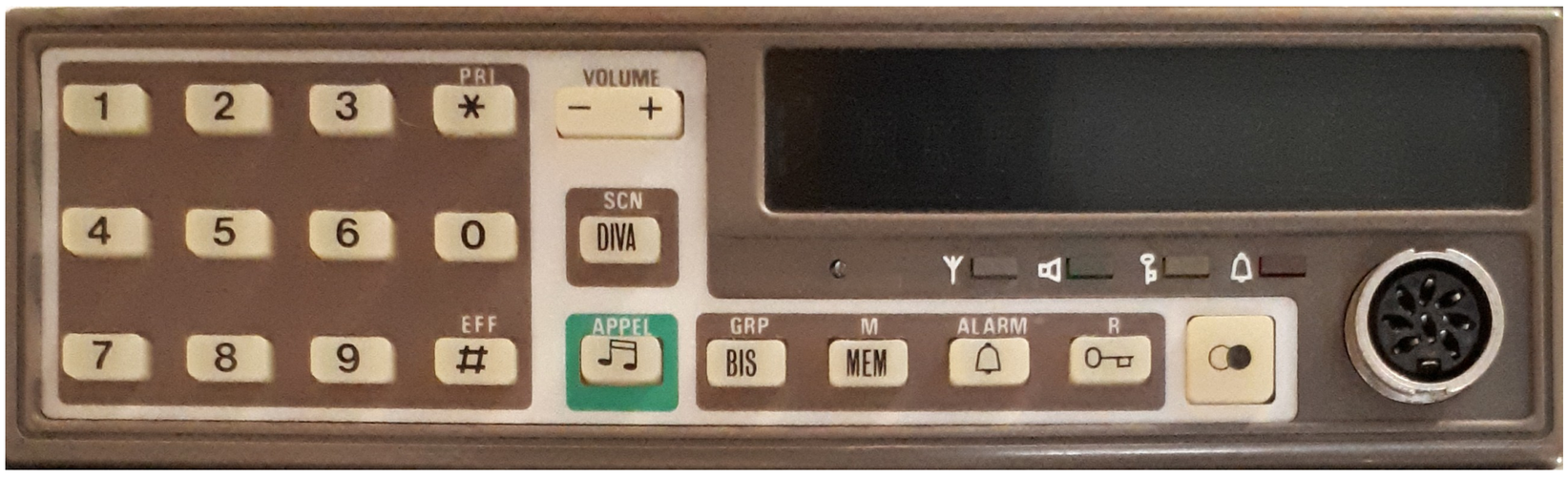
7.1 SC10



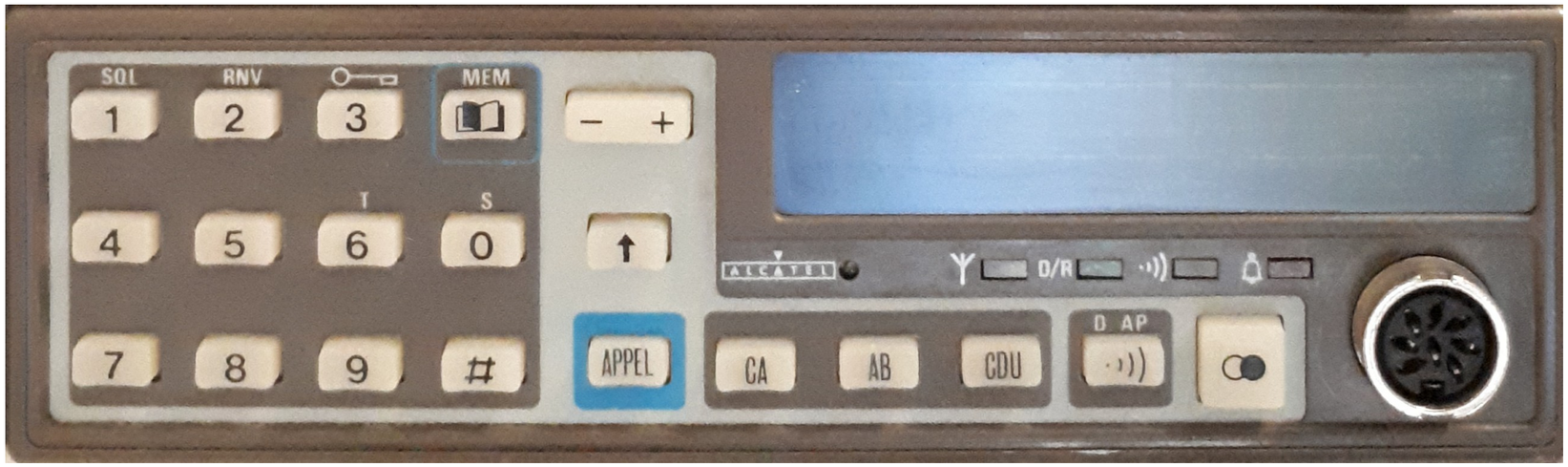
7.2 SC2

7.3 DGC M

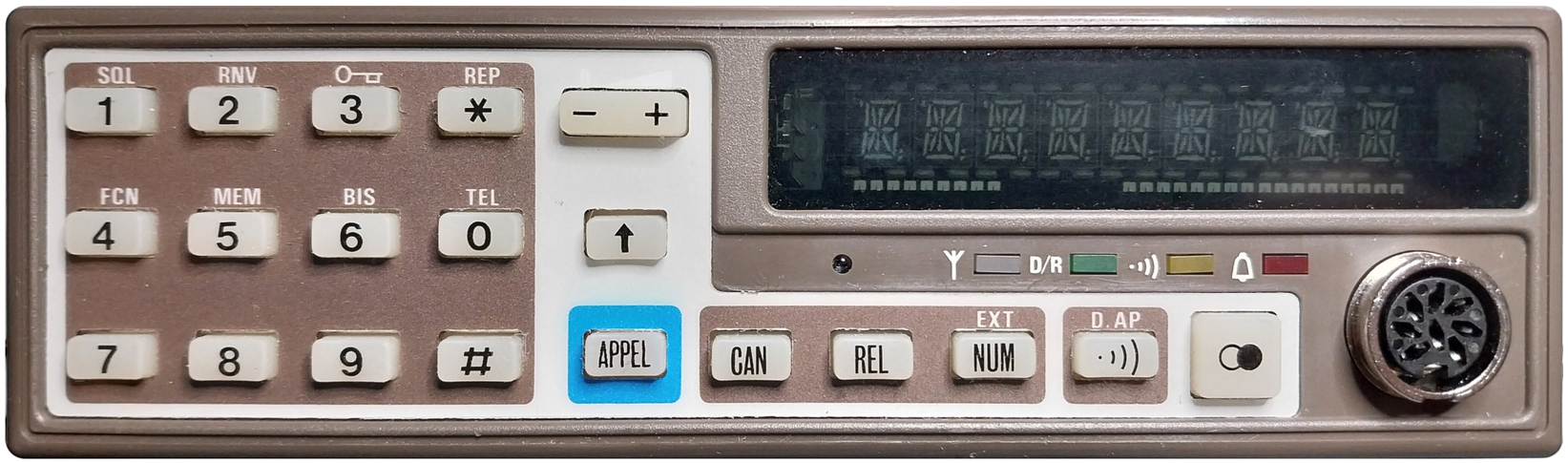
7.4 DGC C



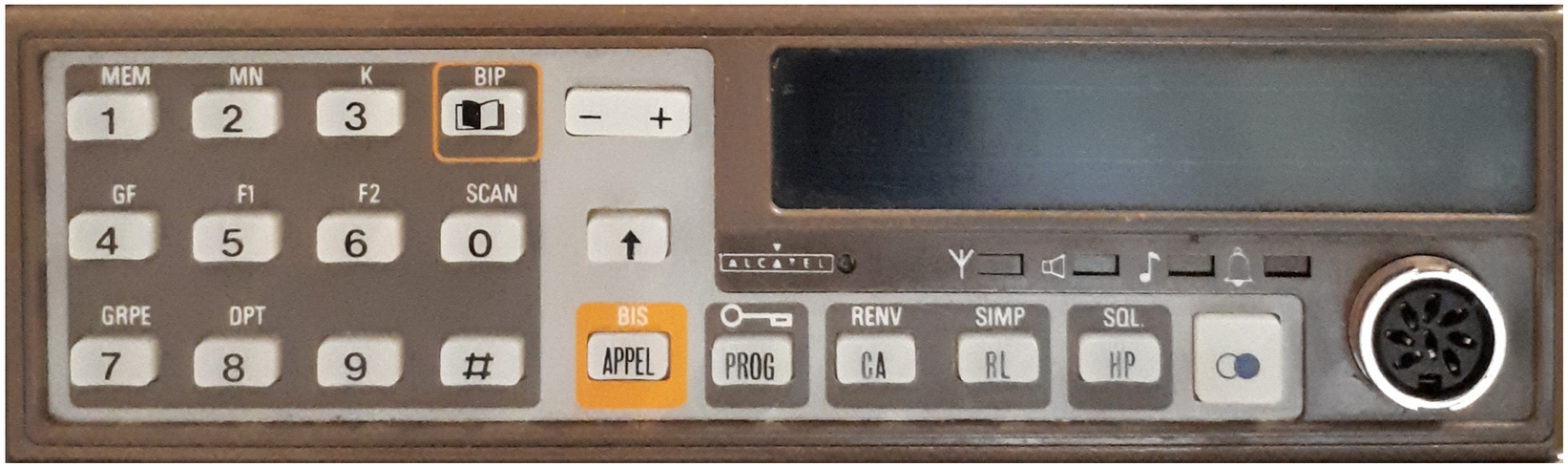
7.5 SC20 EDF 1



7.6 SC20 EDF 2

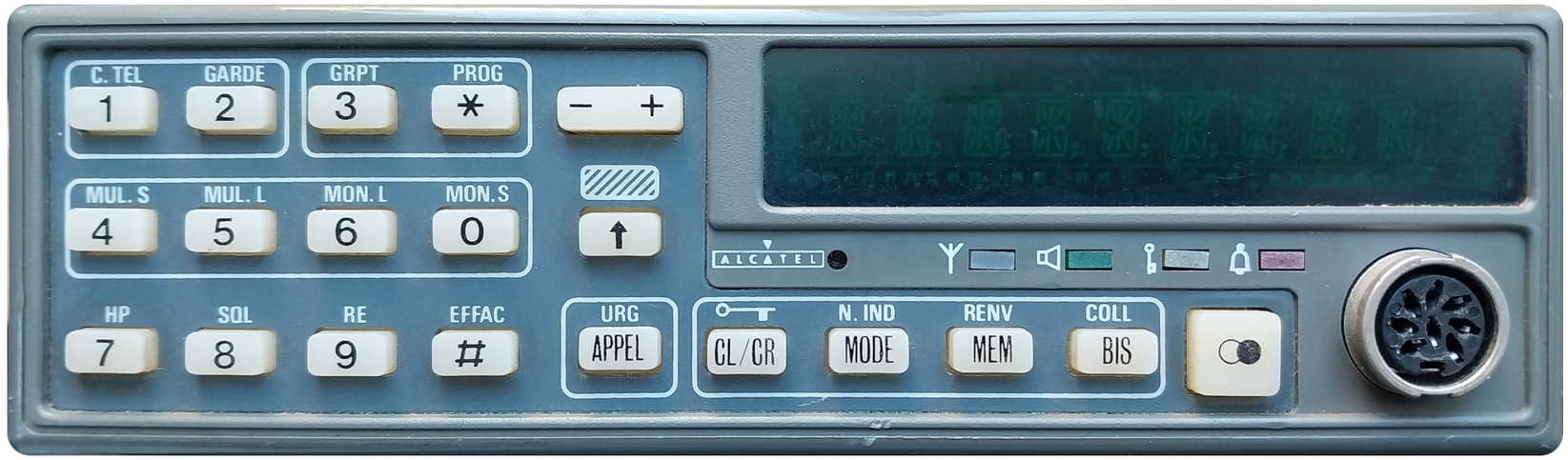


7.7 SC20 DDE



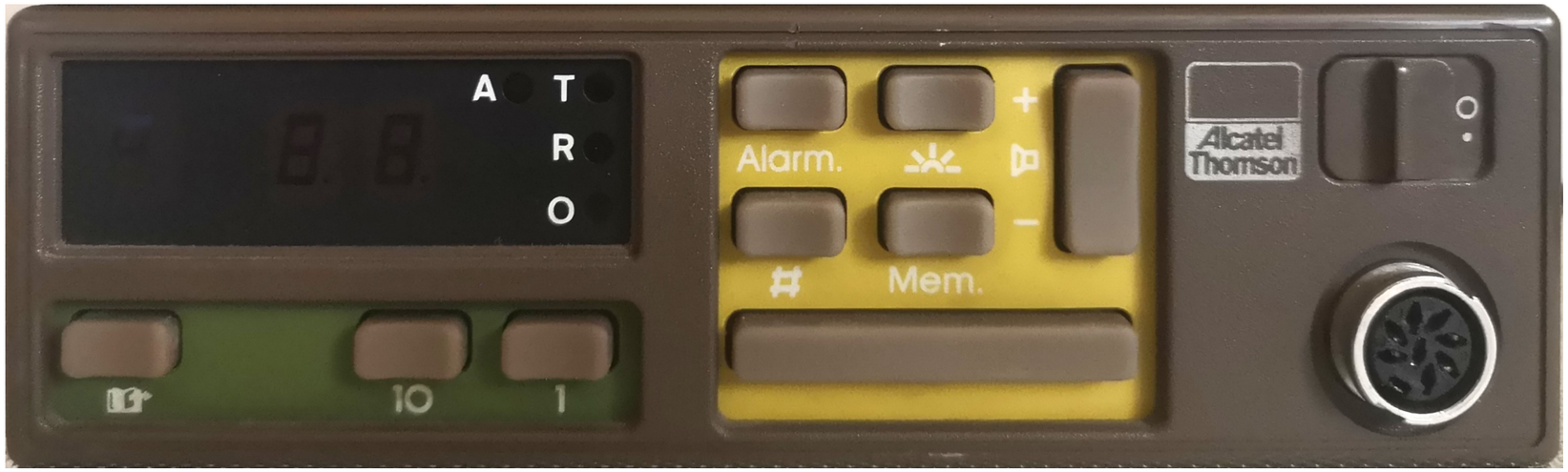
7.8 SC20 Pompier

7.9 SC20 Gendarmerie (Diamant)



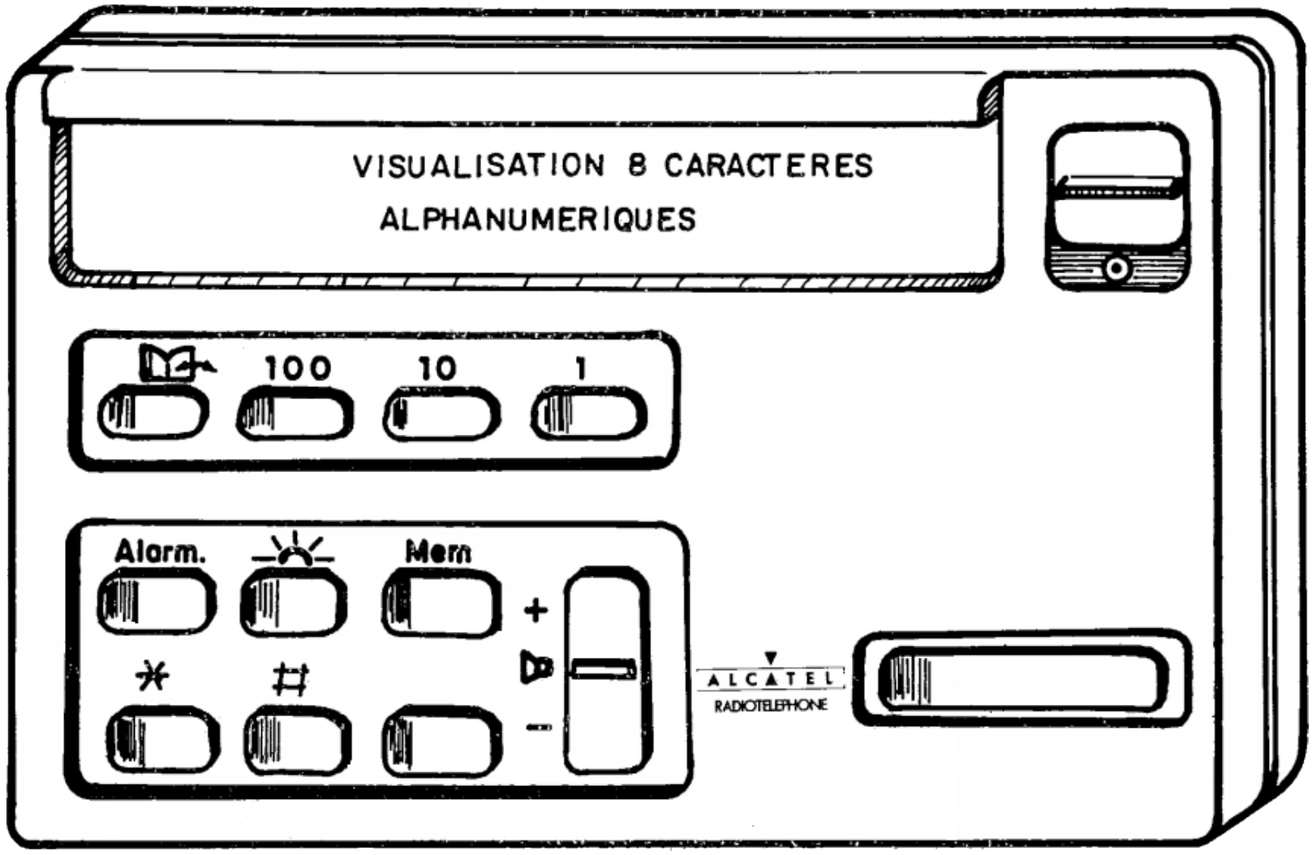
7.10 SC20 BUS

7.11 Mini10



7.12 Mini20 Clavier

7.13 Mini 20 Clavier standard



7.14 Base avec face avant Mini 20 / Clavier

7.15 Base avec face avant et applicatif Digicom

7.16 Microphone métallique 1 bouton (référence 20 124 706)

7.17 Microphone métallique 2 boutons (référence 20 133 543)

8 Liens externes

Cette analyse a été grandement simplifiée grâce aux fichiers mis gracieusement à disposition sur les sites mentionnés ci-dessous.

http://radiomods.free.fr/alcatel/
http://f5jtz.free.fr/sitef5fyu/pageposte/modificationdesradio.htm
http://f4bqn.free.fr/mods-ATR421.htm
http://f5ghp.pagesperso-orange.fr/html/atr_page.htm

D'autres sites mentionnent cette gamme de postes, mais sans fournir d'information jugée utile pour ma démarche :

http://f5jtz.free.fr/pjacquet/atr42x.html

9 Remerciements

Je remercie les membres du forum tsf70.com qui m'ont apporté l'aide nécessaire à la remise en état de marche de mon premier ATR423 : gagarine, Juju-4x4 et Megamix34.

Je remercie F4GKN de m'avoir transmis les binaires de ses EPROM montées sur des cartes de troisième génération. Ceci m'a permis de constater que le deux références de PLL qui peuvent être câblées sur MN01/HF se pilotent différemment et nécessitent par conséquent une EPROM de gestion et/ou de personnalisation spécifique(s). Je vais par la même occasion pouvoir m'atteler à la rétro ingénierie de cette génération de carte logique.
Je lui suis tout aussi reconnaissant pour les photos de ses équipements qu'il m'a transmises, et qui me permettent d'illustrer l'Annexe 1 de ce document.

Je remercie Tom pour le partage de copies numérisées de documents d'ALCATEL concernant les différents modèles d'ATR420 et 9210, et pour le don des postes de cette gamme qu'il possédait. Sauf erreur de ma part, aucun des documents contenus dans les fichiers compressés (extension «.rar ») n'était jusqu'ici disponible sur Internet !
Tout est classé, référencé, et accessible à cet emplacement : https://blog.shibby.fr/2017/10/alcatel-atr42x-la-resurrection/

Les copies d'EPROM récoltées sont regroupées à cet emplacement : https://blog.shibby.fr/wp-content/uploads/Images/Radio/Alcatel/ATR420/EPROM

Je remercie robert et Skaf du forum tetrahub.net, pour les informations partagées et leurs photos en rapport avec le MICA ici.