Visitons la Rom Monitoring

(1e partie) par André Chéramy et Claude Sittler

Nous allons analyser aujourd'hui une Rom qui incorpore un moniteur et des outils de déplombage. Cette Rom a été mise au point par Jean-Jacques Jung, un Oricien de la 1e heure.

Le Reset Système (Cold Start, F88F) a été dérouté : il appelle maintenant une routine simplifiée en F89A (il y manque le transfert de la table des vecteurs système en page 2). Le vecteur NMI, envoie directement à la routine F8B2 (Warm Start qui correspond aussi au bouton Reset) sans passer par la page 2 (en 0247). De même le vecteur IRQ, envoie directement à la routine EE22 sans passer par la page 2 (en 0244). Les 3 interruptions système sont donc maintenant protégées contre toute inhibition ou détournement. Le même type de prévention a été appliqué en C4B4 (001A, imprimer chaîne AY), C5E8 (023B, prendre un caractère au clavier), CCF4 (023E, vecteur imprimante), EE31 (024A, retour IRQ), F907 (0238, afficher caractère), FA01 (0238, afficher caractère), FFFA (0247, vecteur NMI) et FFFE (0244, vecteur IRQ).

Certaines commandes ont été modifiées. La commande CALL permet en option de fixer la valeur des registres A, X et Y avant de lancer le programme à l'adresse indiquée. Le démarrage automatique avec CLOAD a été bloqué. Les adresses de début et de fin du fichier chargé sont affichées. Les programmes chargés sont maintenant insensibles au Reset et aux POKE empoisonnés. C'est notamment le cas des CALL#F88F, POKE 26,1 et DOKE#247,1 qui restent sans effet.

La Rom comporte 8 nouvelles commandes (CLEAN, DES, DUMP, HDK, MOD, MON, MOVE et SEARCH), mais pour trouver de la place, certaines commandes ont été supprimées (CSAVE, EDIT, STORE, RECALL, TRON, TROFF, LLIST, LPRINT), ainsi que certaines caractéristiques (lettres minuscules et caractères alternés pour LORES).

Par rapport à ce qui se passe avec une Rom normale, la RAM est modifiée de B400 à B4FF (256 octets) et de B6D8 à B7FF (1192 octets) soit 1448 octets. Le clavier minuscule normal peut être chargé par la suite directement de B6D8 à B7FF.

Quelques fonctions secondaires ont été modifiées (défilement et reprise par SPC, sortie de fonction et retour au Basic par ESC, entrée des adresses et octets en hexadécimal et enfin le message «Ready» à été remplacé par «OK BOY» (idem pour certains autres messages qui contenaient des minuscules et ont été 'capitalisés').

Enfin, cette Rom a été construite à partir de la Rom 1.1 de 2e génération, que l'on peut trouver sur la disquette Sedoric v1.006 Cette Rom diffère de la 1e sur 3 points, comme il a été décrit dans le Ceo-Mag n°75-76 pages 18-19.

Voici maintenant une liste des modifications appliquées à la Rom v1.1 (2e génération) pour bâtir cette Rom Monitor. Cette liste respecte l'ordre des adresses de C000 vers FFFF, plutôt qu'un ordre logique. Par conséquent, pour suivre le travail des routines, il est parfois nécessaire de sauter d'un endroit à l'autre. Il aurait probablement été plus astucieux d'en faire l'exposé de manière plus logique en respectant le chaînage des routines. Mais notre travail a déjà été suffisamment compliqué comme ça, pour que nous ayons envie de vous servir un plat de spaghettis.

A) Table des adresses d'exécution située en C006-C089.

Les 8 commandes ci-dessous ont été supprimées pour libérer de la place et remplacée par 8 nouvelles commandes dont l'adresse d'exécution '-1' a été mise à jour.

En C008-C009 Adr de EDIT changée en C808 pour MON
En C00A-C00B Adr de STORE changée en E606 pour DUMP
En C00C-C00D Adr de RECALL changée en E62F pour SEARCH
En C00E-C00F Adr de TRON changée en F87B pour MOVE
En C010-C011 Adr TROFF changée en E91E pour CLEAN
En C022-C023 Adr de LLIST changée en FF67 pour HDK
En C024-C025 Adr de LPRINT changée en E66B pour MOD
En C074-C075 Adr CSAVE changée en EA60 pour DES

B) Table des mots-clés située en C08A-C2A7.

Le nom de 8 commandes a été modifié. Des noms plus courts ont parfois été utilisés, ce qui a permis de raccourcir la table de 9 octets. Cette place libérée a été réutilisée pour déplacer le message «BREAK», précédemment situé à la fin de la table des messages et donc pour libérer de la place dans cette dernière. Le bouleversement de la table des mots-clés est superficiel, car la plupart des noms de commandes ont seulement été décalés.

C0ED-C0F0 EDIT remplacé par MON en C0ED-C0EF
C0F1-C0F5 STORE remplacé par DUMP en C0F0-C0F3
C0F6-C0FB RECALL remplacé par SEARCH en C0F4-C0F9
C0FC-C0FF TRON remplacé par MOVE en C0FA-C0FD
C100-C104 TROFF remplacé par CLEAN en C0FE-C102
C105-C126 Les 8 Cdes suivantes décalées en C103-C124
C127-C12B LLIST remplacée par HDK en C125-C127
C12C-C131 LPRINT remplacée par MOD en C128-C12A
C132- C1DF Les 39 Cdes suivantes décalées en C12B-C1D8
C1E0-C1E4 CSAVE remplacée par DES en C1D9-C1DB
C1E5-C2A7 Les Cdes restantes décalées en C1DC-C29E
La table se termine par #00 en C29E au lieu de finir en C2A7.

C) Table de messages terminés par un #00.

Normalement située en C2A8-C3C5, elle commence maintenant en C29F. Dans la place dégagée ci-dessus, de C29F à C2A7, on trouve les 9 octets #00, #0D, #0A, #42, #52, #45, #41, #4B et #00 correspondant aux 2 messages suivant :

C29F «#00» bouche trou ou message nul.

C29A-C2A7 «Retour à la ligne, ligne suivante, 'BREAK' et #00". L'adresse de ce message a été ajustée en C98A-C98D où l'ancienne adresse C3BD a été remplacée par C2A0.

C3B2-C3C5 les anciens messages «Retour à la ligne, ligne suivante, 'Ready ' , retour à la ligne, ligne suivante et #00" (C3B2-C3BC) et «Retour à la ligne, ligne suivante, ' BREAK' et #00" (C3BD-C3C5) ont été remplacés par «Retour à la ligne, ligne suivante, ligne suivante, encre verte (escape B), 'OKAY BOY', retour à la ligne, ligne suivante, ligne suivante et #00" (C3B2-C3C2) et «Retour à la ligne, ligne suivante et #00» (C3C3-C3C5).

D) Prévention du détournement des vecteurs système

En C4B4-C4B6, le JSR 001A qui passe par la page zéro pour afficher «Ready» est remplacé par JSR CCB0 qui va directement à la routine en ROM 'Affichage chaîne pointée

par AY'. Impossible donc de détourner le Ready, une 'protection' courante qui empêchait de reprendre la main.

En C5E8-C5EA, le JSR 023B qui passe par la page deux pour prendre un caractère au clavier est remplacé par JSR EB78 qui va directement à cette routine en ROM. Impossible donc de détourner cette fonction maintenant.

Le même type de prévention a été appliqué en CCF4 (023E, vecteur imprimante), EE31 (024A, retour IRQ), F907 (0238, afficher caractère), FA01 (0238, afficher caractère), FFFA (0247, vecteur NMI) et FFFE (0244, vecteur IRQ).

E) Ancienne commande EDIT en C692-C6B2

a) Neutralisation de la commande EDIT

C692- 60 RTS retourne si la commande EDIT est appelée par langage machine.

b) Nouvelle routine 'Saisit un caractère au clavier, le teste et l'écrit'. Cette routine est appelée par la nouvelle commande MOD à la place de la routine homologue située en C592 dans la Rom normale («Saisir un caractère et le mettre dans le tampon clavier») afin de la compléter.

C693- A2 00 LDX #00 initialise le compteur de caractères entrés
C695- 20 E8 C5 JSR C5E8 saisit dans A un caractère au clavier (teste si CTRL/O)
C698- C9 20 CMP #20 est-ce 'espace' ?
C69A- F0 0A BEQ C6A6 si oui, continue en C6A6
C69C- C9 1B CMP #1B est-ce 'ESC' ?
C69E- F0 09 BEQ C6A9 si oui, continue en C6A9
C6A0- 20 97 C5 JSR C597 si non, reprise normale de la routine «Saisir un caractère et le mettre dans le tampon clavier». CTRL/A permet de recopier les caractères sous-jacents. La touche 'Return' permet de valider. 'Espace' permet de conserver l'octet et passer à l'adresse suivante. 'ESC' permet de sortir de la commande MOD.
C6A3- 4C 82 E6 JMP **E682** et finalement le copie à l'adresse pointée
C6A6- 4C 8C E6 JMP **E68C** incrémente 33-34 et reboucle dans la commande MOD
C6A9- 4C A8 C4 JMP C4A8 retourne à l'interpréteur

Le reste du code de l'ancienne commande EDIT en C6AC-C6B2 est inchangé (résidu).

F) Ancienne commande LPRINT située en C809-C815.

Nouvelle entrée pour la commande MON

Syntaxe : Mettre en 0280 l'adresse du code à exécuter (par un DEEK ou une routine en langage machine) et taper MON. Cette commande est donc réduite à sa plus simple expression, mais elle est plus souple que CALL, car permet un adressage indirect.

C809- 6C 80 02 JMP (0280) exécute où pointe 0280

Le reste du code de l'ancienne commande LPRINT en C80C-C815 est inchangé (résidu).

G) Modification de la commande END en C973-C99F.

En C9BA-C9BD le LDA#A0 et LDY#C2 (AY pointe maintenant sur C2A0, le nouvel emplacement du message 'BREAK'). Le reste de l'ancienne routine END est inchangé.

H) Modifications de la routine 'Afficher le caractère dans A' située en CCEE-CD12.

En CCF4-CCF6 le JSR 023E (vecteur imprimante) pointe maintenant directement en F5C1 adresse réelle de la routine en ROM. Le reste de l'ancienne routine est inchangé.

Le même type de prévention a été appliqué en C4B4 (001A, imprimer chaîne AY), C5E8 (023B, prendre un caractère au clavier), EE31 (024A, retour IRQ), F907 (0238, afficher caractère), FA01 (0238, afficher caractère), FFFA (0247, vecteur NMI) et FFFE (0244, vecteur IRQ).

I) Anciennes Cdes TRON et TROFF en CD16-CD1E.

Nouvelle routine «Affiche X espaces» X doit être correctement initialisé à l'entrée (non nul).

CD16- 20 D4 CC JSR CCD4 affiche un espace
CD19- CA DEX décrémente le compteur
CD1A- D0 FA BNE **CD16** reboucle si pas fini
CD1C- 60 RTS sinon retourne avec X=0

Le reste de l'ancienne routine TROFF est inchangé.

J) Table des messages de chargement K7 en E50B-E56B.

Les lettres sont maintenant en majuscules et les couleurs d'affichage ont été modifiées.

E50B-E519 Message «Papier noir, encre rouge, 'SEARCHING ..' et #00"

E51A-E526 Message «Papier noir, encre rouge, 'LOADING ..' et #00"

E527-E537 Message «ligne suivante, retour à la ligne, «ERRORS FOUND», retour à la ligne, ligne suivante et #00"

E538-E542 Message «Papier noir, encre verte, 'FOUND ..' et #00"

E543-E551 Message «Papier noir, encre cyan, 'VERIFYING ..' et #00"

E552-E56B Message «' VERIFY ERRORS DETECDED', retour à la ligne, ligne suivante et #00" (avec une faute).

K) Amélioration du code de la routine «Afficher 'Searching ..'» située en E57D-E584.

E581-E584 le JSR E5EA + RTS a été judicieusement remplacé par un JMP E5EA. L'octet récupéré est immédiatement utilisé dans la routine suivante.

L) Récupération de la zone de l'ancienne routine «Afficher 'Saving ..' + nom» en E585-E593.

La nouvelle routine «Incrémente l'adresse en 02-03 et teste si la fin de la zone pointée par l'adresse en 33-34 est atteinte». Retourne avec C=0 si pas fini. Elle est appelée par SEARCH, CLEAN et MOVE.

E584- E6 02 INC 02 incrémente LL
E586- D0 02 BNE E58A teste si LL atteint #00
E588- E6 03 INC 03 si oui, reporte retenue sur HH
E58A- 38 SEC prépare 2 soustractions
E58B- A5 02 LDA 02
E58D- E5 33 SBC 33
E58F- A5 03 LDA 03 en sortie, on aura C=0 si
E591- E5 34 SBC 34 l'adresse pointée en 02-03
E593- 60 RTS est inférieure à l'adresse pointée en 33-34

à suivre...