PATRICK GUEULLE

# Cartes à puce

## INITIATION ET APPLICATIONS




NOUVEAU

CD-ROM INCLUS

ETSF

EDITIONS TECHNIQUES ET SCIENTIFIQUES FRANÇAISES

PATRICK GUEULLE

CARTES À PUCE

ETSF

# CARTES À PUCE

## *Série électronique et informatique*

**Philippe André,**
- *La Liaison série RS232 (cédérom inclus)*

**Michaël Bairanzadé,**
- *Initiation au microcontrôleur 68HC11 (disquette incluse)*

**Michel Croquet,**
- *PC et robotique (disquette incluse)*

**Patrick Gueulle,**
- *BASIC pour microcontrôleurs et PC (cédérom inclus)*
- *Cartes à puce (cédérom inclus)*
- *Cartes magnétiques et PC (disquette incluse)*
- *Composants électroniques programmables sur PC (disquette incluse)*
- *Montages à composants électroniques programmables (téléchargement de fichiers depuis le web)*
- *Instrumentation virtuelle sur PC (disquette incluse)*
- *Logiciels PC pour l'électronique (cédérom inclus)*
- *PC et cartes à puces (disquette incluse)*
- *Téléphones portables et PC (cédérom inclus)*

**É. Larchevêque / L. Lellu,**
- *Montages avancés pour PC (disquette incluse)*

**Marc Laury,**
- *Le Microcontrôleur ST623X (disquette incluse)*

**Pascal Morin,**
- *Le Bus I2C par la pratique (disquette incluse)*
- *Mise en œuvre du 8052 AH BASIC (disquette incluse)*

**Patrice Oguic,**
- *Interfaces PC (disquette incluse)*
- *Mesures et PC (téléchargement de fichiers depuis le web)*
- *Moteurs pas-à-pas et PC (téléchargement de fichiers depuis le web)*
- *PC et domotique (disquette incluse)*
- *PC et télémesures (disquette incluse)*

**Éric Quagliozzi,**
- *Pratique du microcontrôleur ST622X (disquette incluse)*

**Bernard Schaffner,**
- *Montages électroniques pour PC (disquette incluse)*

PATRICK GUEULLE

Ingénieur EFREI

# CARTES À PUCE

## Initiation et applications

**2e édition**

**Nouvelle présentation**

ETSF

EDITIONS TECHNIQUES ET SCIENTIFIQUES FRANÇAISES

# Consultez nos catalogues sur le Web

http://www.dunod.com




**C**e pictogramme mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du **photocopillage**.

Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.




Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation du Centre français d'exploitation du droit de copie (**CFC**, 20 rue des Grands-Augustins, 75006 Paris).

© DUNOD, Paris, 2001 pour la nouvelle présentation

© DUNOD, Paris, 1998, 2ème édition

© ETSF, Paris, 1993, 1ère édition


ISBN 2 10 005736 7

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droits ou ayants cause est illicite selon le Code de la propriété intellectuelle (Art L 122-4) et constitue une contrefaçon réprimée par le Code pénal. Seules sont autorisées (Art L 122-5) les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, ainsi que les analyses et courtes citations justifiées par le caractère critique, pédagogique ou d'information de l'œuvre à laquelle elles sont incorporées, sous réserve, toutefois, du respect des dispositions des articles L 122-10 à L 122-12 du même Code, relatives à la reproduction par reprographie.

# TABLE DES MATIÈRES


| | | |
|---|---|---|
| | Avant-propos | VII |
| | Avertissement | IX |
| CHAPITRE | | |
| 1 | **Vocabulaire et normalisation** | 1 |
| | Qu'est-ce qu'une carte à puce ? | 2 |
| | Les cartes à mémoire | 3 |
| | Les cartes à microprocesseur | 4 |
| | Les « objets portables » à mémoire | 5 |
| | Les cartes et objets sans contact | 6 |
| | Les normes dimensionnelles | 7 |
| | Position des contacts et brochages | 7 |
| | Les échanges de données | 11 |
| 2 | **Les circuits intégrés pour cartes à puce** | 13 |
| | Les composants spécialisés | 14 |
| | Les circuits intégrés apparentés | 28 |
| | Le protocole I2C | 31 |
| | Les micromodules | 33 |
| 3 | **La périphérie des cartes** | 37 |
| | Un cordon universel | 38 |
| | Les connecteurs de cartes | 40 |
| | « Fausses cartes » en époxy | 42 |
| | Petit adaptateur de brochage | 45 |
| | Une sonde logique pour cartes à puce | 46 |
| | Les interfaces de cartes | 48 |
| | Mise en œuvre du TDA 8000 | 49 |
| | Schéma d'application | 56 |
| | Les coupleurs de cartes | 56 |
| | Les lecteurs de cartes à puce | 58 |
| | Deux alimentations 21 V pour cartes à puce | 60 |
| | Un convertisseur 5 à 12 V/21 V à découpage | 61 |
| | Un convertisseur 10 V/21 V à pompe de charge | 64 |
| | Réalisation pratique | 65 |
| 4 | **Mise en œuvre des cartes synchrones** | 67 |
| | Un lecteur encodeur de « 1re génération » | 68 |


© DUNOD - La photocopie non autorisée est un délit.

| | | |
|---|---|---|
| | Un logiciel pour T1G et GPM 256 | 72 |
| | Un logiciel intégré pour télécartes | 76 |
| | Un lecteur-encodeur de « 2e génération » | 80 |
| | Un logiciel pour télécartes « européennes » | 82 |
| | Un logiciel pour T2G et cartes apparentées | 87 |
| | Lecture des GPM416 | 89 |
| | Lecture des GPM 896 | 93 |
| | Les cartes à puce I2C | 97 |
| | Réalisation d'une « fausse carte » à puce I2C | 102 |
| 5 | **Applications pratiques des cartes synchrones** | 105 |
| | Un testeur autonome de télécartes | 106 |
| | Une serrure de sûreté à télécarte | 113 |
| | Un destructeur de cartes à puce | 118 |
| 6 | **Introduction aux cartes asynchrones** | 125 |
| | La structure des cartes asynchrones | 127 |
| | Un lecteur-encodeur simplifié | 128 |
| | Réalisation pratique | 130 |
| | Le logiciel embarqué | 130 |
| | Lecture de la réponse au RESET | 137 |
| | Décodage de la réponse au RESET | 143 |
| | Le dialogue avec les cartes | 146 |
| | Exemples pratiques | 154 |
| 7 | **Le cédérom du livre** | 157 |

# AVANT-PROPOS

Parmi les applications spectaculaires de l'électronique en cette fin du XX$^{e}$ siècle, c'est peut-être la carte à puce qui concerne le plus chacun d'entre nous dans sa vie courante.

Pour le commun des mortels, la carte à puce est un nouveau «sésame» qui, auréolé d'un indéniable mystère, commence à remplacer les clefs et la monnaie.

Pour l'électronicien, c'est en plus un inépuisable sujet de curiosité et d'expérimentation, mais finalement aussi une famille de composants électroniques particulièrement riche d'applications, à laquelle il est parfaitement légitime de s'intéresser.

Cela d'autant plus que les principaux brevets protégeant l'idée tombent les uns après les autres dans le domaine public...

Au-delà des réticences initiales et bien compréhensibles des pionniers de ces techniques, il est maintenant prouvé qu'il n'y a pas d'inconvénient à dévoiler les mécanismes permettant de lire et écrire dans les cartes à puce de toutes sortes.

La sécurité de ces véritables «forteresses électroniques» que peuvent et doivent être les cartes dédiées aux applications les plus «sensibles» repose en effet sur des mécanismes internes qui, sauf négligences graves, bénéficient d'une protection quasiment absolue.

Après une indispensable initiation au vocabulaire et aux normes en vigueur dans le monde des cartes à puce, ce livre vous apprendra à lire et écrire dans les principales familles de cartes, puis à mettre sur pied de véritables applications pratiques.

L'auteur souhaite à ses lecteurs de prendre à cette découverte autant de plaisir qu'il en a lui-même éprouvé en explorant cette branche particulièrement passionnante de l'électronique moderne !

# AVERTISSEMENT

Tous les circuits imprimés de ce livre ont été dessinés sur un micro-ordinateur compatible PC, muni du logiciel BOARDMAKER.

Nos lecteurs intéressés par ce produit en trouveront une version limitée mais parfaitement fonctionnelle sur le CD-ROM accompagnant cet ouvrage.

Ils pourront ainsi, s'ils le souhaitent, modifier à leur gré les tracés d'origine puis les réimprimer à l'échelle de leur choix.

L'auteur tient à remercier ici les éditeurs et importateurs de BOARDMAKER pour leur aimable collaboration.

Sincères remerciements aussi à GEMPLUS CARD INTERNATIONAL, au CNET de Caen (anciennement SEPT), à STMicroelectronics (anciennement SGS-THOMSON), PHILIPS SEMICONDUCTORS, INFINEON (anciennement SIEMENS), SEFEA, COREL ELECTRONIQUE, ITT-CANNON, MICROCHIP, ATMEL, et plus généralement à tous ceux dont l'aide nous a été précieuse pour mener à bien ce travail.

Rappelons enfin que les montages décrits dans ces pages ne doivent être réalisés et utilisés qu'à des fins expérimentales ou personnelles, à l'exclusion de toute exploitation commerciale ou industrielle.

Pour toute demande de licence des brevets INNOVATRON, il conviendrait de s'adresser à :

INNOVATRON, 1 rue Danton, 75006 PARIS.

CHAPITRE PAGE

# 1 VOCABULAIRE ET NORMALISATION


**Qu'est-ce qu'une carte à puce** 2
**Les cartes à mémoire** 3
**Les cartes à microprocesseur** 4
**Les « objets portables » à mémoire** 5
**Les cartes et objets sans contact** 6
**Les normes dimensionnelles** 7
**Position des contacts et brochages** 7
**Les échanges de données** 11

| | | |
|---|---|---|
| 2 | Les circuits intégrés pour cartes à puce | 13 |
| 3 | La périphérie des cartes | 37 |
| 4 | Mise en œuvre des cartes synchrones | 67 |
| 5 | Applications pratiques des cartes synchrones | 105 |
| 6 | Introduction aux cartes asynchrones | 125 |
| 7 | Le cédérom du livre | 157 |

Le monde fascinant des cartes à puce possède naturellement son vocabulaire spécifique (oserons nous dire son jargon ?) qu'il importe de connaître pour prétendre y accéder.

Parallèlement, les principaux acteurs de cette véritable révolution technologique ont su se mettre d'accord, sous l'égide des organismes internationaux compétents, pour définir très tôt des normes garantissant un niveau satisfaisant de compatibilité entre produits, sans pour autant figer une évolution toujours très active.

## QU'EST-CE QU'UNE CARTE À PUCE ?

Dans l'état actuel des choses, une carte à puce (ou carte à microcircuit) est une carte en matière plastique épousant les mêmes dimensions que les cartes à pistes magnétiques (cartes de crédit par exemple).

L'innovation consiste à loger dans l'épaisseur habituelle de la carte, un ou plusieurs circuits intégrés et un connecteur plat capable d'assurer la liaison électrique avec un « lecteur » spécial.

On appelle « micromodule » le très mince circuit imprimé qui accueille, sur sa face apparente, les contacts du connecteur, et au dos duquel est montée la puce de silicium (technologie dite *Chip On Board* ).

Comme il reste beaucoup de place disponible autour du micromodule, il n'est toutefois pas évident que ce choix dimensionnel soit le meilleur, et on songe à en définir de nouveaux.

Des cartes « transformables » ont même déjà été imaginées : il s'agit de cartes à puce au format habituel, mais prédécoupées autour du micromodule selon les dimensions d'une carte miniaturisée.

Les cartes à puce se distinguent surtout les unes des autres par les fonctionnalités de leur micromodule, autrement dit de leur circuit intégré interne.

On peut distinguer trois grandes familles de cartes à puce :

– les cartes à mémoire simple ;
– les cartes à mémoire personnalisée ;
– les cartes à microprocesseur.

## LES CARTES À MÉMOIRE

### Les cartes à mémoire simple

Comme son nom l'indique, une carte à mémoire simple renferme seulement une certaine quantité de mémoire, sans aucune protection particulière. Cela signifie que n'importe qui peut y lire ou y écrire des informations à l'aide d'un équipement approprié, librement disponible dans le commerce ou même souvent très simple à construire par ses propres moyens. Nous y reviendrons !

La plupart des cartes à mémoire simple sont réalisées en technologie EEPROM, et sont donc recyclables (effaçables et réinscriptibles). Leur capacité est généralement de l'ordre de quelques kilobits, voire quelques dizaines.

Ces cartes sont en principe destinées à des applications n'ayant pas à être sécurisées : fichier portable non secret, cartes de suivi de production…

### Les cartes à mémoire personnalisée

En revanche, pour mériter l'appellation de « carte à mémoire personnalisée », une carte à puce doit contenir au moins l'un des quatre systèmes de protection suivants, réalisés en logique câblée sans le secours d'aucun microprocesseur :

- zone protégée en écriture après destruction d'un fusible ;
- zone protégée en lecture et écriture par un « code porteur » (code confidentiel dit « PIN » ou *Personal Identification Number*), le porteur étant défini comme l'utilisateur final de la carte ;
- blocage de la carte au bout d'un nombre donné de présentations d'un PIN erroné ;
- protection par un « code émetteur » (l'émetteur étant l'organisme qui délivre les cartes et décide de leur contenu).

Deux technologies coexistent dans cette famille : EPROM « OTP » ineffaçable puisque la puce est enfermée dans un enrobage opaque aux ultraviolets, et EEPROM effaçable puis reprogrammable.

Les capacités disponibles sont généralement inférieures à 1 kilobit.

© DUNOD - La photocopie non autorisée est un délit.

Le pionnier de cette famille est la TÉLÉCARTE, suivie maintenant par d'autres applications comme la CINÉ-CARTE, la carte PIAF (parcmètre personnel), la carte de lavage de voitures de BP et MOBIL…

C'est la « carte à jetons » par excellence, contenant des « unités » prépayées et qu'on jette (ou collectionne !) quand elle est épuisée.

Relativement bien protégée contre la fraude, elle reste cependant fort simple à lire et à programmer.

Les cartes un peu plus perfectionnées permettent d'envisager des applications exigeant à la fois une meilleure sécurité et de fréquentes mises à jour d'informations : cartes prépayées rechargeables, porte-monnaie électronique simple, contrôle d'accès, dossier portable sécurisé, carte d'abonnement, cartes de fidélité.

## LES CARTES À MICROPROCESSEUR

La carte à microprocesseur (dite aussi à microcalculateur) est évidemment le *nec-plus-ultra* en matière de cartes à puce : véritable micro-ordinateur, elle rassemble une unité centrale, des mémoires de programme et des mémoires de données spécialement agencées.

Produit informatique à part entière, elle contient plusieurs systèmes de protection :

- zone protégée en écriture ou en écriture et lecture par un code secret émetteur, ceci après personnalisation par l'émetteur ;
- zone protégée en lecture et écriture par un code secret porteur (PIN) ;
- blocage de la carte après présentation d'un nombre donné de codes secrets erronés, mais avec possibilité de réhabilitation par l'organisme émetteur ;
- mise en ouvre d'algorithmes cryptographiques (par exemple DES ou RSA) pour assurer la sécurité des transferts de données.

Il existe des cartes à microprocesseur monoservice dédiées à une seule application, et des cartes multiservices permettant la cohabitation de zones applicatives complètement indépendantes les unes des autres, pouvant même héberger du code programme spécifique.



© DUNOD - La photocopie non autorisée est un délit.

La plupart des cartes à microprocesseur sont supportées par un puissant système d'exploitation appelé, par exemple, « COS » (*Chip Operating System* ou *Card Operating System*) par analogie avec le « DOS » (*Disk Operating System*) des PC.

Il s'agit d'un logiciel « masqué » en ROM et dont les caractéristiques sont les suivantes :

- organisation de la mémoire en zones banalisées, protégées ou non ;
- gestion dynamique de l'espace mémoire ;
- gestion des codes confidentiels ;
- chargement éventuel de sous-programmes spécifiques à l'application, lors de la personnalisation.

Le développeur d'applications peut utiliser le COS tel quel, ou rajouter ses sous-programmes personnels dans l'EPROM ou l'EEPROM, ou encore concevoir un masque ROM spécifique reprenant tout ou partie du COS.

Ces cartes conviennent aux applications les plus « sensibles » : carte bancaire, carte santé, cartes de TV à péage, contrôle d'accès sécurisé, monoservice ou multiservices.

## LES « OBJETS PORTABLES » À MÉMOIRE

À côté des familles « classiques » de cartes que nous venons de définir, il ne pouvait pas ne pas apparaître quelques technologies originales. Elles méritent assurément tout notre intérêt !

Bien que spécialement conçus pour être encartés, les micromodules munis de mémoires ou de microprocesseurs peuvent en effet avantageusement être montés sur d'autres supports. Par exemple, une clef en matière plastique aux dimensions d'une « serrure » spéciale munie d'un connecteur approprié.

C'est ce que proposent notamment SEFEA et GEMPLUS, et qu'on rencontre sur certains décodeurs de télévision à péage particulièrement répandus.

Outre une esthétique originale, le principal avantage de cette présentation est la robustesse de la clef, très supérieure à celle d'une carte.

De plus, le problème des licences de brevets se pose sans doute différemment puisqu'il n'y a plus de carte au sens strict du terme.

## LES CARTES ET OBJETS SANS CONTACT

Le principe « à contacts » de la carte à puce traditionnelle constitue un handicap, et parfois même un vice rédhibitoire, pour bon nombre d'applications potentielles.

La carte à puce telle que nous la connaissons est en effet tributaire de toute une connectique pour son alimentation et ses échanges de données.

Outre les problèmes de fiabilité que cela peut poser (pollution et usure des contacts, vulnérabilité des lecteurs), ce principe exclut d'emblée de nombreuses familles d'applications.

Même s'il serait certainement mal accepté qu'une carte de paiement puisse être débitée sans un geste volontaire de son titulaire (l'équivalent, en somme, de sa « signature »), les avantages d'un dialogue à distance sont innombrables.

Débarrassée de ses contacts, la carte à puce peut gagner énormément en robustesse, et donc affronter les pires environnements : intempéries, eau de mer, hautes températures, produits chimiques... C'est particulièrement appréciable en milieu industriel et en extérieur (applications automobiles, marines ou sportives, par exemple).

Mais une possibilité de dialogue sans contact à une certaine distance permet aussi d'envisager des transactions « au vol » : identification de personnes passant simplement à travers une porte ouverte, reconnaissance de véhicules traversant un poste de péage sans même s'arrêter, gestion de pièces sur une chaîne de fabrication, marquage inviolable d'équipements donnés en location, ou même tatouage électronique d'animaux vivants.

Des dispositifs connus sous le nom de « transpondeurs » existent depuis longtemps déjà avec des fonctionnalités de ce type, et sont couramment employés dans l'industrie et les transports.

Il s'agissait à l'origine d'équipements coûteux et relativement encombrants, qu'il n'aurait pu être question d'intégrer dans une carte plastique de format standard, surtout en épaisseur.

La miniaturisation constante des composants et la diminution de leur consommation permet maintenant d'envisager la réalisation de dispositifs dotés de mémoires non



© DUNOD - La photocopie non autorisée est un délit.

volatiles, et capables de dialoguer avec un lecteur spécifique distant de quelques centimètres à près d'un mètre.

Ce lecteur pouvant fort bien téléalimenter la « puce » par induction, l'absence de pile dans le badge constitue un avantage déterminant sur le plan de la fiabilité et de la compacité.

Mais la technique à mettre en œuvre est délicate malgré la simplicité de son principe. Des procédés de modulation et de supervision fort élaborés sont nécessaires pour garantir le très haut degré de sûreté que l'on exige dans les applications visées.

L'apparition de composants spécialement développés pour cet usage permet cependant de penser que, dans peu d'années, les cartes à puce sans contact seront présentes dans pratiquement toutes nos poches...

## LES NORMES DIMENSIONNELLES

Nous avons vu que les cartes à puce normalisées épousent les dimensions des cartes à pistes magnétiques ou simplement « embossées » : environ 85 mm × 54 mm, pour 0,76 mm d'épaisseur.

Cependant, les actuels connecteurs se révélant beaucoup trop encombrants pour tenir dans certains équipements à carte, il a été imaginé de créer une carte à puce miniature en éliminant l'essentiel de la surface inutilisée autour du micromodule.

On arrive ainsi à une carte plus petite qu'un timbre-poste, dite SIMCARD, essentiellement utilisée dans les téléphones portables GSM.

## POSITION DES CONTACTS ET BROCHAGES

Bien entendu, des normes ont aussi été édictées pour standardiser autant que possible la connectique des cartes et des lecteurs.

La carte à puce étant une invention française, les développements les plus anciens (télécarte, carte bancaire, etc.) ont appliqué la norme « AFNOR », dite « à contacts excentrés », que décrit la figure 1.1.

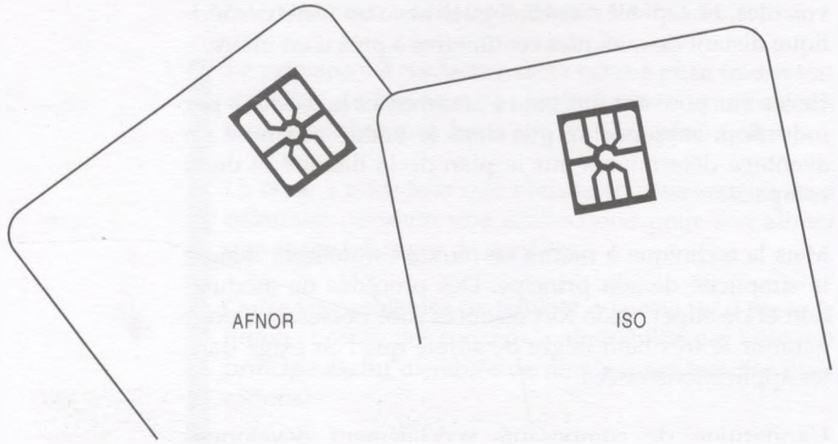
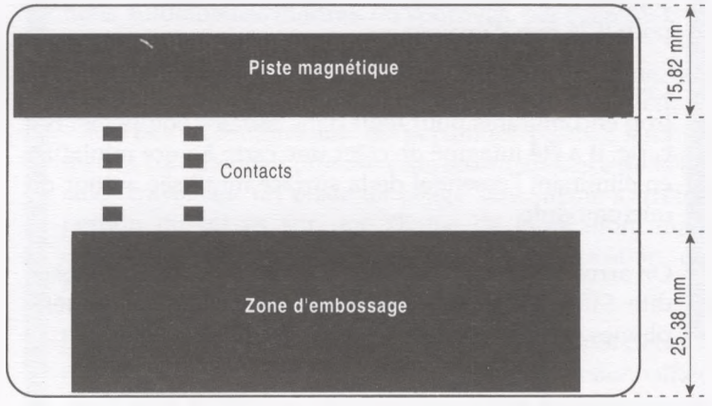



**Figure 1.1.** Les deux positions normalisées des puces.

Puis sont apparues les normes internationales ISO 7816, définissant un positionnement « centré » des contacts du micromodule, avec, de surcroît, une rotation de 180°.

**Figure 1.2.** Affectation des différentes zones des cartes.




La figure 1.2 apporte une justification technique à cette évolution qui s'applique petit à petit à toutes les cartes, même si cela doit entraîner la modification des matériels existants. La disposition « ISO » place en effet le micromodule entre la zone dévolue (au *verso*) aux pistes magnétiques, et celle réservée (au *recto*) à l'embossage de textes pouvant être imprimés sur une facturette à l'aide d'un « fer à repasser » de commerçant.





En pratique, il n'est pourtant pas impossible de faire coexister un micromodule et des pistes magnétiques dans la même zone, comme ce fut un moment le cas sur les cartes de crédit VISA. Cela obligeait, il est vrai, à soigner tout particulièrement l'opération d'encartage.

Dans ce cas particulier, d'ailleurs, la position ISO ne présentait aucun avantage puisqu'un micromodule « centré » serait encore tombé en face de la piste « T2 », maintenant abandonnée, comme le montre la figure 1.3.

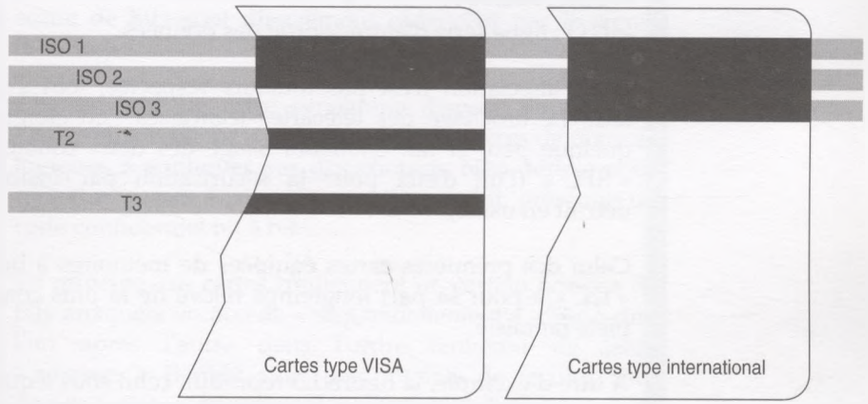



**Figure 1.3.** Positions normalisées des pistes magnétiques.

Cela étant posé, la norme définit aussi le brochage des micromodules, qui peuvent comporter jusqu'à huit contacts disposés selon la figure 1.4.

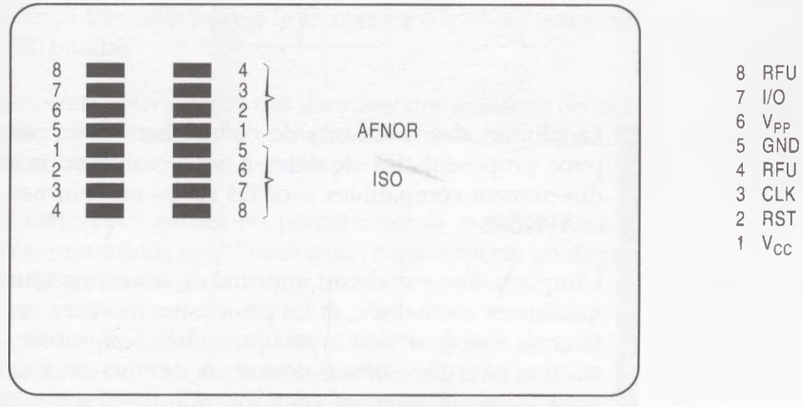



**Figure 1.4.** Brochage des micromodules.

© DUNOD - La photocopie non autorisée est un délit.

Deux de ces contacts étant « Réservés pour de Futurs Usages » (RFU), il n'est pas rare de rencontrer des micromodules à six contacts seulement.

Les six accès essentiels à la puce sont en effet les suivants :

- GND : masse électrique ;
- Vcc : alimentation de la puce (en général + 5 volts) ;
- Vpp : tension de programmation (pas toujours nécessaire) ;
- RST : remise à zéro de la carte (RESET) ;
- CLK : horloge ;
- I/O : ligne série d'entrée-sortie des données.

Cette affectation n'est pas toujours respectée, loin s'en faut. Le brochage des télécartes françaises s'en éloigne quelque peu, et fait d'ailleurs usage des deux contacts « RFU » (l'un d'eux pour la sécurisation par fusible détruit en usine).

Celui des premières cartes équipées de mémoires à bus « I2C » a pour sa part longtemps relevé de la plus complète fantaisie.

À titre d'exemple, la figure 1.5 reproduit celui sous lequel on a un moment encarté les circuits intégrés 24C02 et 24C04, totalement différent d'ailleurs de celui des cartes à puce I2C de PHILIPS !

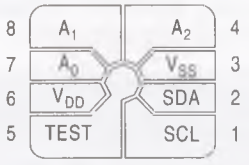



**Figure 1.5.**
Ancien brochage de micromodule à puce I2C.

La plupart des fabricants de connecteurs pour cartes à puce proposent des modèles à seize contacts, et donc directement compatibles avec les cartes aux normes ISO et AFNOR.

L'implantation sur circuit imprimé de ces connecteurs est quasiment normalisée, et les principaux modèles des différentes marques sont à peu près interchangeables, abstraction faite des contacts détecteurs de « présence carte » dont le positionnement et la fonction électrique varient quelque peu.



© DUNOD - La photocopie non autorisée est un délit.

## LES ÉCHANGES DE DONNÉES

Un seul contact (plus exceptionnellement un « RFU ») étant affecté aux données émises et reçues par la carte, il est clair que la transmission de celles-ci doit se faire en série, c'est-à-dire un bit après l'autre.

On peut distinguer deux familles de cartes, respectivement baptisées synchrones et asynchrones.

Les cartes à mémoire simple ou sécurisée sont normalement du type synchrone, ce qui signifie que l'entrée et la sortie de bits sont directement cadencées par le signal d'horloge.

Chaque type de carte synchrone dispose d'un jeu de « micro-instructions », séquences particulières de niveaux logiques à appliquer sur des contacts bien définis pour remettre la carte à zéro, lire ou écrire un bit, présenter un code confidentiel bit à bit…

En principe, ces cartes contiennent un certain nombre de bits auxquels on accède « séquentiellement », c'est-à-dire l'un après l'autre dans l'ordre croissant de leurs « adresses ». Il n'est alors pas possible de reculer, sauf remise à zéro de la carte qui permet alors de repartir de la toute première adresse.

Les cartes asynchrones sont, pour la plupart, des cartes à microprocesseur dont l'entrée et la sortie des données se font sous la forme d'octets (groupes de huit bits) circulant sur la ligne série selon un protocole voisin de celui des transmissions RS 232 ou similaires : bit de start, bits de données, bit de parité, bits de stop, le tout à une cadence très inférieure à la fréquence d'horloge (souvent 9 600 bauds).

Ces octets peuvent être des données, des adresses, ou des instructions selon le programme contenu dans la mémoire de la carte et exécuté par celle-ci.

La carte peut garder en permanence la maîtrise de ses communications avec l'extérieur, ce qui apporte un degré élevé de sûreté.

La norme ISO 7816 définit les moindres détails de ce protocole de communication, qui admet toutefois de multiples variantes. On retiendra donc qu'il ne sera guère possible d'aller bien loin dans des manipulations autour

de cartes asynchrones, sans un minimum de documentation sur l'application à laquelle elles sont destinées.

Mais nous verrons que ces informations sont parfois librement disponibles, notamment dans le cas des cartes bancaires ! Même si cela peut surprendre, la sécurité de l'application ne s'en trouve nullement compromise tant que les codes confidentiels de l'émetteur et du porteur sont tenus secrets.

En revanche, on pourra opérer sur la plupart des cartes synchrones à partir des données, souvent relativement simples, figurant dans la fiche technique du circuit intégré utilisé.

Mais encore faut-il savoir de quel circuit intégré il s'agit, et dans le cas d'un composant spécialement destiné à être encarté, arriver à obtenir suffisamment de documentation à son sujet.

Fort heureusement, ces précieux renseignements sont de plus en plus facilement accessibles, à mesure que s'accroît la confiance des fabricants dans la sécurité de leurs produits et dans la rigueur de leurs clients.

En effet l'électronicien isolé, fût-il un industriel de renom, ne trouvera pas sur le marché de cartes complètement vierges, susceptibles d'être programmées pour n'importe quelle application. Il devra donc se contenter de cartes déjà partiellement « personnalisées » par tel ou tel émetteur, ou directement par leur fabricant, et donc infalsifiables.

Une exception remarquable à cette règle absolue concerne les cartes à mémoire simple qui, n'étant pas sécurisées, ne peuvent servir qu'à des applications pour lesquelles la notion même de falsification serait vide de sens.

CHAPITRE PAGE

| 1 | Vocabulaire et normalisation | 1 |
|---|---|---|

# 2 LES CIRCUITS INTÉGRÉS POUR CARTES À PUCE

**Les composants spécialisés** 14
**Les circuits intégrés apparentés** 28
**Les micromodules** 35

| 3 | La périphérie des cartes | 37 |
|---|---|---|
| 4 | Mise en œuvre des cartes synchrones | 67 |
| 5 | Applications pratiques des cartes synchrones | 105 |
| 6 | Introduction aux cartes asynchrones | 125 |
| 7 | Le cédérom du livre | 157 |

Une carte à puce n'étant finalement qu'un cas particulier de circuit intégré, il semblerait normal que n'importe quel électronicien puisse se procurer librement les documentations techniques des composants qui les équipent.

Cependant, les applications des cartes à puce étant ce qu'elles sont, ces précieuses publications sont souvent diffusées avec réticence !

Il nous a donc fallu une bonne dose de persévérance et plusieurs années pour réunir les informations dévoilées dans ce chapitre...

## LES COMPOSANTS SPÉCIALISÉS

Le tableau de la figure 2.1 récapitule les principales caractéristiques des circuits intégrés les plus couramment utilisés pour la fabrication des cartes à mémoire personnalisée (autrement dit synchrones), dont l'évolution s'étend déjà sur quatre générations.

Purement arbitraire, le mode de classement adopté est fondé sur le nombre de bits de la mémoire.

Nous avons répertorié les marques les plus représentatives, parmi lesquelles SGS-THOMSON occupe, depuis l'origine, une place très disputée de leader mondial.

Quelques fabricants n'ayant pas jugé utile de nous fournir des informations suffisantes ne sont pas cités, tandis que les grands « encarteurs » sont parfaitement capables de développer leurs propres « masques » de circuits intégrés, dont ils ne divulguent évidemment pas les spécifications.

Ce panorama n'est donc pas totalement exhaustif, mais il recouvre tout de même l'immense majorité des cartes actuellement en circulation.

Premier produit en date (mémoire EPROM NMOS de 256 bits), le ST 1001 est strictement réservé à la fabrication des télécartes françaises et livré exclusivement aux encarteurs agréés pour leur production, sous le contrôle sans faille de FRANCE TELECOM.

Au début de sa carrière (c'est-à-dire en 1983) ce composant s'est appelé ET 1001, puis TS 1001, de légères modifications de la topographie de sa « puce » accompagnant ces changements de nom successifs.





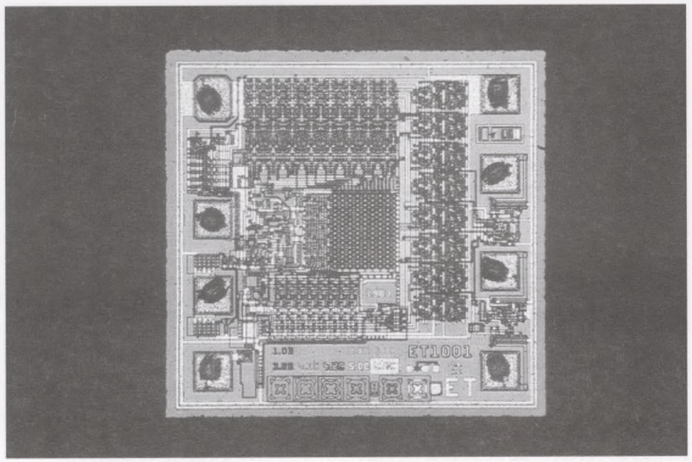
| Nombre de bits | Génération de circuit | Références / marques | Principales fonctions de sécurité | Principales applications |
|---|---|---|---|---|
| 104 | 3e | SLE 4406 Siemens<br>PCF 2006 Philips<br>AT88SC06 Atmel | Code de transport compteur « boulier » | Premières télécartes allemandes, cartes à jetons, GPM 103 Gemplus |
| 112 | 3e | Anciens ST 1305 (SGS-Thomson) | Code de transport compteur « boulier » | Premières télécartes « européennes », cartes à jetons |
| 192 | 3e | ST 1304<br>nouveaux ST 1305 (SGS-Thomson) | Code de transport compteur « boulier » zone « utilisateur » | Télécartes « européennes », cartes à jetons et diverses |
| 208 | 3e | ST 1303 (SGS-Thomson) | Code de transport, « boulier » | Premières T2G expérimentales (1993) |
| 212 | 4e | SCS 152 Microchip | Code de transport, cryptographie | Cartes à jetons « haute sûreté » |
| 221 | 4e | SLE443X Siemens<br>PCF 203X Philips<br>PCF 223X Philips | Code de transport, cryptographie | Télécartes « EUROCHIP » |
| 256 | 1re | ST 1001<br>SGS-Thomson<br>TMS 3561<br>Texas Instr. | 96 premiers bits protégés en écriture par fusible | T1G FRANCE TÉLÉCOM |
| 256 | 1re | ST 1200<br>SGS-Thomson<br>SLE 4412 Siemens | 96 premiers bits protégés en écriture par fusible, 9e bit à 1 | Télécartes autres que France Télécom, cartes à jetons, GPM 256 Gemplus |
| 272 | 4e | ST 1332<br>SGS-Thomson | Code de transport, cryptographie | T2G FRANCE TÉLÉCOM |
| 272 | 4e | ST 1331, ST 1333, ST 1335, ST 1336<br>SGS-Thomson | Code de transport, cryptographie | Cartes à jetons « haute sûreté », cartes rechargeables / recyclables |
| 416 | 2e | ST 1301<br>SGS-Thomson<br>SLE 4404 Siemens<br>PCF 7940 Philips | Fusible, code porteur, code émetteur, compteur d'effacements | Cartes à jetons « haute sûreté », cartes rechargeables, monétique, GPM 416 Gemplus |

**Figure 2.1.** Principaux circuits intégrés pour cartes synchrones.

La dernière version en date, qui équipe depuis plus de dix ans les télécartes de FRANCE TELECOM, est celle de 1987.

Comme le produit présente un grand intérêt pour beaucoup d'applications non téléphoniques, il a fallu prévoir une variante rendue volontairement impropre à la fabrication frauduleuse de « vraies fausses télécartes ».

© DUNOD - La photocopie non autorisée est un délit.




La « puce » ET 1001 d'une télécarte française (grossie 50 fois).

Le ST 1200 est donc parfaitement identique au ST 1001, à la seule exception que son neuvième bit est pré-programmé à 1 avant livraison à l'encarteur.

Même si des cartes à ST 1200 vierges étaient mises en circulation, il ne serait donc pas possible de les transformer en télécartes, du moins françaises puisque rien ne permet de remettre commodément ce bit à 0.

Le composant ST 1200 équipe les cartes GPM 256 de GEMPLUS, ses équivalents (F 256 SCHLUMBERGER, etc.), et certaines « clefs à mémoire » (les MK 10 de SEFEA).

Des « secondes sources » sont disponibles, notamment chez TEXAS INSTRUMENTS et SIEMENS.

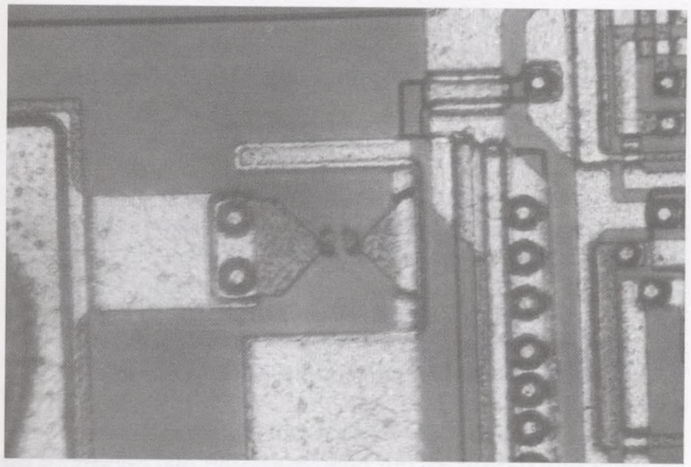
Les 96 premiers bits de sa mémoire EPROM sont protégés contre l'écriture par destruction définitive d'un fusible à la fin de sa personnalisation en usine, ce qui permet d'y inscrire des données d'authentification ne devant en aucun cas pouvoir être contrefaites. C'est la « zone fabricant » ou « zone d'identification ».

Les 160 bits qui suivent représentent la « zone des unités », dans laquelle l'application vient « griller » un bit à chaque fois qu'une unité est consommée.

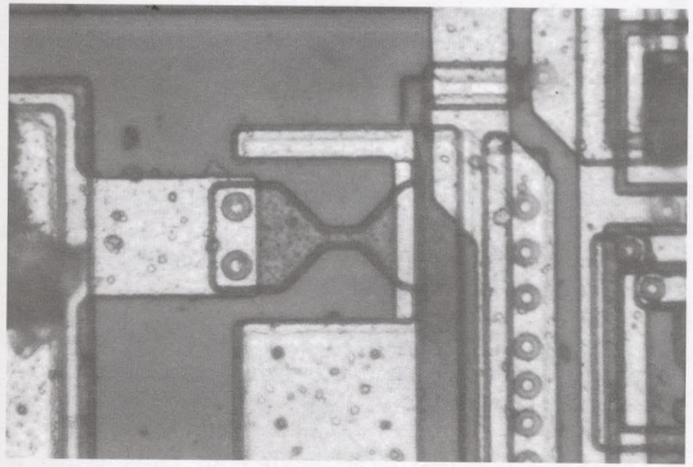
Les huit contacts (ISO1 à ISO8) disponibles sur le micromodule sont utilisés selon l'affectation de la figure 2.2, pour la mise en œuvre du protocole de communication « 3 fils » décrit sur la figure 2.3.



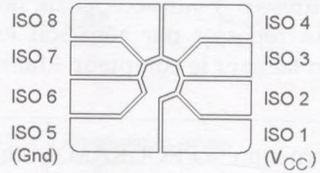




Le fusible de protection en écriture, coupé (grossi 500 fois).



Le même fusible, avant sa destruction (grossi 500 fois).




Brochage ISO 7816 du micromodule.

ISO 6 : $V_{pp}$ (21 V)
ISO 7 : sortie données
ISO 8 : fusible

| ISO 2 : | ISO 4 : | ISO 3 : | Micro-instruction : |
|---|---|---|---|
| 0 | 0 | ⎍ | RESET |
| 0 | 1 | ⎍ | UP |
| 1 | 1 | ⎍⎍ | PROGRAM ( 0 → 1) |

**Figure 2.3.** Protocole de communication « 3 fils ».

© DUNOD - La photocopie non autorisée est un délit.

La lecture et l'écriture dans la carte font appel à un jeu de « micro-instructions », séquences précises d'états logiques sur les contacts ISO2 et ISO4, tandis que les données transitent sur ISO7 et que l'alimentation se fait par ISO1 (Vcc), ISO6 (Vpp), et ISO5 (masse).

On notera que même pour des opérations de lecture seule, le contact ISO6 doit recevoir une tension d'alimentation au moins égale à Vcc, c'est-à-dire 5 V.

Le contact ISO8, quant à lui, doit être mis à la masse pour autoriser l'écriture dans la zone des 96 premiers bits. Cela si et seulement si le fusible de protection est intact.

Le fusible de toutes les cartes en circulation doit normalement être détruit, ce qui peut se vérifier en connectant un simple ohmmètre entre ISO5 et ISO8 : l'absence de déviation franche confirme que le fusible est irréversiblement coupé.

La micro-instruction « RESET » permet à tout moment, et notamment après une mise sous tension, de remettre à zéro le compteur d'adresses de la mémoire.

Après un RESET, son tout premier bit (souvent appelé bit 0) peut être lu sur le contact ISO7.

La micro-instruction « UP » permet, pour sa part, de faire avancer d'un cran le compteur d'adresses, et donc d'accéder au bit suivant.

On notera que rien n'est prévu pour faire reculer le compteur d'adresses. Pour accéder de nouveau à un bit déjà lu, il faut repasser par zéro soit en exécutant un RESET, soit en laissant le compteur « faire le tour » après le 256$^{e}$ bit.

La micro-instruction « PROGRAM », enfin, permet de transformer en 1 le bit courant s'il est encore à 0 (autrement dit de consommer une unité) pourvu qu'il ne se situe pas dans la « zone fabricant » si le fusible est détruit.

Le succès de l'opération d'écriture suppose qu'une tension de 21 volts soit appliquée au contact ISO6 (Vpp), le Vcc devant déjà être présent.

Bien entendu, s'agissant d'une mémoire EPROM « vierge à 0 », rien ne permet de transformer des 1 en 0, si ce n'est

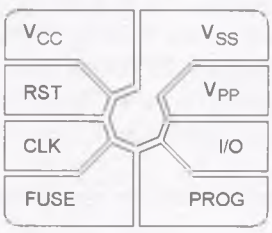
un effacement global par exposition de la puce à un rayonnement ultraviolet (opération exclue puisque la puce est hermétiquement scellée à l'intérieur de la carte...).

La seconde génération de composants (EEPROM CMOS bitension) assure déjà une sécurité très supérieure tout en offrant davantage de souplesse. La mémoire EPROM est en effet remplacée par de l'EEPROM (réinscriptible) tandis qu'une logique câblée de gestion de codes confidentiels est intégrée.

Le circuit intégré ST 1301 de SGS-THOMSON est un pionnier dans cette catégorie de composants : cette mémoire de 416 bits est en effet protégée par un fusible et un code secret (porteur et émetteur), et incorpore un réseau logique programmable.

Il sert à réaliser les cartes GPM416 de GEMPLUS et ses équivalents, ainsi que certaines clefs à mémoire (par exemple, les MK 20 de SEFEA).

La figure 2.4 décrit l'affectation des huit contacts de son micromodule, tandis que la figure 2.5 montre que son espace mémoire est organisé de la façon suivante :




| | |
|---|---|
| $V_{PP}$ | Programming voltage |
| I/O | Serial Data Input/Output. |
| PROG | Programming Order Input (Selection between Read or Write modes). |
| FUS | Fuse Input |
| CLK | Clock Input (for synchronization) |
| RST | Reset Input |
| $V_{CC}$ | +5 V Power Supply |
| $V_{SS}$ | Ground |

**Figure 2.4.** Brochage du micromodule du ST 1301.

© DUNOD - La photocopie non autorisée est un délit.

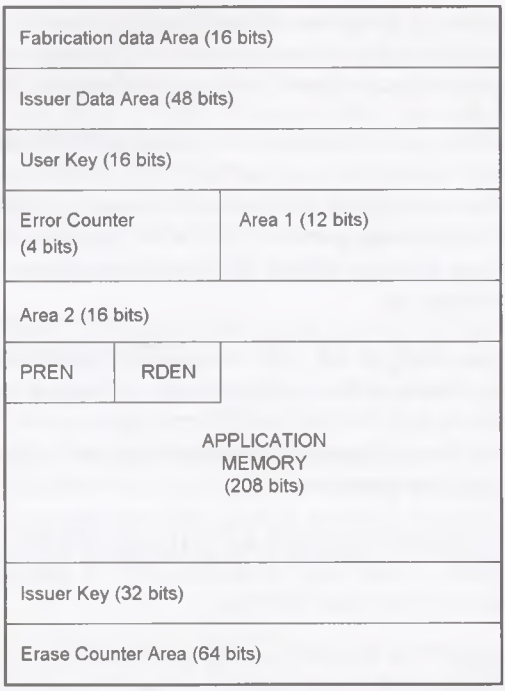



**Figure 2.5.** Organisation de la mémoire du ST 1301.

- une zone « fabricant » de 16 bits, programmée irréversiblement en usine par SGS-THOMSON et identifiant son client (autrement dit l'encarteur) ;
- une zone « émetteur » de 48 bits programmable irréversiblement par le client pendant la phase de personnalisation ;
- une clef « porteur » de 16 bits, programmée par SGS-THOMSON avec un code dit « de transport » que le client devra présenter pour pouvoir personnaliser la carte. Cela pourra être ensuite le code confidentiel du porteur de la carte, qui demeure modifiable si on présente d'abord l'ancien ;
- un compteur d'erreurs à 4 bits, qui enregistre le nombre de présentations d'un code erroné. Il est effacé dès la présentation du bon code, mais la puce se bloque définitivement si quatre erreurs consécutives sont commises ;
- une zone « N° 1 » de 12 bits, librement accessible en lecture comme en écriture, mais qui est effacée dès qu'un code correct est présenté ;
- une zone « N° 2 » de 16 bits, qui ne peut être écrite ou effacée qu'après présentation du code porteur ;



© DUNOD - La photocopie non autorisée est un délit.

– la « zone applicative » de 208 bits dont les modalités d'accès en lecture et en écriture sont fixées par ses deux premiers bits (PREN ou *PRogram ENable* et RDEN ou *ReaD ENable*), et par la présentation ou non du bon code porteur.

Son effacement nécessite la présentation du code porteur puis de la clef « émetteur » ;

– la clef « émetteur » de 32 bits, qui doit être programmée pendant la phase de personnalisation, puis en principe demeurer secrète ;
– un « compteur d'effacements » à 64 bits qui mémorise le nombre d'effacements de la zone applicative, et peut servir à limiter celui-ci si on le « pré-programme » à une valeur adéquate.

ISO 6 : Vpp (21 V)
ISO 7 : entrée-sortie données
ISO 4 : fusible

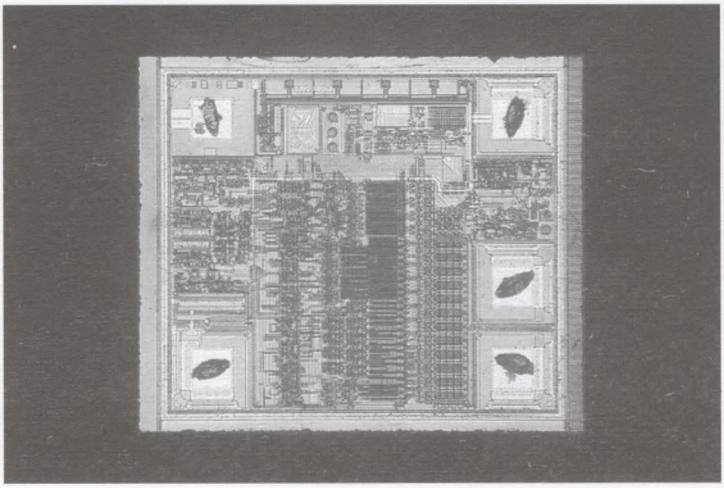
| ISO 8 : | ISO 2 : | ISO 3 : | Micro-instruction : |
|---|---|---|---|
| X | 1 | 0 | RESET |
| 0 | 0 |  | UP |
| 0 | 0 |  | CMP |
| 1 | 0 |  | PROGRAM ( 1 → 0) enchaîner ces deux séquences ERASE (0 → 1) |
| 0 | 0 |  | |

**Figure 2.6.** Protocole de communication du ST 1301.

Le dialogue avec la carte se fait selon un protocole série dont la figure 2.6 donne le détail, et qui dérive de celui de la figure 2.3. Une « micro-instruction » supplémentaire (CMP) sert à présenter les clefs, tandis que la manœuvre de programmation (transformation de 1 en 0 quand ISO7 est à 0) peut aussi servir à effacer des blocs entiers de 16 bits (transformation de 0 en 1 quand ISO7 est à 1).

La troisième génération de mémoires sécurisées (EEPROM CMOS monotension) est celle de la première « Telefonkarte » allemande.

Comme le ST 1001, le ST 1304 est réservé exclusivement à des clients privilégiés, tandis qu'une version à usage général est offerte sous la référence ST 1305 (48 bits de comptage d'unités, 24 bits « fabricant », 40 bits « émetteur », protection par code « de transport »).



La « puce » ST 1304 d'une télécarte allemande (grossie 50 fois).

Les ST 1305 les plus récents, bien que compatibles avec leurs aînés, bénéficient d'une capacité mémoire accrue (192 bits au lieu de 112), permettant d'offrir une « zone émetteur » supplémentaire.

La figure 2.7 montre que cinq contacts seulement sont utilisés sur les huit que peut offrir le micromodule, et on rencontre d'ailleurs des cartes à ST 1305 équipées d'un micromodule à six contacts seulement (ce sont alors ISO4 et ISO8 qui disparaissent).

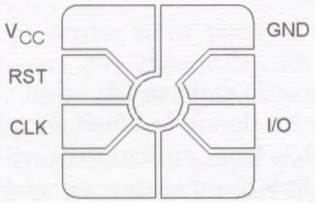



**Figure 2.7.** Brochage du micromodule du ST 1305.

Le « plan mémoire » des ST 1305 les plus récents est reproduit sur la figure 2.8, celui des versions plus anciennes n'allant que jusqu'à l'adresse 111, et celui des plus proches équivalents (SLE 4406, PCF 2006, etc.) ne dépassant pas l'adresse 103.

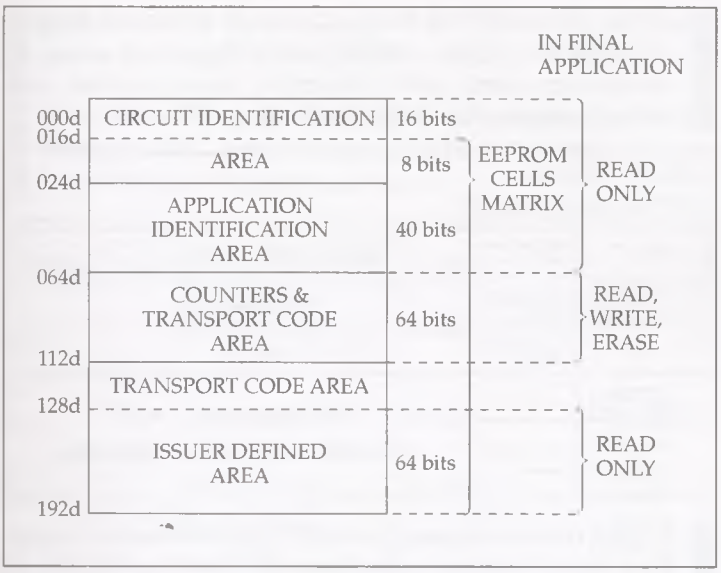



**Figure 2.8.** Organisation de la mémoire du ST 1305.

Dans tous les cas, la zone de comptage d'unités fonctionne de la même manière, selon un principe inspiré de celui des « bouliers ».

Cette zone de 40 ou 48 bits est divisée en un certain nombre de « compteurs » de 8 bits, l'un d'entre eux pouvant être amputé de quelques bits dans certains cas.

Le premier compteur (celui qui est placé à l'adresse la plus haute) comptabilise directement des unités. Une unité consommée y est représentée par un bit transformé, cette fois, de 1 en 0, la carte étant dite « vierge à 1 ».

Lorsque les huit bits de ce compteur ont été mis à 0, on peut faire jouer un mécanisme de « retenue » en les remettant tous à 1, mais en mettant simultanément un bit à 0 dans le compteur suivant.

Ce second compteur est donc dit « par 8 », tandis que le troisième compte « par 64 », le quatrième « par 512 », et le cinquième « par 4096 ».

Bien entendu, ce compteur « octal » est placé sous le contrôle d'une puissante logique de sécurité empêchant que des compteurs puissent être remis à 1 sans qu'un 0 ne soit inscrit à titre de « retenue » dans le compteur de poids immédiatement supérieur. Cela reviendrait en effet à « recharger » des unités dans la carte !

Toutes ces cartes fonctionnent selon le protocole de communication « 2 fils » décrit sur la figure 2.9, dont les micro-instructions sont largement incompatibles avec celles du protocole « 3 fils » de la figure 2.3.

**Figure 2.9.** Protocole de communication « 2 fils ».

| ISO 7 : données<br>ISO 6 : non connecté | | |
|---|---|---|
| ISO 2 : | ISO 3 : | Micro-instruction : |
| 1 |  | RESET |
| 0 |  | UP |
|  | 0 | PROGRAM ( 1 → 0)<br>enchaîner ces deux séquences |
| 0 |  | |

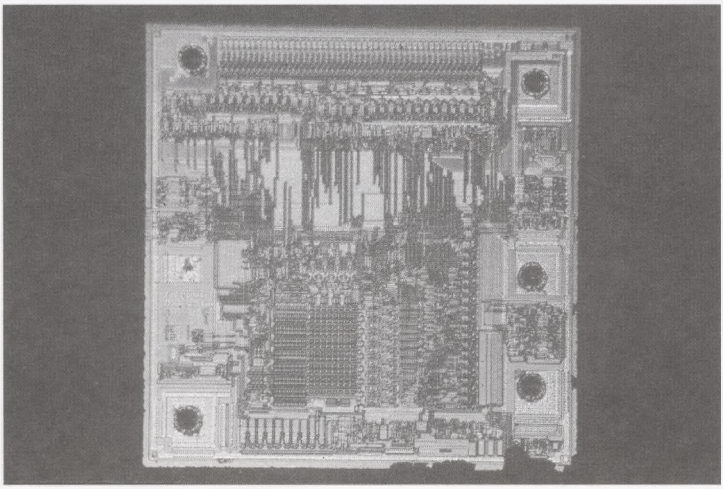
Il n'est cependant pas prévu de micro-instruction spécifique pour l'écriture avec retenue, celle-ci se faisant en enchaînant deux commandes WRITE sur un même bit.

La quatrième génération de puces réunit la T2G (télécarte de seconde génération) française, la télécarte européenne « EUROCHIP », et les cartes non téléphoniques basées sur ces mêmes technologies.

Tous les circuits de 4e génération ont en commun un système de comptage par boulier inspiré de ce qui vient d'être décrit, et une logique de sécurité très évoluée puisque faisant appel à des techniques cryptographiques.

Le ST 1332 est réservé à la production de T2G pour France Télécom, et jouit donc d'un certain degré de compatibilité avec la T1G, l'actuelle télécarte de « première

La « puce » EUROCHIP d'une télécarte européenne (grossie 50 fois).



génération » : carte « vierge à 0 », protocole « 3 fils », même brochage du micromodule (mais sans Vpp).

Il en va de même des produits dérivés comme le ST 1331 et le ST 1333, dont les figures 2.10 et 2.11 reproduisent respectivement les plans mémoire.

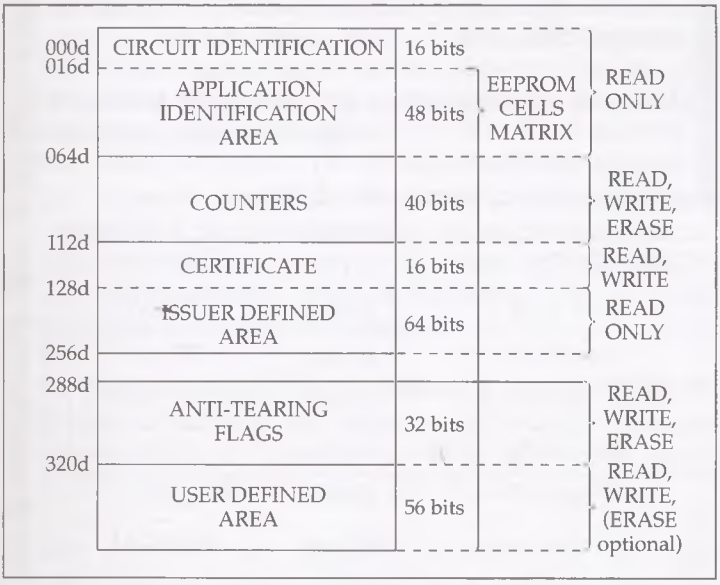



**Figure 2.10.**
Plan mémoire des ST 1331 et ST 1336.

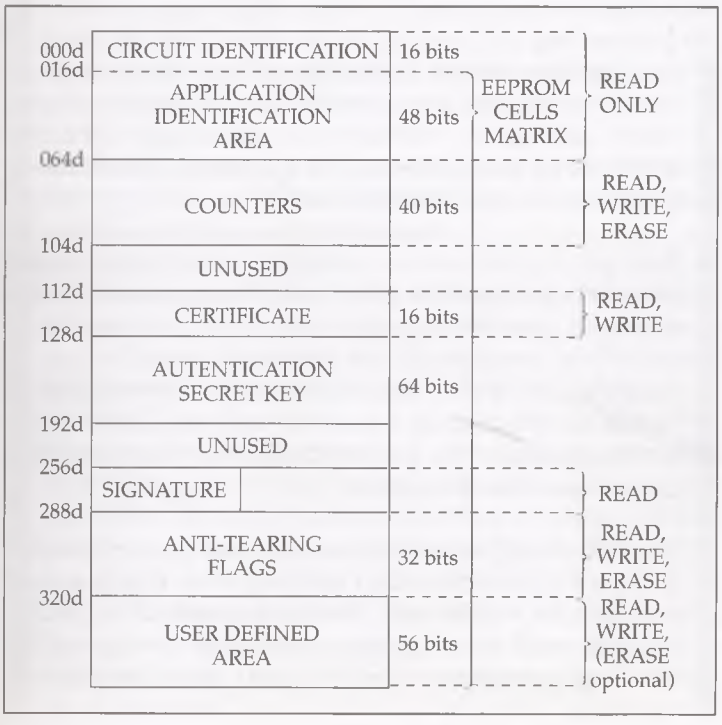



**Figure 2.11.**
Plan mémoire des ST 1333 et ST 1335.

La famille SLE 443X de Siemens (et ses « secondes sources » de marque Philips) sert à réaliser les télécartes EUROCHIP de plusieurs pays européens : Allemagne, Suisse, Pays-Bas, Grande Bretagne.

Chaque opérateur téléphonique utilise sa propre variante, celle de BRITISH TELECOM s'appelant, par exemple, SLE 4438.

La figure 2.12 reproduit ce qu'il nous a été possible d'apprendre sur le SLE 4433, informations qui confirment une certaine similitude avec les ST 1335 et ST 1336 : cartes « vierges à 1 » et à protocole « 2 fils ».

**Figure 2.12.** Aperçu du plan mémoire du SLE 4433.

| | | |
|---|---|---|
| *Anti-Tearing Flags* | 4 bits | EEPROM |
| *User Area* | 16 bits | PROM |
| *User Area* | 16 bits | PROM |
| *User Area/Key 2* | 48 bits | PROM/ROM |
| *Key 2 Flag* | 1 bit | ROM |
| *Key 1* | 48 bits | ROM |
| *Counter Area* | 40 bits | EEPROM |
| *Identification Data Area* | 64 bits | ROM |

0 — adresses croissantes

Du côté des cartes à microprocesseur (autrement dit asynchrones), tout a commencé avec les cartes de première génération, réalisées en technologie EPROM-NMOS et surtout destinées aux applications bancaires et de télévision à accès conditionnel.

Bien que ces composants contiennent chacun un système micro-informatique au grand complet, six contacts suffisent pour les mettre en œuvre.

En effet, il n'y a plus lieu de prévoir la protection par un fusible de telle ou telle zone de la mémoire, des sécurités au moins aussi sûres pouvant facilement être introduites par voie purement logicielle.

L'accès aux différentes zones de la mémoire n'est possible que par l'intermédiaire de l'interface série, et cela sous le contrôle du logiciel que l'on aura implanté en ROM. Celui-ci peut, si nécessaire, procéder à des opérations d'auto-programmation de l'EPROM, naturellement irréversibles.

Le microprocesseur équipant ce genre de puce est du type « 8 bits » et dispose d'un jeu d'instructions fort complet.

Tout cela est très suffisant pour développer des applications déjà performantes, sans toutefois offrir la souplesse des EEPROM. Toutes les utilisations nécessitant la tenue, dans la carte elle-même, d'un historique des transactions effectuées sont limitées par la saturation de l'espace d'EPROM disponible. Il faut alors envisager le remplacement périodique de la carte.

La seconde génération de cartes à microprocesseur (EEPROM CMOS monotension), riche, par exemple, des références de la forme ST 16XYZ chez SGS-THOMSON, ne souffre pas de ce genre de limitation tout en offrant une sécurité de très haut niveau.

Le dispositif de sécurité comprend une matrice de contrôle d'accès définissant les règles selon lesquelles un programme tournant dans une partie de la mémoire pourra accéder aux données stockées dans d'autres parties.

Des détecteurs de conditions opérationnelles positionnent des bits dans un « registre de sécurité », permettant ainsi au logiciel de vérifier, à tout moment, l'environnement de fonctionnement de la puce. Cela permet, en principe, de déjouer les principales tentatives d'accès illicite aux mémoires, y compris par mise à nu de la puce.

L'interface électrique se contente de cinq contacts, positionnés selon la norme habituelle sur un micromodule qui en possède six ou parfois huit.

Un langage assembleur au jeu d'instructions très complet permet de programmer des applications extrêmement performantes, y compris des algorithmes de chiffrement à clef secrète comme le DES.

En revanche, les algorithmes à clef publique comme le RSA ne peuvent être mis en œuvre de cette façon avec une rapidité suffisante (il faudrait 10 à 15 s pour traiter 256 bits, alors qu'on n'accepte guère d'attendre plus de 500 ms).

Les circuits de « troisième génération » emploient donc des « coprocesseurs de cryptage » optimisés pour traiter rapidement les calculs à base d'exponentiations utilisés en chiffrement.

## LES CIRCUITS INTÉGRÉS APPARENTÉS

Parallèlement aux circuits intégrés spécifiquement conçus pour être encartés et qu'on ne trouvera donc sans doute jamais en boîtier DIP, bien des composants très communs présentent toutes les caractéristiques voulues pour servir à la fabrication de cartes à puce, notamment à mémoire simple ou personnalisée. Ce sont principalement les mémoires à accès série réalisées en technologie EEPROM.

Les fabricants de cartes ne s'en privent assurément pas, et achètent certains de ces composants sous la forme de « wafers », rondelles de silicium qu'ils découpent eux-mêmes en puces qui seront montées sur micromodules puis encartées.

Bien entendu, les documentations de ces circuits intégrés sont disponibles sans problème, tandis que la figure 2.13 montre comment réaliser soi-même une « fausse carte » en circuit imprimé de 8/10 de millimètre pour expérimenter commodément avec les versions couramment commercialisées en boîtier DIP.

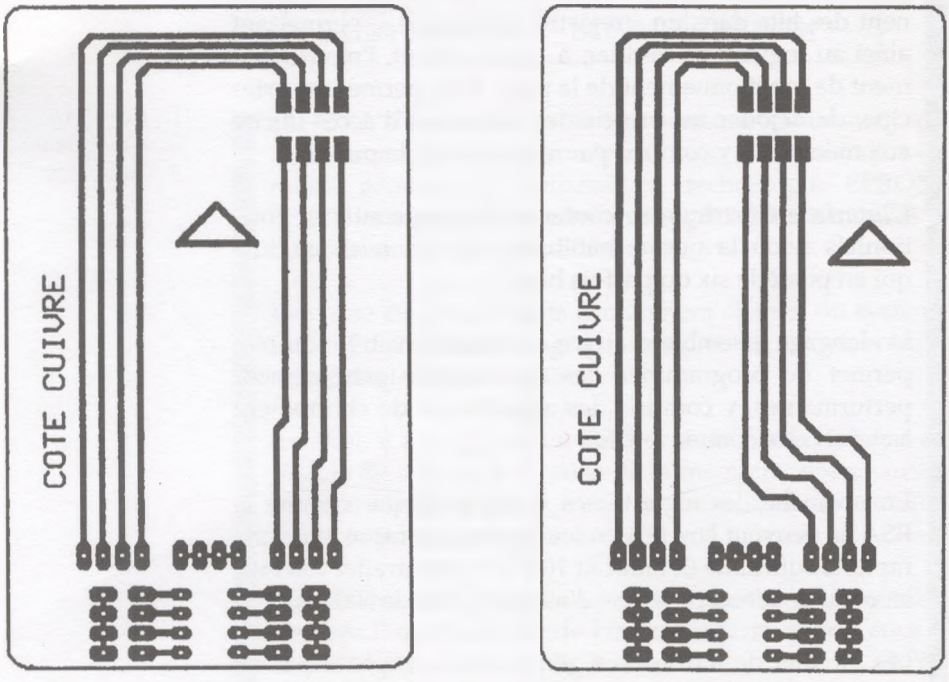



**Figure 2.13.** Deux « fausses cartes » pour boîtiers DIP.

Le mince stratifié présensibilisé nécessaire est un produit standard du CIRCUIT IMPRIMÉ FRANCAIS (CIF), et ne pose donc pas de problème d'approvisionnement.

La variante de la figure 2.13 b permet, pour sa part, de graver une « fausse carte » de type ISO (puce centrée) et non plus AFNOR (puce excentrée).

Après découpage très soigneux aux dimensions exactes des cartes standard, il sera procédé au câblage selon le plan de la figure 2.14 : un support à 8 contacts, et 7 tronçons de 4 éléments d'une « barrette sécable » à contacts « tulipe ».

Cette disposition permet d'affecter n'importe quel contact du « micromodule » à n'importe quelle broche du boîtier DIP, et même de réaliser les quelques interconnexions éventuellement nécessaires (mise à la masse ou au Vcc de plusieurs broches, par exemple), à l'aide de fils rigides de 6/10 mm.

La technologie EEPROM (ou E2PROM) permet de réaliser des mémoires présentant un attrait certain pour bien des applications « cartes à puce », car elles réunissent, dans une certaine mesure, les avantages des EPROM et des RAM.

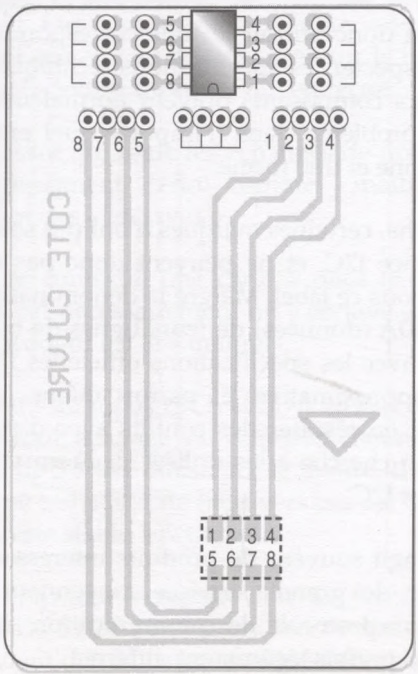



**Figure 2.14.** Plan de câblage des « fausses cartes ».

© DUNOD - La photocopie non autorisée est un délit.

Les capacités couramment disponibles dépassent maintenant 16 kilobits, et rejoignent donc celles d'EPROM « parallèles » comme la 2716.

Les protocoles de communication sont généralement assez classiques, à commencer par des dérivés de l'I2C.

Nous n'avons pas la prétention de cataloguer ici toutes les références ni tous les fabricants d'EEPROM série ! Nous n'avons retenu que les produits que l'on rencontre couramment dans les cartes à puce, les autres étant présentés en détail dans notre ouvrage *Composants électroniques programmables sur PC*, paru dans cette même collection.

Fortes de leur interface série à deux fils seulement (horloge et données), les EEPROM série à bus I2C semblent appelées à devancer, dans les applications « cartes à puce », les autres familles telles que MICROWIRE ou SPI.

I2C est en réalité une marque déposée de PHILIPS. Ne peuvent donc s'en prévaloir officiellement que les fabricants en ayant acquis la licence, mais on rencontre bien évidemment de multiples imitations, plus ou moins fidèles...

Beaucoup de marques ont heureusement acquis la licence et peuvent donc utiliser le sigle correspondant, à condition de respecter les spécifications techniques qui y sont liées. Leurs composants doivent normalement fonctionner sans problème dans n'importe quel environnement I2C en bonne et due forme.

En revanche, certaines marques n'ont pas souhaité acquérir la licence I2C, et ne peuvent donc pas vendre leurs produits sous ce label. Malgré la dénomination SCL (horloge) et SDA (données) de leurs lignes de bus, leur compatibilité avec les spécifications officielles I2C n'est souvent qu'approximative, et parfois même inexistante. Il peut donc en résulter des conflits avec d'autres composants si on cherche à les utiliser dans un véritable environnement I2C.

Mais il s'agit souvent de produits intéressants, capables de rendre de grands services moyennant la mise en œuvre d'un protocole de communication très proche de l'I2C, mais parfois légèrement différent.

Cela ne posera en général guère de problème lorsque la carte à puce sera l'unique composant apparenté I2C d'un système.

## Le protocole I2C

Il ne saurait être question de reproduire ici l'intégralité de la spécification I2C, d'ailleurs largement diffusée et facile à se procurer.

Quelques rappels sont toutefois souhaitables pour la bonne mise en œuvre des cartes à puce basées sur des mémoires qui communiquent selon ce protocole.

Le bus lui-même est constitué (hors masse et alimentation) de deux fils baptisés SCL (horloge) et SDA (données).

Les composants branchés sur ce bus doivent être capables de surveiller en permanence l'état de ces deux lignes sans les perturber en quoi que ce soit, mais aussi de leur imposer, quand il le faut, un niveau logique bas.

Fondamentalement, les étages destinés à attaquer le bus seront donc de type « collecteur ouvert » ou « drain ouvert ».

On définit fort logiquement comme « émetteur » tout composant qui envoie des données sur le bus, et comme « récepteur » tout composant qui en reçoit.

Le composant qui règle les échanges de données est tout aussi logiquement défini comme « maître », tous les autres étant des « esclaves ».

Dans notre contexte, une carte à puce (c'est-à-dire une mémoire) est nécessairement un « esclave » tandis que le lecteur-encodeur est le « maître ».

Le bus étant au repos (SCL et SDA en état « haute impédance »), tout échange de données commence par une condition de START émise par le maître. Il s'agit simplement d'une transition de haut vers bas sur SDA, pendant que SCL reste stable à l'état haut.

Inversement, tout échange doit se terminer par une condition de STOP (une transition de bas vers haut sur SDA pendant que SCL reste stable à l'état haut).

© DUNOD - La photocopie non autorisée est un délit.

À la fin d'une opération de lecture d'une carte à puce I2C, la condition de STOP marque son retour dans un état d'attente. En revanche, à la fin d'une opération d'écriture, elle déclenche par contre le cycle de programmation interne à l'EEPROM.

Un signal « ACK » (acknowledge) sert à indiquer la bonne exécution de chaque transfert de données. L'émetteur, qu'il soit maître ou esclave, libère SDA après la transmission du huitième bit de données. Pendant la neuvième impulsion d'horloge, le récepteur force alors SDA à l'état bas pour accuser réception de l'octet qui lui a été envoyé.

En effet, dans une carte à puce I2C, c'est par octets entiers et non plus bit à bit que l'on vient lire ou écrire des données.

La figure 2.15 résume ces différentes étapes, tout en montrant comment chaque bit est transmis : le récepteur lit l'état de SDA lors du front montant sur SCL, tout changement d'état de SDA ne devant intervenir que lorsque SCL est à l'état bas.

Parallèlement aux octets de données, le bus véhicule aussi des adresses.

Chaque « abonné » à un bus I2C possède en effet sa propre adresse, dont les quatre premiers bits sont imposés par la famille de composants à laquelle il appartient.

Dans le cas général d'une mémoire, ce code est toujours égal à 1010.

Le dernier bit de l'adresse (celui de poids faible) est un indicateur de lecture ou d'écriture : 1 pour une opération de lecture, 0 pour une opération d'écriture.

Les trois bits qui restent permettent d'accéder à un composant déterminé parmi plusieurs identiques, connectés au même bus, ou bien de sélectionner une « page » de 256 octets parmi plusieurs disponibles dans un même composant.

Dans le cas d'une carte à puce de 256 octets communiquant uniquement avec son lecteur-encodeur, ces trois bits demeurent tout simplement à 0.

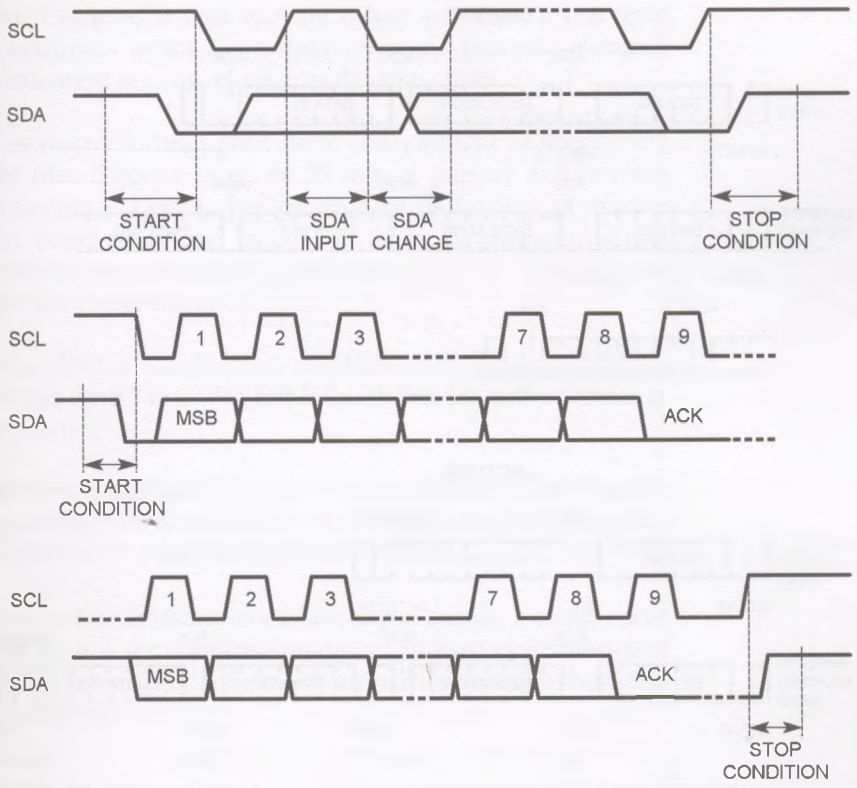



**Figure 2.15.** Protocole I2C.

En lecture, l'octet d'adresse sera ainsi 10100001, alors qu'en écriture il sera 10100000.

Plusieurs modes de lecture et d'écriture sont disponibles sur la plupart des EEPROM I2C. La figure 2.16 donne le détail de ceux qui peuvent être utilisés avec le ST 14C02 de SGS-THOMSON, une version « carte à puce » de la très classique 24C02, dont la capacité est précisément de 256 octets.

## LES MICROMODULES

Seule partie visible de l'électronique d'une carte à puce, le micromodule est un peu la « signature » de son fabricant, en même temps qu'un connecteur très particulier et de fabrication délicate.

© DUNOD - La photocopie non autorisée est un délit.

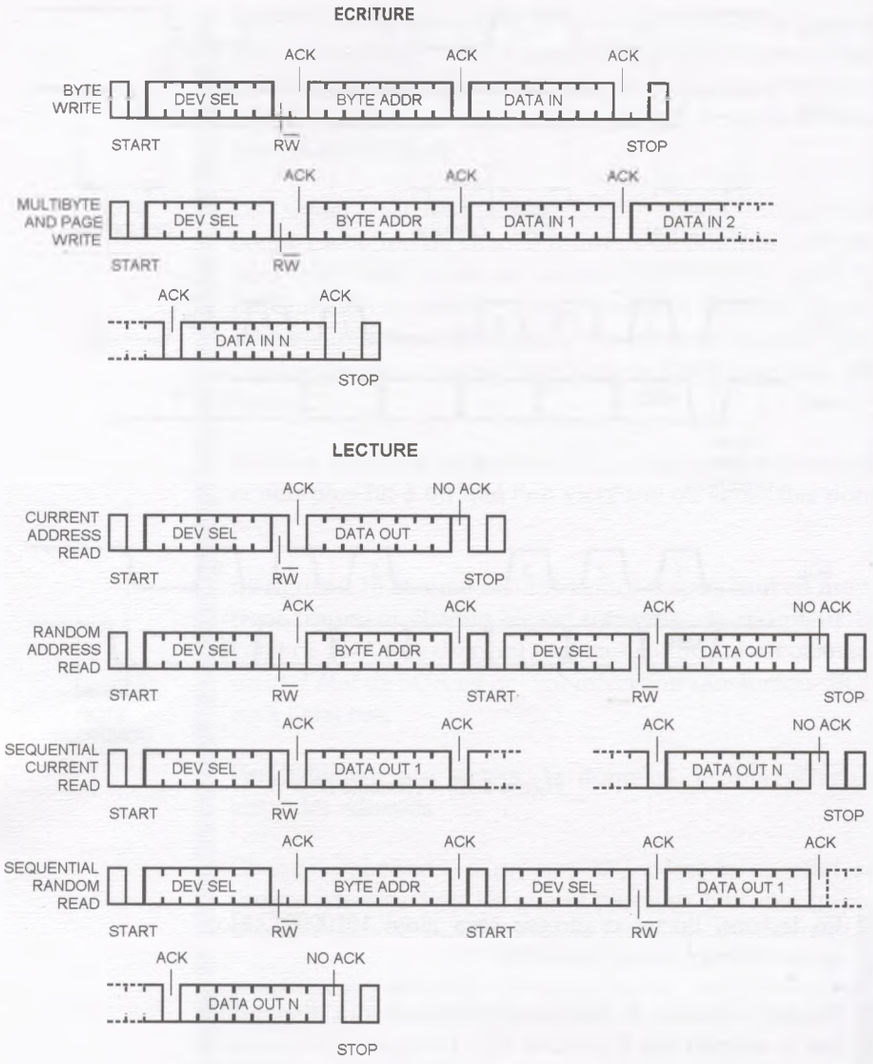



**Figure 2.16.** Comment lire et écrire dans un ST 14C02.

En effet, le micromodule doit non seulement permettre l'accès électrique à la puce pendant toute la vie normale de la carte, mais aussi jouer un rôle important durant sa fabrication.

Les puces étant particulièrement sensibles à l'électricité statique, il est souhaitable que tous leurs contacts restent mis à la terre pendant la majeure partie du processus de production.





En revanche, il faut tout de même procéder à des tests électriques avant l'encartage, et donc pouvoir éliminer facilement ces courts-circuits de protection.

Les micromodules sont donc couramment fabriqués sur du film d'époxy large de 35 mm et perforé aux normes « cinéma ». Leur forme est étudiée de façon à permettre un court-circuitage facile sur toute la longueur d'une bobine, et un isolement tout aussi facile de chaque puce par simple perforation.

Elle obéit aussi de plus en plus à des impératifs esthétiques dont la variété fait le bonheur des collectionneurs de cartes.

À titre d'exemple, la figure 2.17 reproduit le motif qui est gravé sur les films servant à produire les télécartes chez GEMPLUS CARD INTERNATIONAL.

Il en existe évidemment beaucoup d'autres, à commencer par ceux à six contacts seulement utilisés pour fabriquer les cartes les plus modernes, en particulier celles à microprocesseur.

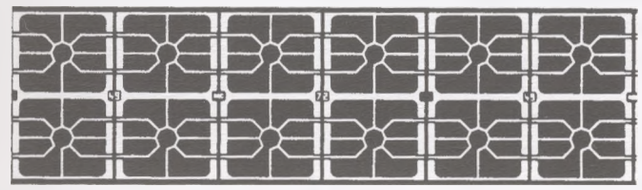
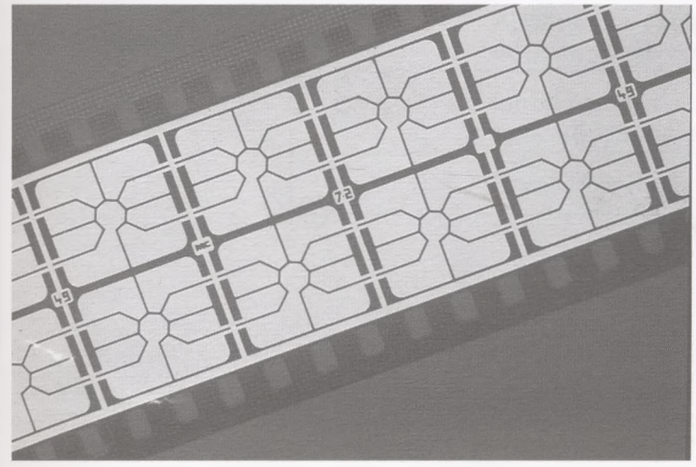


**Figure 2.17.** Micromodules « en continu » de Gemplus.



Les micromodules en continu chez Gemplus.

Le photocopillage non autorisé est un délit.

| CHAPITRE | | PAGE |
|---|---|---|
| 1 | Vocabulaire et normalisation | 1 |
| 2 | Les circuits intégrés pour cartes à puce | 13 |

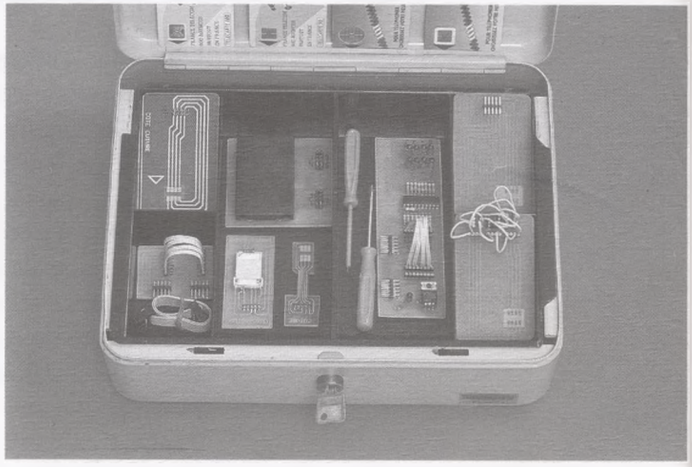

# 3 LA PÉRIPHÉRIE DES CARTES


**Un cordon universel** 38
**Les connecteurs de cartes** 40
**« Fausses cartes » en époxy** 42
**Petit adaptateur de brochage** 45
**Une sonde logique pour cartes à puce** 46
**Les interfaces de cartes** 47
**Les coupleurs de carte** 56
**Les lecteurs de cartes à puce** 58
**Deux alimentations 21 V pour cartes à puce** 60
**Réalisation pratique** 65

| | | |
|---|---|---|
| 4 | Mise en œuvre des cartes synchrones | 67 |
| 5 | Applications pratiques des cartes synchrones | 105 |
| 6 | Introduction aux cartes asynchrones | 125 |
| 7 | Le cédérom du livre | 157 |

Pour mettre en œuvre les cartes à puce dans de bonnes conditions, un environnement spécifique est indispensable : connecteurs de cartes conformes aux différentes normes en usage, interfaces, coupleurs, lecteurs-encodeurs, « fausses cartes » donnant accès aux connecteurs usuels, adaptateurs de brochage, et même sonde logique spécialisée.

Facilement réalisable à peu de frais, même un matériel simplifié apportera des solutions élégantes à des problèmes aussi variés que l'exploration de lecteurs et de cartes, la simulation de cartes, ou bien entendu le développement d'applications personnelles.



La « boîte à outils » idéale.

## UN CORDON UNIVERSEL

Les normes concernant les cartes à puce prévoient un maximum de huit contacts, nombre souvent ramené à six dans les applications récentes.

Si on ajoute les deux broches du contact détecteur de « présence carte » dont sont munis pratiquement tous les connecteurs, on aboutit à un maximum de dix liaisons utiles, quelles que soient les dimensions des cartes ou la position de la puce.

Nous avons donc décidé de standardiser tous les éléments de notre « boîte à outils » autour d'un câble de liaison universel à dix conducteurs, équipé de deux fiches HE10 à dix contacts, câblées en parallèle fil à fil.

Tous nos montages ou presque seront donc munis d'une barrette à double rangée de cinq picots (droits ou coudés, au choix), et pourront être interconnectés de toutes les façons imaginables à l'aide d'un unique type de câble.

© DUNOD - La photocopie non autorisée est un délit.





La figure 3.1 définit l'affectation de ces picots, en fonction de la numérotation normalisée des contacts des cartes à puce. On notera que, dans le cas des cartes à six contacts, ce sont ISO4 et ISO8 qui disparaissent.

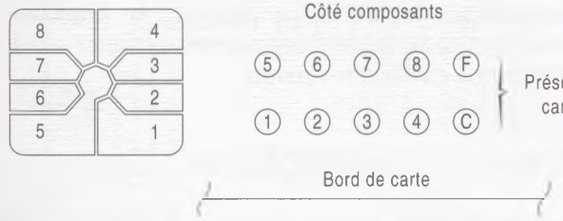



**Figure 3.1.** Brochage de notre connecteur universel.

Bien évidemment, les signaux électriques correspondant à ces contacts peuvent varier très largement d'un type de carte à l'autre. Nous avons vu qu'en principe une norme est prévue, mais c'est parfois la disposition des plots de soudage sur les puces de silicium qui prime ! On commence déjà bel et bien à ressentir l'intérêt de dispositifs adaptateurs de brochage...

La figure 3.2 décrit la réalisation du câble de liaison, utilisant de la nappe à dix conducteurs et des fiches à sertir (avec un petit étau). Il est très important que ces deux

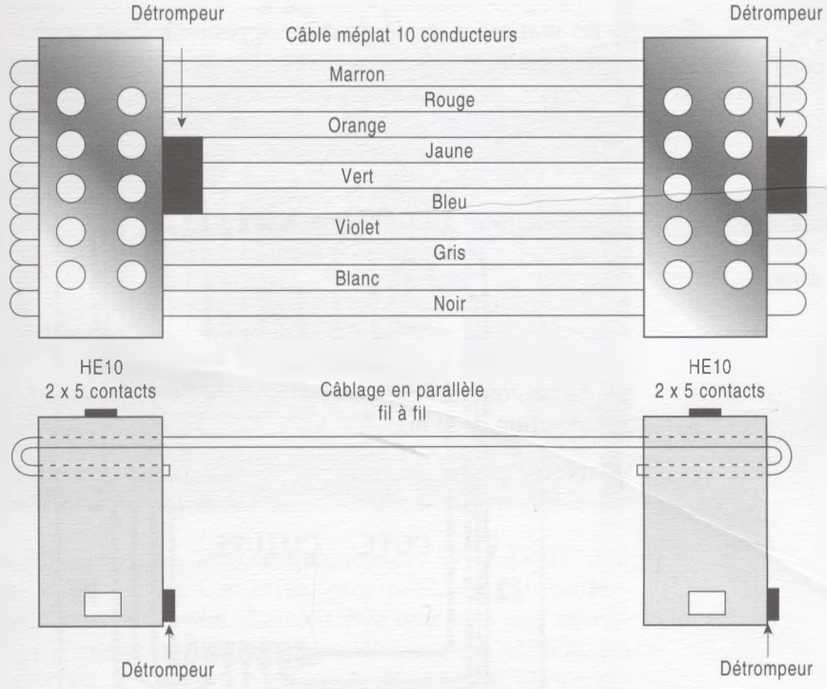



**Figure 3.2.** Schéma du cordon d'interconnexion.

connecteurs HE10 soient bien réunis en parallèle fil à fil, autrement dit que leurs détrompeurs soient orientés du même côté.

S'il est fait usage de picots coudés sur les modules à interconnecter, les fiches ne pourront se brancher que dans le bon sens, le détrompeur venant buter sur le circuit imprimé en cas d'inversion.

## LES CONNECTEURS DE CARTES

Deux cas seulement sont à envisager pour les cartes à puce au format standard des cartes de crédit : contacts excentrés (norme française AFNOR), ou contacts centrés (norme internationale ISO).

Les connecteurs de carte du commerce (et notamment celui d'ITT-CANNON disponible au détail pratiquement partout) comportent la plupart du temps seize contacts, et sont donc compatibles avec les deux standards.

C'est toutefois à l'utilisateur qu'il appartient de choisir le jeu de contacts correspondant aux cartes qu'il souhaite utiliser, ou de câbler carrément les deux en parallèle.

En matière d'outils de développement, il est souhaitable de pouvoir traiter séparément les deux cas. Notre module support de connecteur, dont la figure 3.3 fournit le tracé du circuit imprimé, est donc muni de deux prises dis-

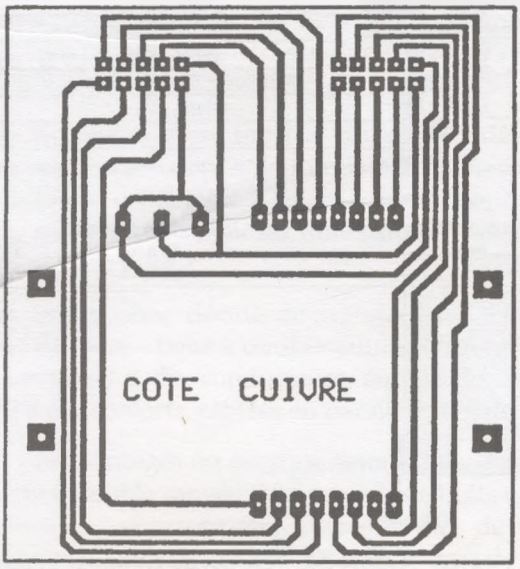



**Figure 3.3.**
Circuit imprimé du connecteur de cartes.

tinctes : l'une donnant accès aux contacts AFNOR, et l'autre aux contacts ISO comme le montre le plan d'implantation de la figure 3.4.

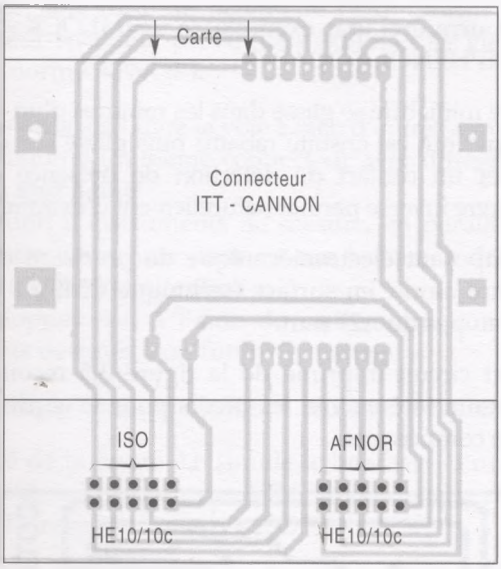
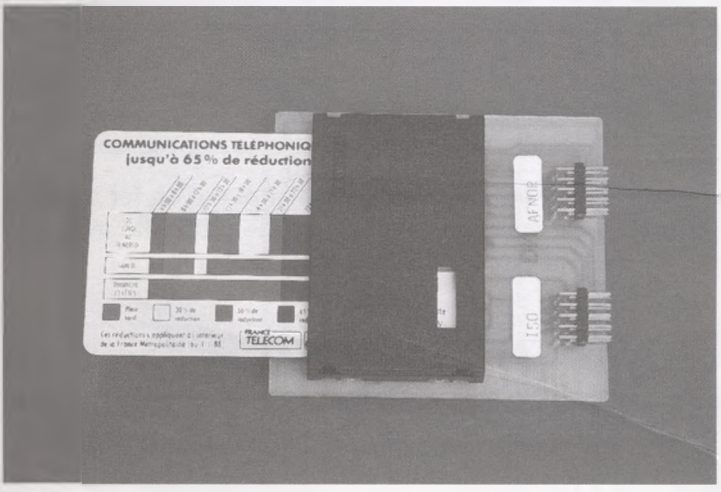



**Figure 3.4.** Plan de câblage du connecteur de cartes.

Bien entendu, le contact de détection de présence carte est amené en parallèle sur les deux prises.




Le connecteur de cartes ISO et AFNOR.

Le cas des cartes à puce miniatures « SIMCARD » doit être traité à part. Ces cartes plus petites qu'un timbre-poste peuvent éventuellement être obtenues par découpage d'une carte ISO mais pas d'une carte AFNOR (sa puce n'est pas dans le bon sens !) En principe, elles n'exploitent que six contacts utiles sur les huit disponibles.

Bien qu'on trouve chez certains revendeurs de téléphones portables des adaptateurs adhésifs permettant de revenir au « grand format », un connecteur spécifique est souvent nécessaire.

Cela pourra être, par exemple, le « SIMLOCK » proposé par AMPHENOL-SOCAPEX.

La carte miniature se glisse dans les rainures d'un couvercle basculant, qui est ensuite rabattu puis glissé sur un jeu de balais et un contact de détection de présence carte. La manœuvre inverse permet naturellement d'extraire la carte.

Ce composant électromécanique de précision est prévu pour être monté en surface (technique CMS), à l'aide de picots au pas de 1,27 mm.

Le petit circuit imprimé de la figure 3.5 reçoit donc le connecteur côté cuivre, les picots pour le cordon restant du côté composants.

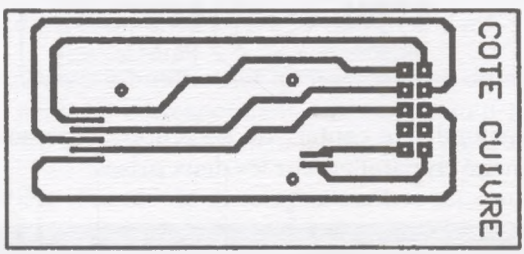



**Figure 3.5.**
Circuit imprimé du connecteur pour SIMCARD.

Les trois trous accueillant les pions de centrage seront percés à 1,5 mm, garantissant un bon positionnement des picots à souder en face de leurs pistes respectives.

Moyennant un peu de soin et l'emploi d'un fer à souder très fin, le soudage ne pose pas de problème majeur. Il n'y a même pas besoin de plan de câblage !

## « FAUSSES CARTES » EN ÉPOXY

Sous cette appellation un peu osée se cachent tout simplement des circuits imprimés en époxy de 8/10 mm, aux dimensions des cartes à puce courantes, munis à la fois de contacts placés comme ceux des micromodules et de picots pour nos câbles à connecteurs HE10.

Nous avons d'ailleurs déjà eu l'occasion de faire appel à cette technique pour la transformation en cartes à puce de certaines mémoires présentées en boîtier DIP (figure 2.13).

Associées aux connecteurs de carte précédemment décrits, ces fausses cartes permettent d'utiliser une carte conforme à n'importe quelle norme sur un lecteur ou encodeur prévu pour n'importe quelle autre norme : par exemple, une carte de parcmètre PIAF (norme ISO) sur un lecteur-encodeur prévu pour exploiter les vieilles télécartes (norme AFNOR).

Mais ce principe ouvre la voie à bien d'autres applications :
- utilisation d'un même connecteur avec différents montages tour à tour ;
- insertion d'instruments de mesure, en parallèle ou en coupure, entre une carte et son lecteur, à des fins de contrôle ou d'exploration ;
- développement, à l'aide de composants courants, de circuits destinés à un futur « encartage ».

Ces exemples ne sont d'ailleurs nullement limitatifs !

Le tracé de la figure 3.6 simule le brochage d'une carte à puce conforme à la norme AFNOR, tandis que celui de la figure 3.7 respecte la norme ISO.

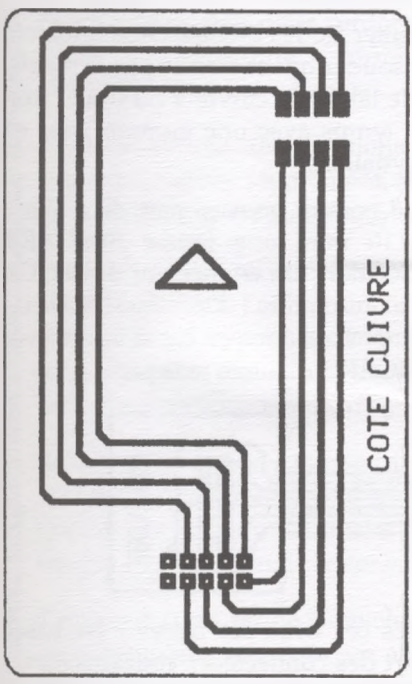



**Figure 3.6.** Réalisation d'une « fausse carte » AFNOR.

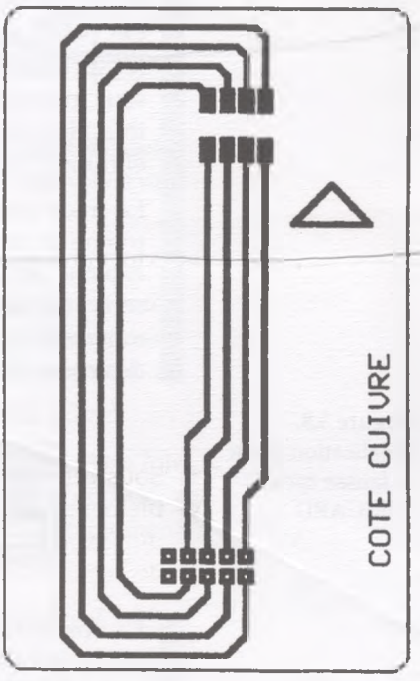



**Figure 3.7.** Réalisation d'une « fausse carte » ISO.

On remarquera que, dans les deux cas, la zone correspondant aux contacts de la norme concurrente est vide de cuivre, afin d'éviter tout risque de court-circuit dans les connecteurs « mixtes ».

Ces circuits imprimés sont à graver sur du stratifié époxy, simple face, d'épaisseur 8/10 mm. C'est un produit standard du CIRCUIT IMPRIMÉ FRANCAIS (CIF), qui convient à merveille pour prendre la place des cartes d'épaisseur nominale 0,76 mm.

Bien entendu, la découpe du pourtour doit être effectuée avec précision, et suivie d'un rodage au papier abrasif fin (400 « à l'eau »).

Après soudure des picots de raccordement du câble d'interconnexion (implantés côté composants), il est à conseiller de vernir le côté cuivre de la carte (par exemple au TROPICOAT), non sans avoir provisoirement protégé la zone des contacts par un petit rectangle de ruban adhésif que l'on retirera délicatement après quelques minutes de séchage.

Si on en a la possibilité, on dorera les contacts du « faux micromodule » (il existe dans le commerce des « kits de galvanoplastie » fort peu coûteux).

On peut aussi se contenter de les étamer chimiquement (et surtout pas au fer à souder qui causerait une surépaisseur inacceptable) ou de laisser le cuivre à nu (on le frottera alors de temps en temps avec une gomme pour en éliminer l'inévitable oxydation).

Le tracé de la figure 3.8 permet pour sa part de réaliser, toujours en époxy 8/10 mm, une fausse SIMCARD capable de prendre place dans un connecteur SIMLOCK sans en empêcher la fermeture. Des modifications mineures pourraient être nécessaires en cas d'usage avec des connecteurs de SIMCARD d'autres marques.

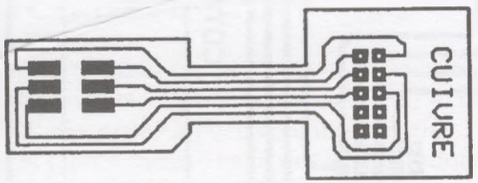



**Figure 3.8.**
Réalisation d'une « fausse carte » SIMCARD.

La conception de toutes ces « fausses cartes » est basée sur le fait que la plupart des connecteurs courants « avalent » à peine la moitié de la carte. Il reste donc une place confortable pour implanter des composants d'une certaine épaisseur.





Bien entendu, ces outils ne seront pas utilisables avec les lecteurs motorisés qui, pour des raisons évidentes de sécurité, entraînent la carte dans les profondeurs de leur mécanisme, ni dans ceux qui referment un volet par dessus.

## PETIT ADAPTATEUR DE BROCHAGE

Quoi de plus simple que le petit accessoire basé sur le tracé de circuit imprimé de la figure 3.9 ?

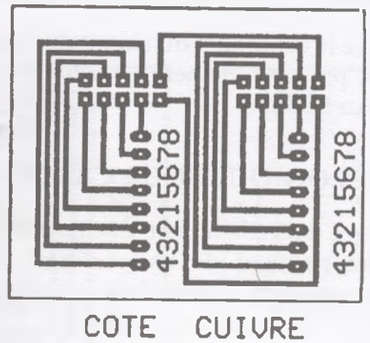



**Figure 3.9.**
Réalisation d'un adaptateur de brochage.

Deux connecteurs pour cordons de liaison, reliés chacun à huit douilles « tulipe », correspondent aux huit contacts normalisés des cartes à puce.

Chacune de ces deux sections identiques peut évidemment être utilisée séparément, associée par exemple à une boîte de connexion sans soudure.

En liaison avec un connecteur de carte, cela permet de relier tout ce que l'on voudra à une carte facilement interchangeable. On peut ainsi étudier son fonctionnement, naturellement, mais aussi développer commodément un lecteur ou un encodeur.

En liaison avec une « fausse carte », cela permet cette fois de relier n'importe quoi à un lecteur ou à un encodeur quelconque, dont on souhaite étudier le fonctionnement ou que l'on a besoin de tester en détail.

Cela peut aussi servir à développer un montage à partir de composants courants, en attendant qu'un jour, peut-être, il puisse être « encarté » ou tout simplement câblé sur une « vraie fausse carte » dédiée à un usage bien précis (carte de test, par exemple).

Mais le but premier de ce petit circuit est de faciliter les adaptations de brochage entre cartes et lecteurs ou programmateurs. Il existe en effet des cartes dont le brochage n'est pas standard, mais qui seraient fonctionnellement compatibles avec bien des équipements existants.

Il suffit de relier un connecteur et une « fausse carte » à notre petit adaptateur, pour pouvoir mettre le brochage en conformité à l'aide de quelques courts cavaliers en fil rigide de 6/10 mm dénudé à chaque extrémité sur 3 mm environ. On retrouve là le principe des adaptateurs de brochage pour liaisons RS 232, chers aux techniciens de l'informatique.

Ajoutons que la continuité du circuit du contact détecteur de carte est prévue à demeure, facilité qui pourra nous être utile plus tard.

## UNE SONDE LOGIQUE POUR CARTES À PUCE

Les montages précédemment décrits facilitent évidemment le branchement de toutes sortes d'appareils de mesure sur une carte à puce dans l'exercice de ses fonc-

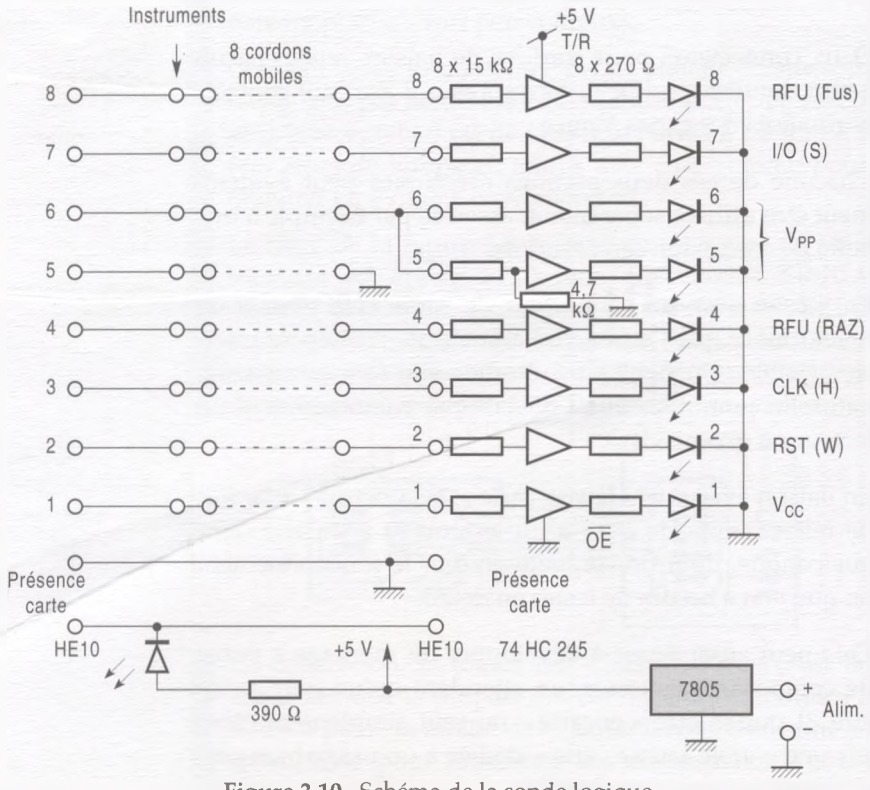



**Figure 3.10.** Schéma de la sonde logique.

tions, mais cela ne suffit pas toujours pour bien visualiser ce que l'on souhaite mettre en évidence. Une vue d'ensemble de tous les signaux est souvent souhaitable.

Sans pour autant être bien compliqué, le montage de la figure 3.10 répond à ce besoin. Comme le précédent, il peut se monter « en coupure » entre un connecteur et une « fausse carte », mais il offre bien d'autres ressources :

– l'une de ses deux sections est munie de huit « tulipes » supplémentaires, destinées au branchement d'appareils de mesure classiques (oscilloscope, analyseur logique, etc.) ;

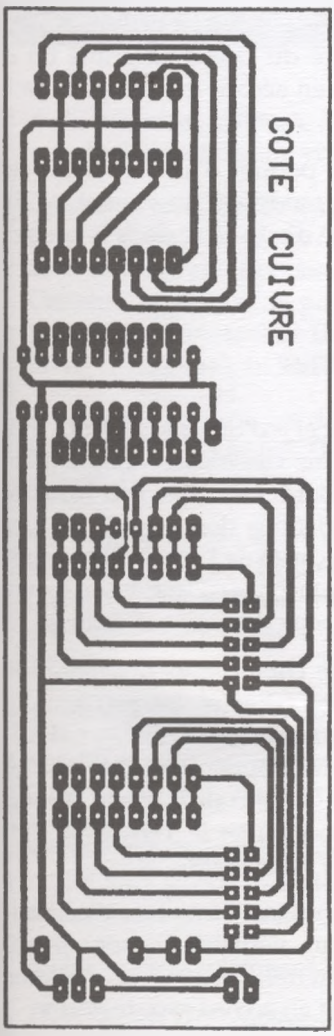



**Figure 3.11.** Circuit imprimé de la sonde logique.

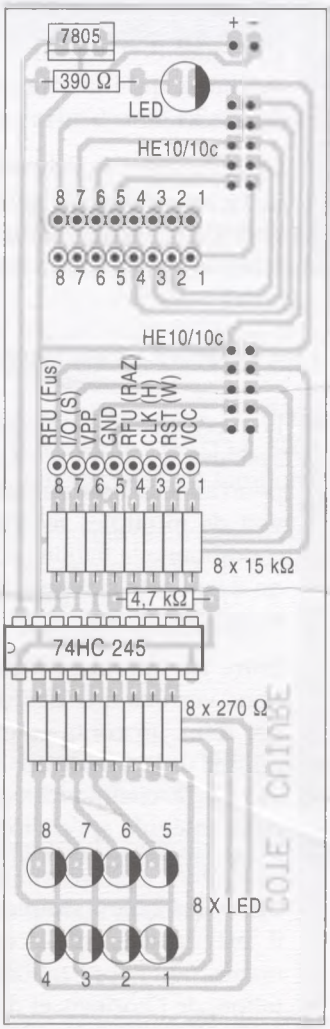



**Figure 3.12.** Plan de câblage de la sonde logique.

*Liste des composants*

**Résistances** (5 % 1/4W) :
R1 à R8 : 270 Ω,
R9 : 4,7 kΩ,
R10 à R17 : 15 kΩ,
R18 : 390 Ω.

**Circuits intégrés :**
CI1 : régulateur 7805,
CI2 : 74HC245.

**Autres semi-conducteurs :**
7 LED vertes,
2 LED rouges.

**Divers :**
1 barrette sécable « tulipe »,
1 barrette sécable à doubles picots coudés.

– l'autre section est équipée de huit « sondes logiques » à LED capables de visualiser en permanence ce qui se passe sur tous les contacts de la carte à la fois.

Comme il n'y a pas besoin de voyant pour la masse, l'un des circuits en possède deux, le second ne s'allumant que si la tension qui lui est appliquée dépasse sensiblement 5 V. C'est bien utile pour mettre en évidence une éventuelle tension de programmation Vpp.

Naturellement, les choses vont souvent bien trop vite pour que l'on puisse les suivre en temps réel, mais il est parfois possible de ralentir l'horloge du système ou de lui en substituer une autre, parfois même au point de pouvoir travailler en « pas à pas ».

La figure 3.11 fournit le tracé du circuit imprimé de ce montage, qu'il faudra câbler en accord avec le plan de la figure 3.12.

Le régulateur 5 V incorporé permet d'alimenter les circuits sous 9 à 15 V environ, tandis qu'un voyant à LED permet de vérifier la présence d'une carte dans le connecteur raccordé au montage.

## LES INTERFACES DE CARTES

Le raccordement « professionnel » d'une carte à puce à un système applicatif n'est pas une chose aussi simple qu'on pourrait le penser de prime abord. La norme ISO 7816 prévoit de multiples recommandations dont le strict respect conditionne la fiabilité et la sécurité de l'application, tandis qu'il faut bien produire, d'une façon ou d'une autre, les tensions d'alimentation et les signaux d'horloge et de reset.

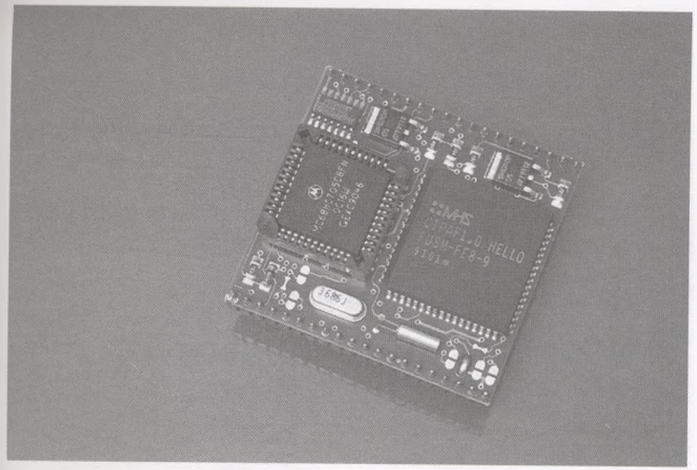
Entre les interfaces à base de composants discrets (dont nous verrons que des versions très simples peuvent suffire dans un contexte expérimental) et l'ASIC « CIPAF » qui fut utilisé dans certains développements d'INNOVATRON (à commencer par le « PIAF »), il existe des circuits intégrés spécialisés qui, comme le TDA 8000 PHILIPS, offrent un moyen terme intéressant.

Bien plus qu'un simple composant d'interface électrique, il est capable d'exécuter un véritable « programme » orchestrant l'application et le retrait des tensions d'alimentation, de l'horloge, et du reset en accord avec la norme.

Il produit par ses propres moyens le signal d'horloge à partir d'un quartz de fréquence double, et la tension







Un coupleur du commerce (développé par INNOVATRON).

d'alimentation protégée Vpp à partir d'une source continue d'une trentaine de volts.

Contrairement au CIPAF qui utilise des élévateurs à découpage et se contente donc d'une alimentation de 5 V, le TDA 8000 contient en effet des régulateurs de tension linéaires. Certaines applications pourront donc nécessiter l'adjonction d'un convertisseur DC-DC séparé (voir schémas à la fin de ce chapitre), en l'absence d'alimentation secteur.

En ce qui concerne les données transitant dans les deux sens par le contact 7 (I/O) de la carte, le TDA 8000 demeure « transparent » et se limite à un rôle de tampon.

On lui ajoute normalement un microcontrôleur pour pouvoir lire et écrire dans toutes sortes de cartes, à moins qu'on ne préfère se servir d'une partie des ressources d'un processeur utilisé pour d'autres fonctions du système.

### Mise en œuvre du TDA 8000

Le TDA 8000 est présenté dans un boîtier DIP28 ou SO28L dont la figure 3.13 fournit le brochage.

Le schéma synoptique du composant, reproduit sur la figure 3.14, permet de mieux comprendre le rôle précis de chacune de ces connexions dont voici le détail :

XTAL : quartz rejoignant la masse.

I/O1 et I/O2 : entrées-sorties carte (normalement une seule, mais certaines cartes peuvent posséder une seconde ligne d'entrée-sortie en C4 ou C8).

*RST : vers la broche de reset de la carte.*

CLK : vers la broche d'horloge de la carte.

PSEL1 et PSEL2 : sélection de la tension Vpp (5 V, 12,5 V, 15 V, ou 21 V).

/PRES et PRES : détection de présence carte (actif bas et actif haut).

VPP : vers le contact de Vpp de la carte.

VH : alimentation haute tension (30 V max) pour génération du Vpp.

GND : masse générale.

VDD : alimentation positive (6,6 à 18 V).

VCC : vers le contact de Vcc de la carte (5 V 100 mA max).

VSUP : entrée du superviseur de la tension d'alimentation du microcontrôleur.

DELAY : condensateur de temporisation du reset du microcontrôleur.

ALARM et /ALARM : signaux de reset pour le microcontrôleur (actif haut et actif bas).

/OFF : signal d'interruption pour le microcontrôleur (actif bas).

/START : demande de début de session (actif bas).

/WRITE : demande d'écriture (application de Vpp à la carte).

CVNC : référence interne de 5 V (à découpler extérieurement).

/CLKDIV : division ou non-division par deux de la fréquence de CLKOUT.

CLKIN : entrée pour signal d'horloge externe.

CLKOUT : signal d'horloge pour le microcontrôleur ou autre usage.

RSTIN : demande de reset de la carte.

I/O1(µC) et I/O2(µC) : lignes de données du microcontrôleur.

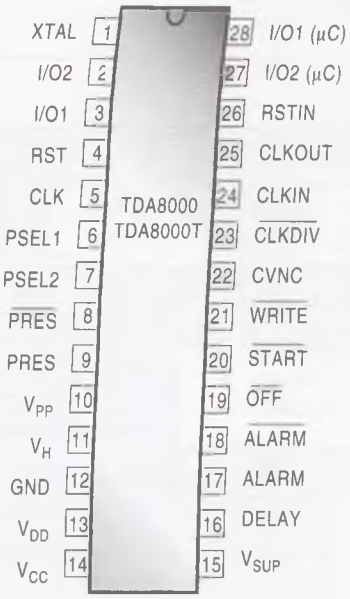



**Figure 3.13.** *Brochage du TDA 8000.*

La figure 3.15 détaille pour sa part l'agencement électrique des principales broches, tandis que la figure 3.16 précise le fonctionnement de la partie horloge.

Le TDA 8000 peut être cadencé soit par un quartz, soit par un signal d'horloge externe pouvant provenir, par exemple, d'un autre TDA 8000 ou du système hôte.

Le contact d'horloge de la carte reçoit une fréquence moitié de celle du quartz (2 à 12 MHz), ou égale à celle appliquée à la broche CLKIN (1 à 6 MHz).

Bien que certaines cartes acceptent des fréquences d'horloge proches de zéro, il n'est pas recommandé d'opérer en dessous de 1 MHz. La fréquence conseillée pour le quartz est 7,16 MHz, conduisant avec une majorité de cartes asynchrones à une cadence de données de 9600 bauds.

L'horloge du séquenceur interne du TDA 8000 est également dérivée de ce signal, par un diviseur supplémentaire, tandis que, selon l'état de la broche /CLKDIV, la sortie CLKOUT recopie purement et simplement la fréquence du quartz ou la divise par deux.

On le voit, ces différentes options permettent d'adapter le TDA 8000 à un maximum de contextes.

© DUNOD - La photocopie non autorisée est un délit.

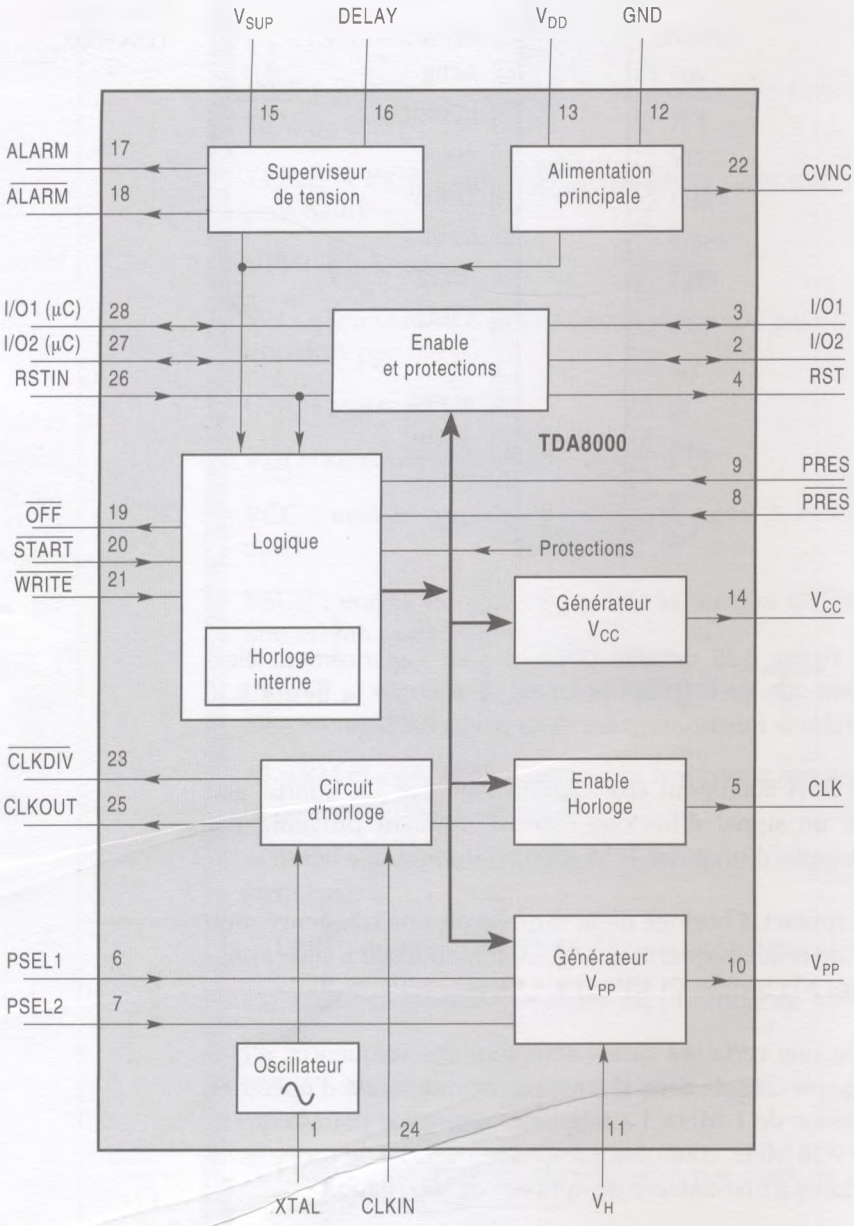



**Figure 3.14.** Architecture interne du TDA 8000.

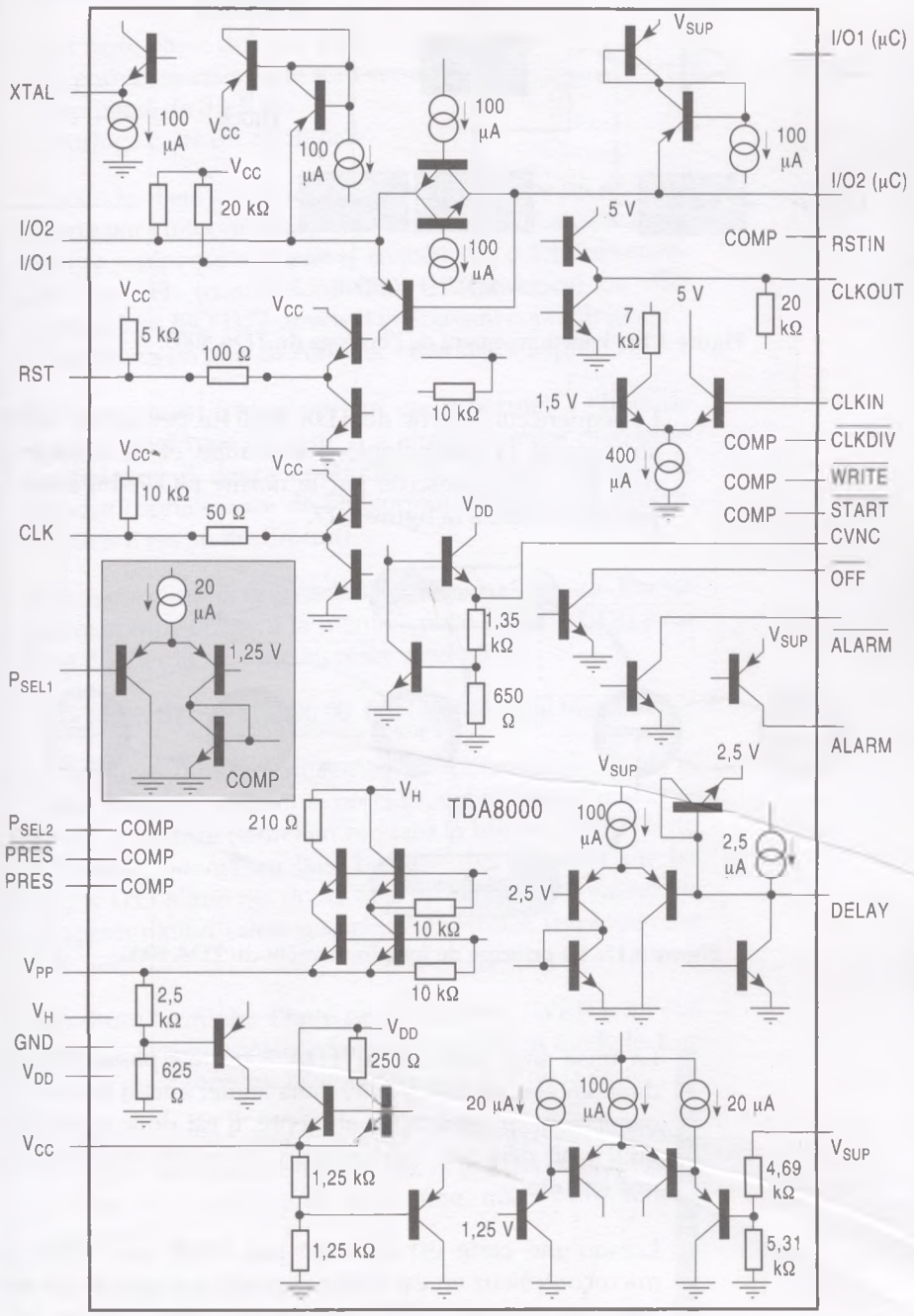



**Figure 3.15.** Structure des accès du TDA 8000.

© DUNOD - La photocopie non autorisée est un délit.

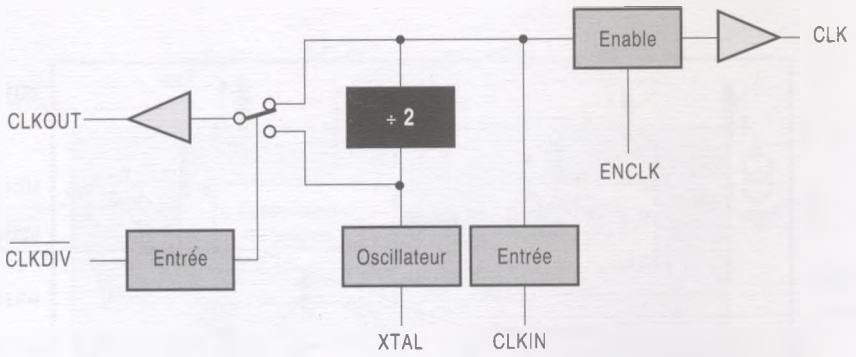



**Figure 3.16.** Fonctionnement de l'horloge du TDA 8000.

Le séquenceur interne du TDA 8000 lui permet de suivre strictement la chronologie d'activation et de désactivation des cartes prescrite par la norme ISO 7816, selon le principe défini à la figure 3.17.

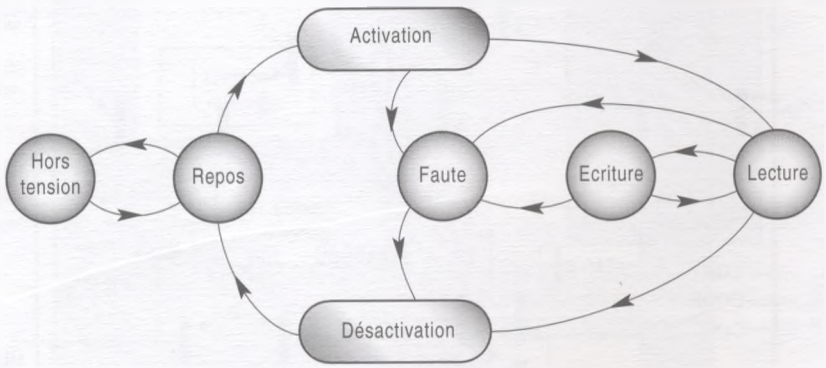



**Figure 3.17.** Le principe de fonctionnement du TDA 8000.

La mise sous tension du TDA 8000 fait passer celui-ci dans un état de repos (*idle*) dans lequel aucun contact du connecteur de carte n'est alimenté. Il est donc indifférent qu'il y ait déjà une carte dedans, ou qu'on en introduise une ensuite.

Lorsqu'une carte est détectée par PRES ou /PRES, le microcontrôleur en est informé par le passage au niveau haut de la ligne /OFF qui, généralement, déclenchera une interruption.

C'est alors le processeur qui prendra l'initiative d'entamer une session carte, en mettant la ligne /START au

niveau bas. La séquence suivante sera alors exécutée par le TDA 8000 :

– Vcc carte passe de 0 à 5 V ;
– les entrées-sorties carte sont connectées ;
– Vpp passe de 0 à 5 V ;
– l'horloge carte est appliquée.

À ce stade, il est classique que l'hôte déclenche un reset de la carte par l'intermédiaire de la ligne RSTIN. La carte émet alors sa « réponse au reset », séquence d'octets commençant par 3Fh (conventions ISO 1177 inverses) ou 3Bh (conventions ISO 1177 directes) et pouvant contenir jusqu'à 32 caractères en plus de cet octet « d'entête » baptisé TS.

Ce message est très important car il permet à l'hôte de savoir à quel type de carte il a affaire, quelles modalités de dialogue il devra appliquer, et, éventuellement, de prendre connaissance de l'historique succinct de la carte (15 caractères au maximum).

À titre d'exemple, une carte bancaire ou une carte France Télécom (qui utilisent la même « puce » BULL CP8) peuvent donner la réponse au reset suivante :

3F 65 35 10 01 04 6C 90 00 (en hexadécimal bien sûr).

Nous étions donc naturellement en mode lecture (*read*), et l'hôte peut maintenant si nécessaire déclencher une opération d'écriture (*write*) en mettant la broche /WRITE du TDA 8000 au niveau bas. Le sens des données sur les lignes I/O s'inverse donc, et Vpp passe à sa valeur de programmation selon une pente contrôlée (typiquement $1\ V\ .\ \mu s^{-1}$).

L'écriture terminée, l'hôte remet la ligne /WRITE à l'état haut. Le système revient immédiatement en mode lecture et peut donc recevoir l'éventuelle réponse de la carte.

En fin de session, une séquence de désactivation inverse de celle d'activation est exécutée, et le TDA 8000 retourne à l'état de repos, prêt pour une mise hors tension « propre » :

– un reset carte est exécuté ;
– l'horloge carte est arrêtée ;
– Vpp carte est ramené à zéro ;
– les lignes d'entrée-sortie sont mises en haute impédance ;
– Vcc carte est ramené à zéro.

© DUNOD - La photocopie non autorisée est un délit.

Naturellement, le TDA 8000 peut, à tout moment d'une session, se mettre en mode « faute » (*fault*) si l'une des anomalies suivantes est détectée :

– court-circuit sur Vcc ou Vpp ;
– courant excessif sur les lignes de données carte ;
– retrait de la carte en cours de session ;
– problème thermique.

Le TDA 8000 met alors la ligne /OFF à l'état bas et exécute spontanément une séquence de désactivation. La suite des événements est alors placée sous la responsabilité du microcontrôleur.

### Schéma d'application

L'application typique du TDA 8000 est illustrée par la figure 3.18.

Il s'agit de l'adjonction d'une fonction « carte à puce » à un système existant, dont le microcontrôleur assurera la gestion de la carte en plus de ses tâches de base.

La connexion du TDA 8000 se fait ici par l'un des ports d'entrée-sortie du 80C51, et par quelques lignes annexes (INT1 et RST).

Naturellement, cette simplicité matérielle aura pour contrepartie une certaine complication du logiciel, qui devra traiter les échanges de données avec la carte selon un protocole qui n'est pas forcément simple (tout dépend du ou des types de cartes qu'il faut pouvoir accepter).

## LES COUPLEURS DE CARTE

Dans la terminologie en vigueur dans le monde des cartes à puce, le mot « coupleur » désigne un sous-ensemble intelligent capable de communiquer d'un côté avec un maximum de types de cartes, et de l'autre avec n'importe quel environnement applicatif courant.

Si les échanges de données entre le coupleur et les cartes à puce se font selon des protocoles très stricts, en revanche le dialogue entre l'hôte et le coupleur peut avoir lieu dans un langage de plus haut niveau facile à mettre en œuvre sans connaissances particulières de la norme ISO 7816.

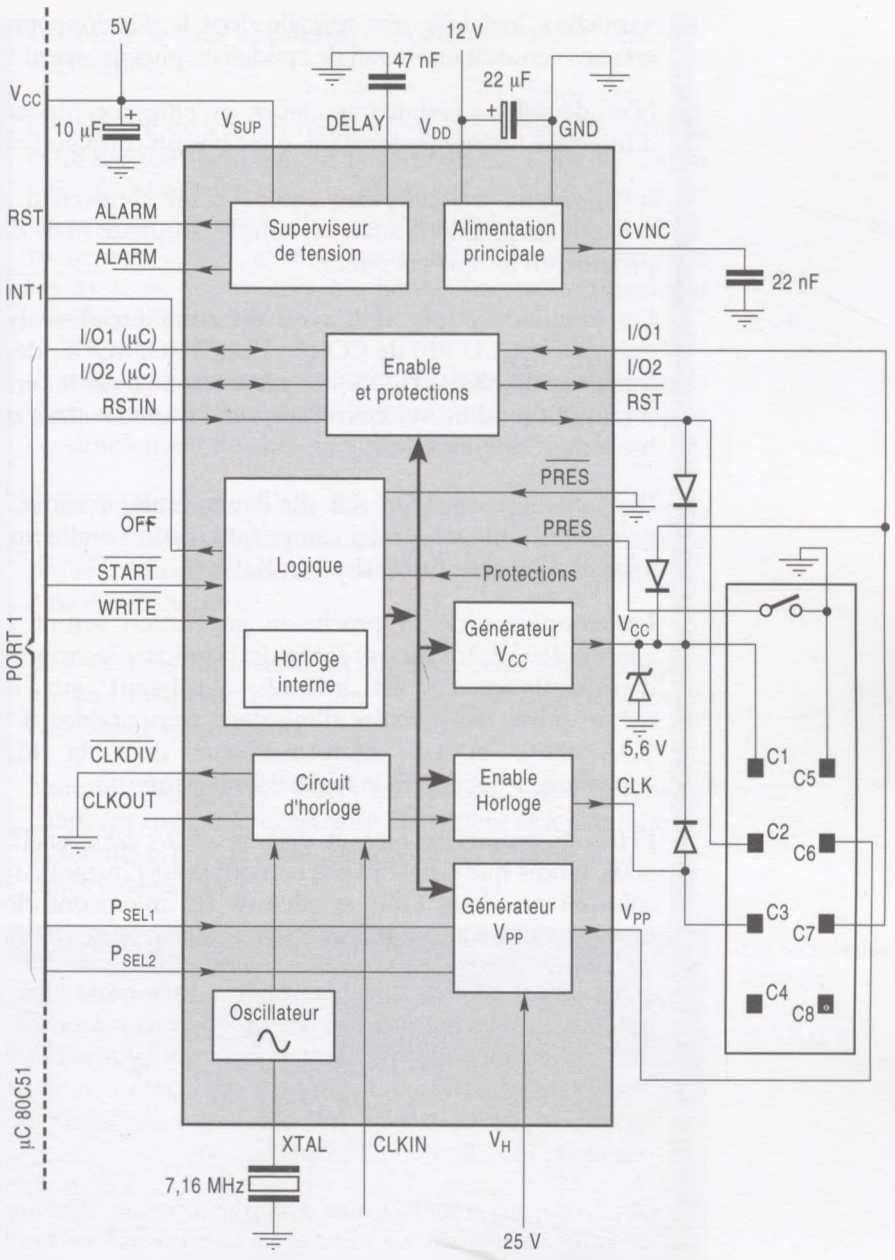



**Figure 3.18.** Schéma d'application du TDA 8000.

Bref, beaucoup plus que l'interface électrique que nous venons d'examiner, le coupleur est plutôt la solution « clef en main » permettant d'accéder de façon simple et fiable aux multiples applications des cartes à puce.

Tout coupleur digne de ce nom comprend donc nécessairement un microcontrôleur embarqué, qui met en œuvre une

© DUNOD - La photocopie non autorisée est un délit.

« couche » logicielle très spéciale dont le développement est sans conteste un travail de spécialiste plus qu'averti.

N'en déplaise à certains vendeurs, un simple composant d'interface, même performant, n'est pas un coupleur.

Inversement, un coupleur équipé d'un connecteur de cartes n'est plus tout à fait un simple coupleur, mais déjà presque un lecteur-encodeur.

Les premiers coupleurs à avoir été commercialisés (par exemple le CCU 910 de COREL ÉLECTRONIQUE, développé par INNOVATRON), se présentaient sous la forme d'un petit module sur circuit imprimé multicouches, réalisé en technologie CMS.

Pouvant être considéré (et d'ailleurs câblé) comme un gros circuit intégré, un tel composant souffre malheureusement d'un coût de fabrication élevé.

Les coupleurs de la prochaine génération seront par conséquent, grâce aux progrès de la micro-électronique, d'authentiques circuits intégrés réunissant, sur une même puce, des circuits d'interface comparables à un TDA 8000, et un microcontrôleur dont la ROM « masquée » hébergera le logiciel embarqué.

PHILIPS propose d'ores et déjà ses TDA 8005 et TDA 8006, tandis que GEMPLUS s'en tient pour l'instant à une solution en deux boîtiers séparés (le microcontrôleur masqué « GemCore » et le circuit d'interface GIC 100).

Dans un cas comme dans l'autre, le simple particulier ne doit guère espérer pouvoir se procurer commodément ces composants qui, bien souvent, seront plus ou moins réservés à telle ou telle « grosse » application comme les terminaux de paiement, les décodeurs de télévision à péage, ou les téléphones portables.

Qu'à cela ne tienne, nous découvrirons au chapitre 5 comment construire de toutes pièces un coupleur simplifié à partir de composants des plus courants.

## LES LECTEURS DE CARTES À PUCE

Par abus de langage, et peut-être par assimilation aux lecteurs de disquettes, on appelle « lecteurs » de cartes à puce des appareils souvent capables aussi bien de lire que d'écrire dans celles-ci.

Le terme le plus approprié est par conséquent « lecteur-encodeur ».

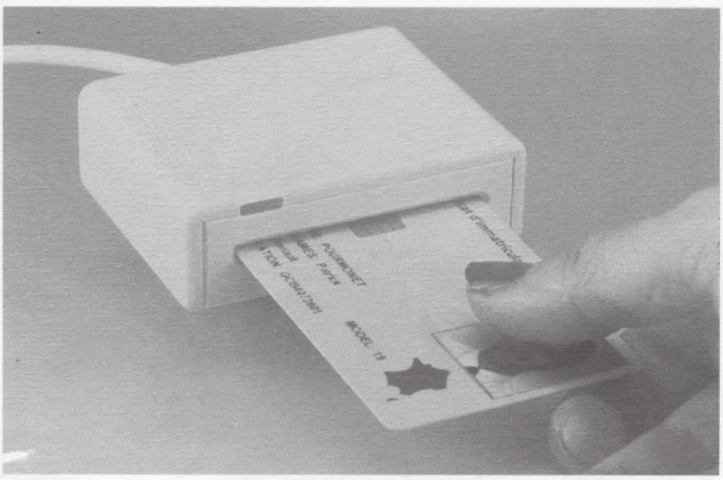
D'un point de vue terminologique, un lecteur de cartes à puce est tout simplement la réunion dans un boîtier ou sur un simple circuit imprimé, d'un coupleur, d'un connecteur de cartes, d'un système d'alimentation (éventuellement à pile), et d'un circuit assurant la liaison avec un système informatique « hôte » (microcontrôleur ou micro-ordinateur).

Certains lecteurs pourront être autonomes, et donc dotés d'un afficheur et, éventuellement, d'un clavier complet ou simplement de quelques boutons.

C'est notamment le cas des lecteurs « porte-clefs » qui, très peu coûteux, commencent à servir aussi bien pour lire le crédit de télécartes que pour gérer un « porte-monnaie électronique ».

Des versions équipées d'un émetteur-récepteur radio permettent même de transformer une carte à puce normale en « badge sans contact ».

Naturellement, nous découvrirons dans les prochains chapitres comment construire facilement et à peu de frais différents types de lecteurs-encodeurs adaptés à de multiples usages.



Un lecteur-encodeur du commerce (le LEXUS).

Mais pour les applications les plus exigeantes, il reste bien sûr toujours possible d'acquérir un lecteur professionnel tout fait comme, par exemple, le tout petit LEXUS d'ELEA Cardware.

© DUNOD - La photocopie non autorisée est un délit.

On peut aussi se tourner vers un « kit de développement » complet, dont le principal intérêt est de contenir, la plupart du temps, un échantillonnage de cartes neuves.

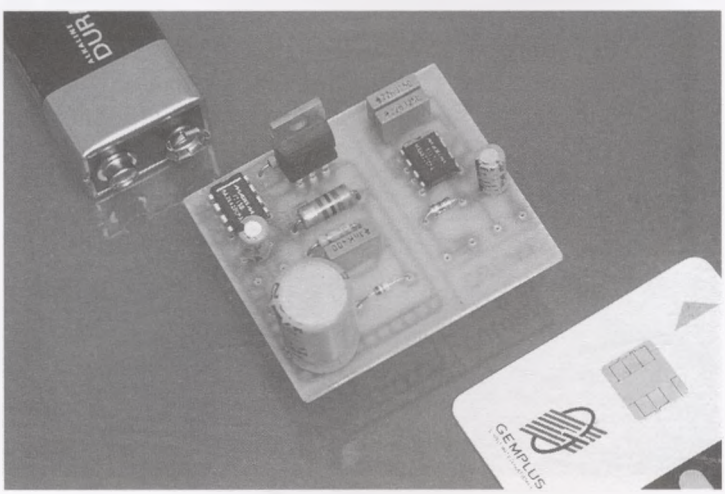
Bien que les prix aient considérablement baissé en quelques années seulement, une telle approche demeure tout de même très sensiblement plus coûteuse...

## DEUX ALIMENTATIONS 21 V POUR CARTES À PUCE

Même si la tendance est aux cartes à puce EEPROM à alimentation 5 V unique, beaucoup de circuits intégrés pour cartes encore très répandus nécessitent une tension de programmation de 21 V.

S'il n'est guère compliqué de faire produire cette tension par une alimentation secteur spécialisée, il en va en revanche tout autrement lorsqu'il faut travailler sur piles ou dans un système alimenté d'origine en 5 ou 12 V seulement.

La plupart du temps, la solution prendra la forme d'un petit convertisseur continu-continu, dont nous allons décrire deux variantes radicalement différentes.




Les deux alimentations réunies sur un même circuit imprimé.

Les deux principales techniques permettant d'élever à 21 V une tension continue de 5 à 12 V sans inversion de polarité sont la conversion à découpage ou à pompe de charge.

Capable de produire facilement des courants relativement importants, la première souffre du double inconvénient de nécessiter un bobinage (*self* ou transformateur) et de présenter des risques de rayonnement HF, bien qu'une conception soigneuse puisse en minimiser sérieusement l'impact.

La seconde est plus simple à mettre en œuvre et nettement moins « polluante », mais ses limites en courant sont vite atteintes. Le choix ne sera donc pas toujours évident.

Mais il faut savoir que la consommation d'une carte à puce sur son Vpp peut se situer dans une très large fourchette : de moins de 500 µA pour une mémoire EEPROM sécurisée comme la GPM 416 (composant ST 1301) à plus de 20 mA pour une carte à microprocesseur et EPROM (composant ST 1834).

Un convertisseur à découpage conçu pour débiter entre 25 et 100 mA conviendra donc en principe à toutes les applications envisagées ici, mais il pourra en revanche être avantageux de se rabattre sur une pompe de charge si on n'a à programmer que des cartes à EEPROM bitension affichant une consommation de l'ordre du milliampère.

## Un convertisseur 5 à 12 V / 21 V à découpage

On ne peut guère s'attaquer à la conception d'un convertisseur continu-continu à découpage sans s'intéresser aux circuits intégrés MAXIM spécialement destinés à cet usage.

Cependant, leur technologie CMOS s'accommode mal de tensions supérieures à une quinzaine de volts.

Deux artifices permettent de contourner plus ou moins élégamment cet obstacle : l'utilisation d'un transformateur élévateur en lieu et place d'une simple *self*, ou l'utilisation d'un transistor découpeur externe puisqu'il est alors possible de s'arranger pour que l'électronique de commande ne soit soumise qu'à une tension réduite.

Le schéma de la figure 3.19 fait donc appel à un MAX 643, composant dépourvu de MOSFET interne et donc plutôt destiné à la réalisation de convertisseurs à courant relativement élevé.

© DUNOD - La photocopie non autorisée est un délit.

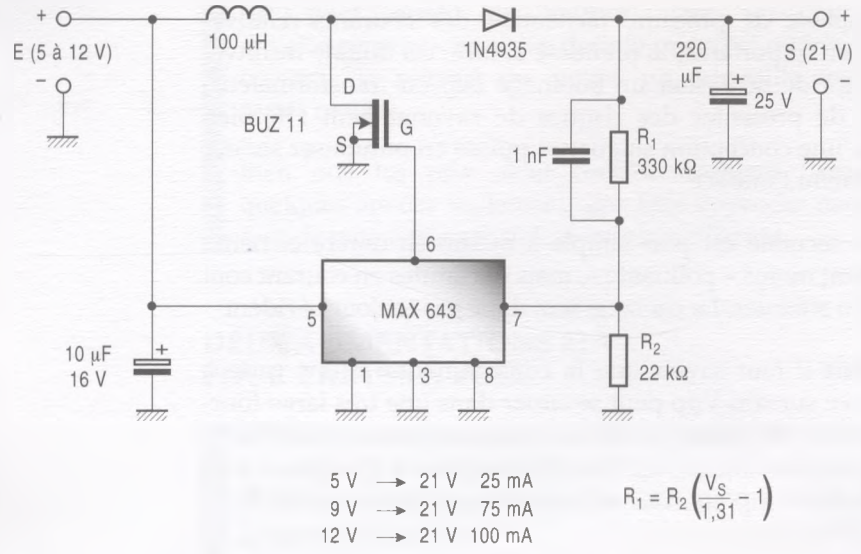



**Figure 3.19.** Schéma du convertisseur à découpage.

La configuration classique de la figure 3.20 est applicable aussi bien aux MAX 641, 642, et 643. Seule la tension de sortie (fixe) varie.

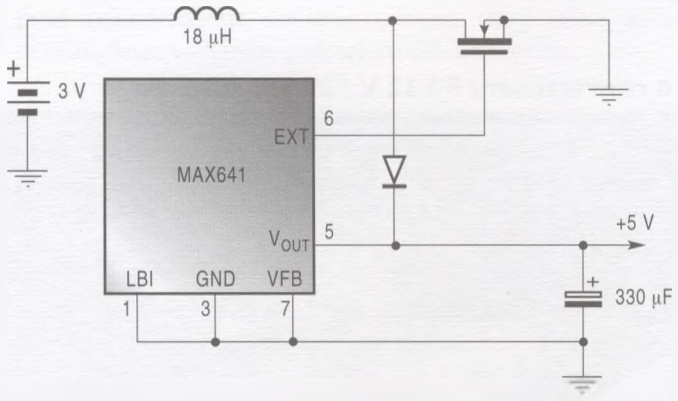



**Figure 3.20.** Schéma d'application du MAX 643.

En ce qui nous concerne, nous exploiterons différemment le brochage de la figure 3.21 en mettant à contribution la broche 7 (VFB).

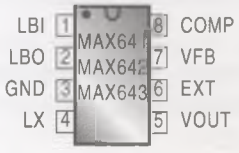



**Figure 3.21.** Brochage du MAX 643.

Grâce à un pont diviseur externe, cette entrée permet en effet d'ajuster la tension de sortie dans une large plage et donc d'utiliser indifféremment n'importe laquelle des trois références.

Autre originalité de ce schéma, la broche 5 (VOUT) est reliée à la tension d'entrée et non à celle de sortie, trop élevée pour elle.

Nous avons confié le découpage à un BUZ 11, MOS de puissance capable de commuter 30 ampères ! Ce surdimensionnement plutôt généreux ne coûte pas bien cher, mais permet de bénéficier d'une résistance passante particulièrement faible (0,04 Ω).

Il serait naturellement possible de se contenter de transistors plus modestes (encore que d'encombrement identique) comme l'IRFZ 14, sans dégradation sensible des performances.

Chacun sait que la *self* joue un rôle crucial dans ce type de convertisseur. Contrairement à ce que l'on pourrait imaginer à première vue, sa valeur doit être d'autant plus faible que le courant à produire est élevé. Cela s'explique par le fait qu'une inductance limite d'autant plus les variations de courant que sa valeur est plus élevée. Or, le principe même de la conversion d'énergie par découpage consiste à faire varier le courant dans la *self* !

Nous avons donc porté à 100 µH la valeur de 18 µH préconisée dans le schéma d'application standard, ce qui mène aux performances suivantes :

– 21 V / 26 mA à partir de +5 V ;
– 21 V / 75 mA à partir de +9 V ;
– 21 V / 100 mA à partir de +12 V.

Cela en utilisant une simple *self* moulée, préférable à un bobinage sur tore de ferrite dans les conditions de fréquence et de courant qui sont les nôtres.

Un modèle particulièrement bien adapté est le KGAD de COREL Électronique (en forme de résistance 11 mm × 4 mm). Le modèle de 100 µH est en effet capable de supporter, sans saturer, un courant de 400 mA.

Pour ce qui est de la diode, la rapidité de recouvrement est capitale. Un bon choix pourra être la 1N 4935, mais on peut aussi se contenter d'une BAT 86 (diode Schottky) en se limitant à un courant de crête de 500 mA.

© DUNOD - La photocopie non autorisée est un délit.

## Un convertisseur 10 V / 21 V à pompe de charge

Le MAX 622, dont la figure 3.22 reproduit le brochage, est l'un des quelques circuits intégrés convertisseurs de MAXIM capables de supporter directement jusqu'à 27 V.

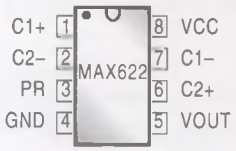



**Figure 3.22.** Brochage du MAX 622.

Il contient une pompe de charge à huit interrupteurs et trois condensateurs théoriquement capable de quadrupler la tension de départ.

En pratique, l'élévation est limitée à 11 V par un circuit de régulation interne, cette tension venant tout simplement s'ajouter à celle d'entrée.

À partir d'une tension de 3,5 à 16,5 V, on peut donc produire 14,5 à 27,5 V, soit en ce qui nous concerne, pas loin de 21 V à partir d'une pile 9 V fraîche ou d'une alimentation de 12 V, moyennant si nécessaire une pré ou post-régulation rudimentaire.

Le courant disponible est normalement de l'ordre du milliampère, mais nous avons pu extraire le triple, sans chute de tension décelable, du schéma de la figure 3.23 qui n'a pourtant rien de particulier si ce n'est une certaine optimisation des valeurs de condensateurs.

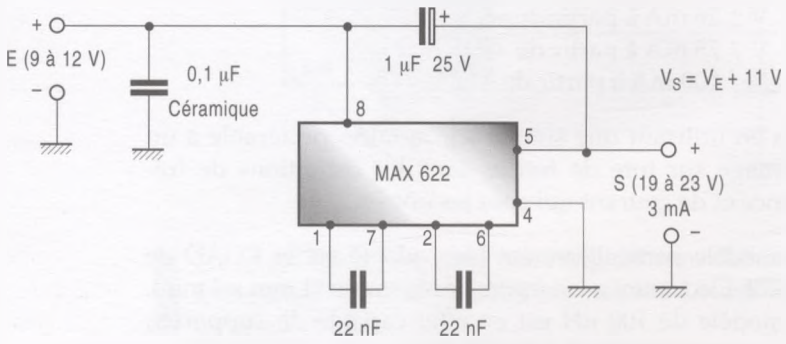



**Figure 3.23.** Schéma du convertisseur à pompe de charge.

Ce montage conviendra donc sans problème à la quasi-totalité des cartes à EEPROM bitension.

## RÉALISATION PRATIQUE

Comme toujours en matière d'alimentations à découpage, la topographie du circuit imprimé est critique, notamment au niveau des masses.

On veillera surtout à graver avec précision le tracé de la figure 3.24, le plus délicat, avant de câbler le montage selon le plan de la figure 3.25.

Le tracé de la figure 3.26, qui se rapporte à la pompe de charge, est moins critique et correspond au plan de câblage très simple de la figure 3.27.

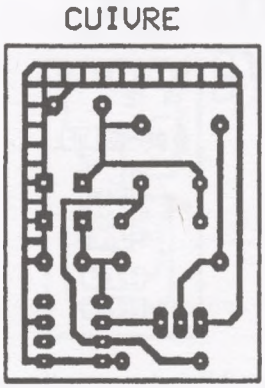



**Figure 3.24.** Circuit imprimé du convertisseur à découpage.

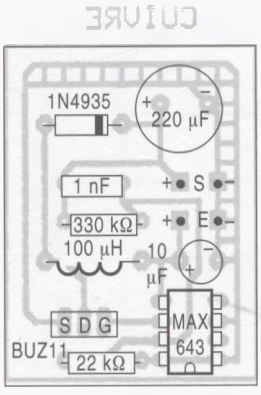



**Figure 3.25.** Plan de câblage du convertisseur à découpage.

*Liste des composants*

**Résistances (5 % 1/4W) :**
R1 : 22 kΩ,
R2 : 330 kΩ.

**Condensateurs :**
C1 : 10 µF 16 V,
C2 : 220 µF 25 V,
C3 : 1 nF.

**Transistors :**
T1 : BUZ 11 ou IRFZ 14.

**Circuits intégrés :**
CI1 : MAX 643.

**Autres semi-conducteurs :**
D1 : 1N 4935.

**Divers :**
L1 : *self* moulée 100 µH.

© DUNOD - La photocopie non autorisée est un délit.

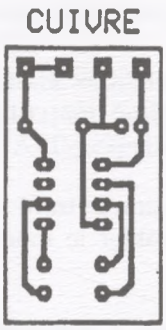



**Figure 3.26.** Circuit imprimé du convertisseur à pompe de charge.

*Liste des composants*

**Condensateurs :**
C1 et C2 : 22 nF,
C3 : 0,1 µF,
C4 : 1 µF 25 V.

**Circuits intégrés :**
CI1 : MAX 622.

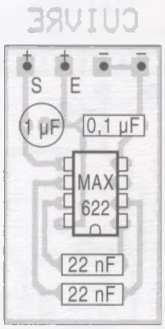



**Figure 3.27.** Plan de câblage du convertisseur à pompe de charge.

CHAPITRE PAGE

| | | |
|---|---|---|
| 1 | Vocabulaire et normalisation | 1 |
| 2 | Les circuits intégrés pour cartes à puce | 13 |
| 3 | La périphérie des cartes | 37 |

# 4 MISE EN ŒUVRE DES CARTES SYNCHRONES

**Un lecteur-encodeur de « 1re génération »** 68
**Un lecteur-encodeur de 2e génération** 80
**Les cartes à puce I2C** 97

| | | |
|---|---|---|
| 5 | Applications pratiques des cartes synchrones | 105 |
| 6 | Introduction aux cartes asynchrones | 125 |
| 7 | Le cédérom du livre | 157 |

La façon la plus simple de partir concrètement à la découverte des cartes à puce consiste à expérimenter autour de cette matière première gratuite et quasiment inépuisable que sont les télécartes usagées ou les autres cartes jetables servant, par exemple, à payer les lavages de voitures ou le stationnement.

Si nous avons révélé, dès 1989, à nos lecteurs comment lire et écrire dans ces composants alors entourés d'un épais mystère (et cela a fait grincer quelques dents à l'époque...), il nous faut aujourd'hui tenir compte de l'évolution technologique (et psychologique !) intervenue ces dernières années.

Il est maintenant amplement démontré qu'il ne suffit pas de savoir lire et écrire dans les cartes à puce pour « pirater » les applications correctement protégées.

En revanche, cela permet de prendre connaissance du contenu détaillé de bien des cartes qui nous concernent directement dans notre vie courante, et même de mettre sur pied des applications personnelles parfois étonnantes.

Il serait vraiment dommage de s'en priver...

## UN LECTEUR-ENCODEUR DE « 1re GÉNÉRATION »

L'avenir des cartes à puce se situe sans le moindre doute du côté de la technologie EEPROM CMOS monotension, mais de très nombreuses applications font encore usage de cartes nécessitant une tension de programmation de 21 V.

Même l'application phare qu'est la télécarte française n'en finit pas de passer à la « T2G » pourtant annoncée depuis des années mais qui hésite à quitter le stade expérimental.

Le lecteur-encodeur dont le schéma apparaît sur la figure 4.1 est entièrement compatible avec tous ceux que nous avons mis au point au fil des années, notamment au niveau des logiciels d'exploitation, mais il supporte une plus grande variété de cartes.

Il est alimenté sur le secteur, par l'intermédiaire d'un transformateur « prise de courant » devant fournir entre 9 et 12 V en alternatif sous au moins 100 mA.

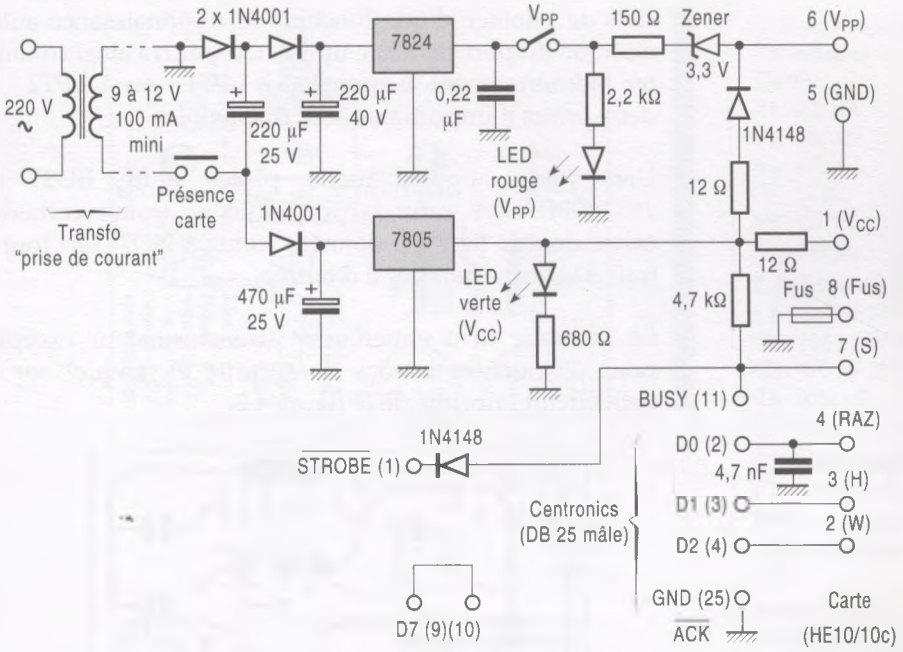



**Figure 4.1.** Schéma du lecteur-encodeur.

Le +5 V (Vcc) est produit par un redresseur monoalternance associé à un régulateur 7805, tandis que l'alimentation 21 V (Vpp) utilise un doubleur de tension et un régulateur 7824 associé à une diode zener montée en soustractrice de tension.

Une amélioration importante (qui pourrait d'ailleurs facilement être appliquée aux versions précédentes) concerne l'adjonction d'une résistance de charge (4,7 kΩ) sur la sortie de la carte. En effet, la sortie des cartes les plus récentes est du type « drain ouvert » contrairement à celle des télécartes.

Pas de changement en ce qui concerne le pilotage de la carte par le port parallèle (Centronics) d'un compatible PC, si ce n'est l'adjonction facultative d'un condensateur de 4,7 nF sur la ligne de RESET, destiné à éviter de possibles remises à zéro intempestives des cartes du type GPM 416. On s'abstiendra donc de le câbler si on n'envisage pas d'opérer sur de telles cartes ou si le défaut ne se produit pas (cela dépend du PC utilisé, et de la longueur du câble de raccordement).

La liaison directe entre les broches 9 (D7) et 10 (/ACK) de la prise Centronics permet, pour sa part, de doter les logi-

© DUNOD - La photocopie non autorisée est un délit.

ciels de pilotage d'une fonction de reconnaissance automatique du port parallèle utilisé. On pourra ainsi connecter indifféremment le montage à LPT1 : ou à LPT2 : si deux prises d'imprimante sont disponibles.

Une diode supplémentaire placée entre BUSY et /STROBE offre enfin la possibilité de traiter certaines cartes dont la ligne de données (contact ISO7) sert tour à tour de sortie, mais aussi d'entrée.

Le montage tient entièrement (transformateur excepté, pour d'évidentes raisons de sécurité électrique) sur le petit circuit imprimé de la figure 4.2.

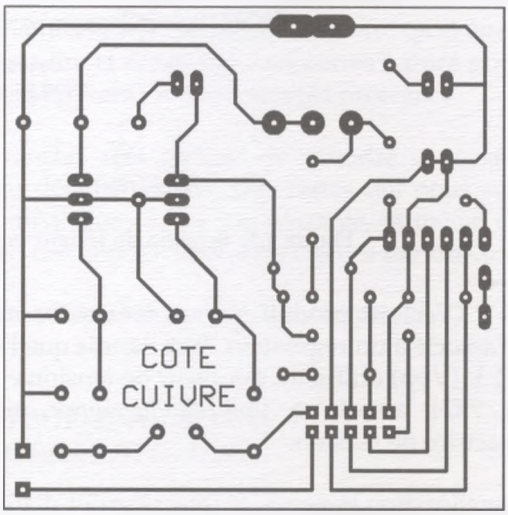



**Figure 4.2.**
Le circuit imprimé du lecteur-encodeur.

La figure 4.3 fournit le plan d'implantation des composants. Parmi ceux-ci, on remarquera un tronçon de cinq éléments d'une barrette sécable à doubles picots carrés (coudés ou droits, au choix).

C'est ici qu'il faudra brancher, par l'intermédiaire d'un cordon réalisé selon la figure 3.2, un connecteur de carte construit d'après les figures 3.3 et 3.4.

Ce même cordon pourrait d'ailleurs servir à relier au montage, sans modification aucune, un connecteur pour clefs à mémoire SEFEA, en vue de la lecture et de la programmation de tels « objets portables » à mémoire.

Le raccordement au port parallèle du PC (fiche DB25 mâle avec capot) se fera au moyen d'un câble à 8 conducteurs d'une cinquantaine de centimètres de long.

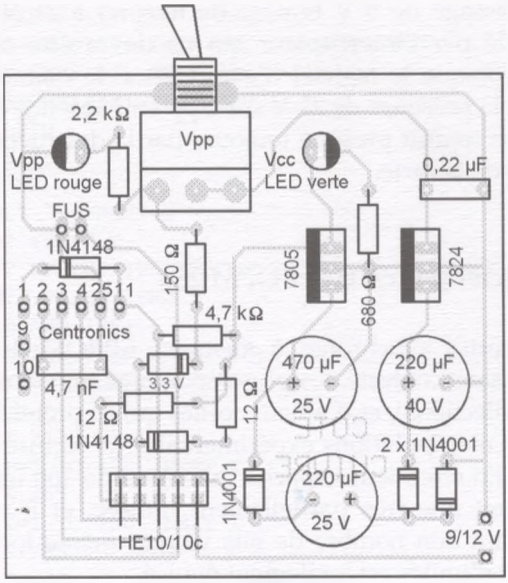



**Figure 4.3.** Plan de câblage du lecteur-encodeur.

*Liste des composants*

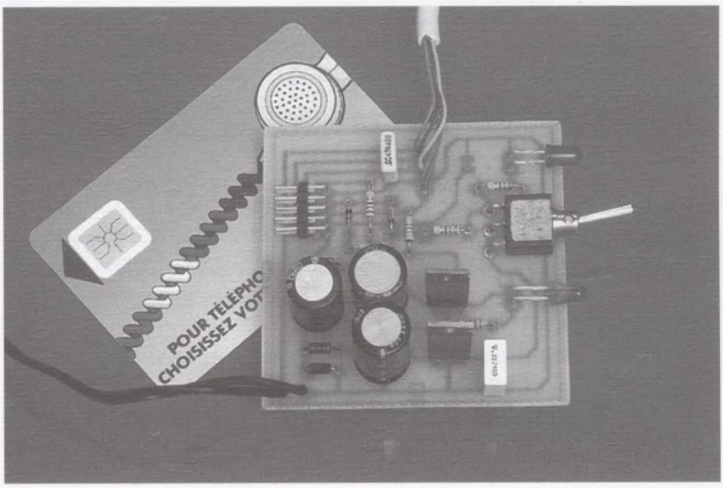
**Résistances (5 % 1/4W) :**
R1 : 2,2 kΩ,
R2 : 150 Ω,
R3 : 4,7 kΩ,
R4 : 12 Ω,
R5 : 12 Ω,
R6 : 680 Ω.

**Condensateurs :**
C1 : 220 µF 25 V,
C2 : 220 µF 40 V,
C3 : 470 µF 25 V,
C4 : 0,22 µF,
C5 : 4,7 nF.

**Circuits intégrés :**
CI1 : régulateur 7805,
CI2 : régulateur 7824.

**Autres semi-conducteurs :**
D1 à D3 : 1N 4001,
D4 : 1N 4148,
D5 : zener 3,3 V 0,25 W,
D6 : LED rouge,
D7 : LED verte.

**Divers :**
Transformateur « prise de courant » 9 à 12 V alternatif 100 mA,
Inverseur unipolaire pour circuit imprimé (APR),
Barrette sécable à doubles picots coudés,
Câble 5 conducteurs,
Prise DB25 mâle avec capot,
Connecteur de carte (fig. 3.4),
Cordon de liaison (fig. 3.2).



Le lecteur-encodeur de 1re génération.

Un voyant vert signale que le montage est sous tension à la suite de l'insertion d'une carte (utilisation du contact de détection du connecteur), et un voyant rouge que la tension Vpp est à sa valeur de programmation.

© DUNOD - La photocopie non autorisée est un délit.

Le passage de 5 V (valeur de lecture) à 21 V est commandé par l'interrupteur qui ne devra être manœuvré que lorsque le logiciel d'exploitation le demandera. En effet, la présence de 21 V sur Vpp en l'absence de 5 V sur Vcc se traduit presque toujours par la destruction immédiate de la carte.

## Un logiciel pour T1G et GPM 256

Les cartes synchrones à mémoire EPROM de 256 bits sont, sans conteste, les plus répandues (notamment dans les collections), et d'ailleurs celles qui se prêtent le mieux à des manipulations expérimentales de lecture et d'écriture. En effet, leur capacité théorique de 160 unités n'est souvent que très partiellement utilisée, et il y subsiste ainsi un bon nombre de bits vierges même lorsque leur crédit d'unités est totalement épuisé.

Le logiciel MANIPT1G.BAS permet d'expérimenter commodément autour de télécartes « T1G » de FRANCE TELECOM, et de cartes privatives telles que les cartes de lavage de voiture utilisables dans les stations-service BP et MOBIL, les cartes de PIAF, etc.

```
10 REM ---- MANIPT1G.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 OUT S,0:KEY OFF :CLS
120 PRINT"Insérer une T1G puis presser ENTER" :PRINT
130 INPUT Z$ :CLS
140 PRINT"APPLIQUER LE Vpp puis presser ENTER" :PRINT
150 INPUT Z$ :CLS
160 PRINT"   barre d'espace : avance lecture"
170 PRINT"   touche +       : mise à 1 de bit"
180 PRINT"   touche ESCape : quitter"
190 PRINT
200 OUT S,250
210 OUT S,248
220 FOR F=1 TO 8
230 FOR G=1 TO 8
240 FOR H=1 TO 4
250 OUT S,249
260 D=INP(E) :GOSUB 380
```

```
270 Z$=INKEY$ :IF Z$="" THEN 270
280 IF Z$=CHR$(27) THEN OUT S,0:GOTO 360
290 IF Z$=CHR$(43) THEN 420
300 IF Z$=CHR$(32) THEN 320
310 GOTO 270
320 OUT S,251
330 NEXT H
340 PRINT" "; :NEXT G
350 PRINT :NEXT F
360 PRINT :PRINT :PRINT"COUPER LE Vpp" :PRINT :BEEP
370 PRINT :PRINT :END
380 K= (D AND 128)
390 IF K<>128 THEN PRINT"1";
400 IF K=128  THEN PRINT"0";
410 RETURN
420 OUT S,253
430 FOR T=1 TO 150 :NEXT T
440 OUT S,255
450 FOR T=1 TO 150 :NEXT T
460 OUT S,253
470 OUT S,249
480 IF INKEY$<>"" THEN 480
490 GOTO 270
500 REM (c)1995 Patrick GUEULLE
```

Ce logiciel exploite le mode de fonctionnement naturel de ces cartes, et offre donc un accès « séquentiel » à leur mémoire au moyen des micro-instructions de la figure 2.3.

Dès qu'une carte est insérée, elle est remise à zéro et le premier bit de sa mémoire est affiché. Il suffit de presser la barre d'espace du clavier pour passer au suivant, avec possibilité de répétition automatique si on désire avancer rapidement.

La figure 4.4 montre le genre de résultat obtenu. Il est possible d'imprimer celui-ci sur papier en déclenchant une recopie d'écran si le lecteur est branché sur LPT2 : et l'imprimante sur LPT1 :.

On remarquera qu'il est prévu de lire un maximum de 256 bits, chiffre qui correspond exactement à la capacité des GPM 256. Il serait facile de modifier cette valeur (à la ligne 220) pour opérer, le cas échéant, sur des cartes moins communes.

Dans le cas précis des T1G de FRANCE TELECOM, la figure 4.5 fournit quelques repères utiles.

La zone des 96 premiers bits, définitivement protégée contre l'écriture par la destruction en usine du fameux fusible, est réputée unique pour chaque télécarte en circu-

© DUNOD - La photocopie non autorisée est un délit.

TELECARTE 50 UNITES (épuisée):

```
1 0 1 1  1 1 1 1  0 0 0 0  0 0 1 1  1 0 0 0  0 1 1 0  0 1 1 0  1 0 0 1
1 0 1 1  0 0 1 1  0 0 1 1  0 1 1 0  0 1 1 0  0 1 0 0  0 1 0 1  1 1 0 1
1 1 0 0  1 0 1 1  0 0 0 0  1 1 0 1  0 0 0 1  0 0 0 0  0 0 0 0  0 1 1 0

1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  1 1 1 1  1 1 1 1
```

CARTE LAVAGE MOBIL (24 unités, neuve):

```
1 0 0 0  1 0 0 0  1 0 0 0  0 0 0 0  0 0 1 0  0 0 0 0  0 0 0 0  0 0 1 0
0 0 1 1  1 1 0 0  0 1 1 1  0 1 0 1  1 0 0 0  0 0 1 0  0 0 1 0  0 1 0 0
1 0 1 0  0 0 0 1  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 1

0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
```

CARTE DE PIAF:

```
0 1 1 0  1 1 1 0  1 0 0 1  1 0 1 0  1 1 0 0  0 0 0 0  0 0 0 1  0 1 1 1
0 1 1 0  0 0 0 0  0 0 0 0  0 0 0 0  1 0 0 1  0 1 0 1  1 1 1 0  1 1 0 1
1 0 0 1  0 1 0 1  1 0 1 0  1 1 0 0  0 1 0 1  1 0 1 0  0 0 0 0  0 0 0 0

0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0  0 0 0 0
```

**Figure 4.4.** Quelques exemples de contenus de GPM 256.

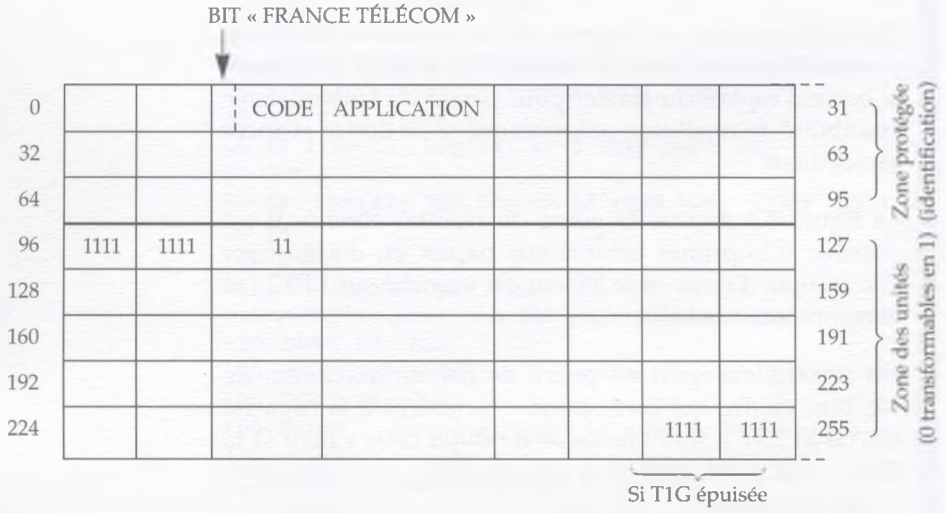



**Figure 4.5.** Plan mémoire des T1G.

lation. Elle associe son numéro de série à un « message d'authenticité » crypté, et à un code baptisé « pouvoir financier » qui fixe le nombre d'unités disponibles lorsque la carte est neuve.

On retiendra que le bit situé à l'adresse 8 n'est en principe à 0 que sur les cartes émises par FRANCE TÉLÉCOM, que les bits 8 à 15 hébergent un « code application » qui était 03h sur les premières T1G mais qui augmente au fil des séries successives, que les dix premiers bits de la « zone des unités » sont mis à 1 en usine lors des tests, et que ses huit derniers bits sont presque toujours à 1 sur les T1G épuisées.

Les choses peuvent être fort différentes dans le cas de GPM 256 dédiées à d'autres applications. Toutes les « cartes lavage » BP ou MOBIL sont, par exemple, strictement identiques pour une valeur faciale donnée (12 ou 24 unités), mais on y « grille » toujours un bit par unité consommée.

À condition que le bit courant se situe dans une zone non protégée en écriture (c'est-à-dire au delà de l'adresse 95 si le fusible est bien détruit), il est possible de le transformer irréversiblement en 1 s'il est encore à 0. Il faut pour cela appuyer sur la touche + (signe plus) du pavé numérique.

L'affichage n'en sera pas affecté, puisque ce bit avait déjà été lu et qu'il n'est pas possible de faire reculer le compteur d'adresses sans repasser par zéro (en commandant un RESET, ou en « faisant le tour »).

En pratique, ce genre d'opération se fera dans la zone qui reste inutilisée après la consommation de toutes les unités, car il est peu probable que vous souhaiterez faire baisser le crédit de cartes encore utilisables...

Tout l'intérêt de l'opération est la possibilité qu'elle offre de « personnaliser » des cartes usagées pour les utiliser dans toutes sortes de serrures électroniques ou de dispositifs de sécurité informatique. Nous y viendrons !

À tout moment, il est possible de quitter le programme en pressant la touche ESCape, auquel cas aucune opération d'écriture n'intervient.

Il suffira alors de relancer le logiciel par un simple RUN (touche F2) pour reprendre la lecture au début de la mémoire, et constater ainsi l'effet des manœuvres précédentes.

Il est important de remarquer que la valeur 150 dans les lignes 430 et 450 du programme fixe la durée de l'impulsion de programmation, et qu'il s'agit là d'une valeur

© DUNOD - La photocopie non autorisée est un délit.

plus ou moins « passe-partout ».

Il n'y aurait que des avantages à l'ajuster, sous le contrôle d'un oscilloscope, en fonction des caractéristiques réelles du PC utilisé, de façon à obtenir approximativement 50 ms.

Il est par exemple recommandé d'utiliser la valeur 50 avec les vieux PC cadencés à 4,77 ou 8 MHz, mais on pourra être amené à excéder 150 avec les matériels les plus récents qui taquinent allègrement les 300 MHz à l'heure où nous écrivons ces lignes.

## Un logiciel intégré pour télécartes

```
10 REM ---- GPM256.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 DIM N(256):DIM M(256)
120 PRINT"CARTES A PUCE EPROM 256 BITS"
130 PRINT"============================":PRINT
140 PRINT :GOTO 380
150 OUT S,0:CLS
160 PRINT"Insérer carte, puis presser ENTER"
170 INPUT Z$ :CLS
180 PRINT"---- LECTURE CARTE EN COURS ----"
190 OUT S,250:OUT S,248
200 FOR F=1 TO 256
210 OUT S,249
220 D=INP(E) :D= (D AND 128)
230 N(F)=1:IF D= 128 THEN N(F)=0
240 OUT S,251
250 NEXT F
260 CLS :I=0
270 FOR F=1 TO 8
280 FOR G=1 TO 8
290 FOR H=1 TO 4
300 I=I+1
310 N$="1":IF N(I)=0 THEN N$="0"
320 PRINT N$;
330 NEXT H
340 PRINT" "; :NEXT G
350 PRINT
360 IF F=3 THEN PRINT
```

```
370 NEXT F :PRINT
380 PRINT"CHOIX + ENTER :" :PRINT
390 PRINT"0  -->  Retour au DOS (quitter)"
400 PRINT"1  -->  Lecture"
410 PRINT"2  -->  Interprétation"
420 PRINT"3  -->  Sauvegarde"
430 PRINT"4  -->  Chargement"
440 PRINT"5  -->  Programmation"
450 PRINT"6  -->  Vérification"
460 PRINT"7  -->  Affichage"
470 PRINT"9  -->  Appel du DOS (shell)"
480 INPUT Z$
490 IF Z$="0" THEN SYSTEM
500 IF Z$="1" THEN 150
510 IF Z$="2" THEN 820
520 IF Z$="3" THEN 590
530 IF Z$="4" THEN 740
540 IF Z$="5" THEN 1090
550 IF Z$="6" THEN 1260
560 IF Z$="7" THEN 260
570 IF Z$="9" THEN SHELL :CLS :GOTO 380
580 GOTO 480
590 CLS :PRINT"Nom à donner au fichier .CAR ?"
600 INPUT S$ :S$=S$+".CAR"
610 OPEN S$ FOR OUTPUT AS #1
620 I=0
630 CLS :PRINT"---- SAUVEGARDE EN COURS ----"
640 FOR F=1 TO 8
650 FOR G=1 TO 8
660 FOR H=1 TO 4
670 I=I+1
680 IF N(I)=1 THEN PRINT#1,"1 ";
690 IF N(I)=0 THEN PRINT#1,"0 ";
700 NEXT H
710 PRINT#1," "; :NEXT G
720 PRINT#1, :NEXT F
730 CLOSE#1 :GOTO 260
740 CLS :PRINT" Nom du fichier .CAR à charger ?"
750 INPUT S$ :S$=S$+".CAR"
760 OPEN S$ FOR INPUT AS #1
770 CLS :PRINT"---- CHARGEMENT EN COURS ----"
780 FOR F=1 TO 256
790 INPUT#1,Q : N(F)=Q
800 NEXT F
810 CLOSE#1 :GOTO 260
820 CLS :PRINT"CODE FAMILLE :                ";
830 F$="":A=9
840 GOSUB 1490:F$=F$+K$
850 A=13:GOSUB 1490:F$=F$+K$
860 IF LEFT$(F$,1)<>"0" THEN PRINT :PRINT :GOTO 380
870 PRINT"  (TêLêCARTE)"
880 PRINT"NUMERO DE SERIE :              ";
890 FOR A=17 TO 29 STEP 4
900 GOSUB 1490:NEXT A
```

© DUNOD - La photocopie non autorisée est un délit.

```
910 FOR A=41 TO 53 STEP 4
920 GOSUB 1490:NEXT A
930 PRINT :PRINT"POUVOIR FINANCIER :            ";
940 P$=""
950 A=89:GOSUB 1490:P$=P$+K$
960 A=93:GOSUB 1490:P$=P$+K$
970 P=VAL(P$) :P=(10*P)-10
980 PRINT"  (";P ;" unités)"
990 PRINT"CONSOMMATION :                ";
1000 C=0
1010 FOR F=97 TO 248
1020 IF N(F)=1 THEN C=C+1
1030 NEXT F :C=C-10
1040 PRINT C ;" UTC"
1050 IF C<P THEN PRINT"IL RESTE:                ";P-C ;" UTC" :BEEP
1060 IF C>P THEN PRINT"CARTE ANORMALE" :BEEP
1070 IF C=P THEN PRINT"CREDIT EPUISE"
1080 PRINT :PRINT :GOTO 380
1090 CLS :PRINT"INSERER CARTE A PROGRAMMER, puis presser ENTER"
1100 OUT S,0:INPUT Z$
1110 CLS :PRINT"APPLIQUER LE Vpp, puis presser ENTER"
1120 INPUT Z$
1130 CLS :PRINT"---- PROGRAMMATION EN COURS ----"
1140 FOR F=1 TO 256
1150 OUT S,249
1160 D=INP(E)
1170 B=N(F)
1180 IF B=0 THEN 1230
1190 OUT S,253
1200 FOR T=1 TO 150 :NEXT T
1210 OUT S,255
1220 FOR T=1 TO 150 :NEXT T
1230 OUT S,251:NEXT F
1240 CLS :PRINT"COUPER Vpp, et presser ENTER"
1250 INPUT Z$ :OUT S,0:GOTO 260
1260 CLS :PRINT"Insérer la carte à comparer, puis presser ENTER"
1270 INPUT Z$ :CLS
1280 PRINT"---- LECTURE CARTE EN COURS ----"
1290 OUT S,250:OUT S,248
1300 FOR F=1 TO 256
1310 OUT S,249
1320 D=INP(E) :D= (D AND 128)
1330 M(F)=1:IF D= 128 THEN M(F)=0
1340 OUT S,251
1350 NEXT F
1360 CLS :I=0
1370 FOR F=1 TO 8
1380 FOR G=1 TO 8
1390 FOR H=1 TO 4
1400 I=I+1
1410 IF N(I)=M(I) THEN PRINT"-";ELSE PRINT"*";
1420 NEXT H
1430 PRINT " "; :NEXT G
1440 PRINT
```





```
1450 IF F=3 THEN PRINT
1460 NEXT F :PRINT :PRINT
1470 GOTO 380
1480 END
1490 K=0
1500 FOR J=0 TO 3
1510 B=N(A+J)
1520 IF B=1 THEN K=K+2^(3-J)
1530 NEXT J
1540 IF K<10 THEN K$=CHR$(48+K)
1550 IF K>=10 THEN K$=CHR$(55+K)
1560 PRINT K$;
1570 RETURN
1580 END
1590 REM (c)1993,97 Patrick GUEULLE
```

Voici maintenant un programme beaucoup plus complet (GPM256.BAS), dont le menu de sélection permet de choisir entre les fonctions suivantes :

- retour au DOS (en fin de travail) ;
- lecture d'une carte (avec affichage sur l'écran de ses 256 bits) et mise en mémoire du résultat ;
- interprétation du contenu de la mémoire (ce qui vient d'être lu), permettant, entre autres choses, de prendre connaissance (si l'on est bien en présence d'une télé-carte T1G) du crédit restant et du numéro de série de la carte ;
- sauvegarde du contenu de la mémoire dans un fichier texte dont le nom sera muni automatiquement d'une extension « .CAR »;
- chargement en mémoire d'un fichier « .CAR », comme si on venait de lire la carte correspondante ;
- programmation d'une carte à partir du contenu de la mémoire (lu dans une carte ou dans un fichier « .CAR »);
- vérification d'une carte (contrôle de la conformité d'une carte avec le contenu de la mémoire) : les bits conformes sont représentés par des tirets et les bits erronés par des astérisques, le contenu de la mémoire restant évidemment inchangé pour permettre, si nécessaire, de réitérer plusieurs fois l'opération ;
- réaffichage du contenu de la mémoire sans nécessité de relire la carte ;
- appel du DOS (fonction SHELL), très utile pour appeler un éditeur de texte permettant de modifier un fichier « .CAR » avant de le recharger dans la même carte (transformation de 0 en 1 uniquement, et hors de la zone des 96 premiers bits si le fusible est bien coupé). Le retour au programme se fera en tapant EXIT.

© DUNOD - La photocopie non autorisée est un délit.

Ce logiciel est vraiment un outil puissant, permettant de procéder à toutes les opérations intéressantes à mener « en tout bien tout honneur » sur les télécartes et autres GPM 256.

Insistons en effet sur le fait que, sauf faute lourde d'un émetteur ou d'un fabricant qui en porterait bien entendu l'entière responsabilité, la conception de ce type de carte exclut, d'emblée, toute possibilité de falsification par ce seul moyen.

## UN LECTEUR-ENCODEUR DE 2e GÉNÉRATION

Avant de nous attaquer à des manipulations sur des cartes à puce monotension, il est intéressant de montrer à quel point il peut être simple de réaliser un lecteur-encodeur dès lors qu'il n'y a pas besoin d'un Vpp supérieur à 5 V.

Le schéma de la figure 4.6 se limite au strict minimum de composants, mais nécessite en revanche la fourniture d'une tension externe de +5 V.

Le plus simple est de prélever celle-ci sur la broche N° 1 de la prise « joystick », une DB 15 pour poignée de jeu dont sont munis quasiment tous les PC. À défaut, une alimentation de laboratoire quelconque fera l'affaire.

À ce détail près, la mise en œuvre de ce lecteur-encodeur est identique à celle du précédent, et il pourra même lire (mais pas écrire) dans les T1G et autres GPM 256.

En revanche, il faut garder présent à l'esprit que dans le cas des cartes monotension, on ne dispose pas du garde-fou commode qui consiste, avec les cartes à technologie bitension, à « oublier » d'appliquer Vpp. Une écriture accidentelle est donc toujours possible, par exemple en cas de manipulations logicielles hasardeuses ou de retrait prématuré d'une carte non désalimentée « proprement ».

La réalisation pratique suppose la gravure d'un petit circuit imprimé conforme au tracé de la figure 4.7 sur lequel tous les composants prendront place selon le plan de la figure 4.8, embase DB 25 (femelle) comprise.

Cette disposition évite le souci d'avoir à raccorder une prise « volante » par un câble multiconducteurs, mais suppose l'utilisation d'un cordon standard DB 25 mâle-mâle pour la connexion au port parallèle du PC.





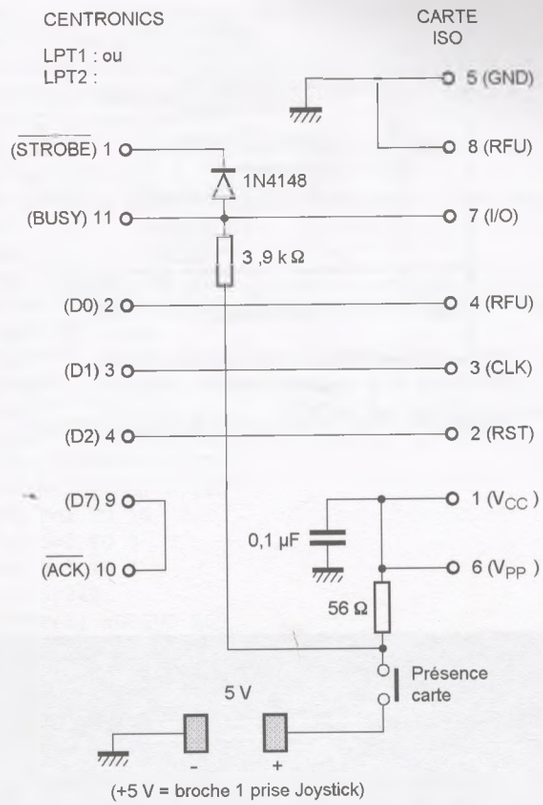



**Figure 4.6.** Schéma du lecteur-encodeur simplifié.

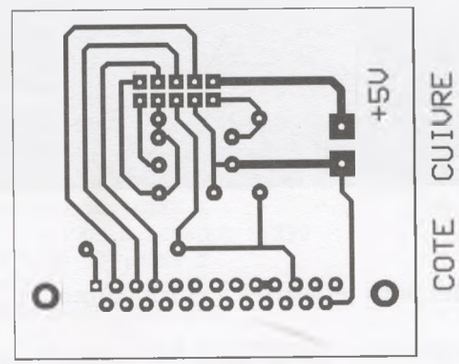



**Figure 4.7.** Tracé du circuit imprimé du lecteur-encodeur.

Attention, les deux fiches devant être reliées fil à fil, les câbles RS 232 spéciaux tels que les « null modems » ne conviennent pas.

On ne tentera pas, non plus, d'utiliser une embase DB 25 mâle pour enficher directement le montage dans le port parallèle, car les connexions se trouveraient inversées.

© DUNOD - La photocopie non autorisée est un délit.

*Liste des composants*

**Résistances (5 % 1/4 W) :**
R1 : 56 Ω,
R2 : 3,9 kΩ.

**Condensateurs :**
C1 : 0,1 µF.

**Semi-conducteurs :**
D1 : 1N 4148.

**Divers :**
Embase DB 25 femelle coudée pour circuit imprimé,
Barrette sécable à doubles picots carrés coudés,
Bornier à deux circuits.

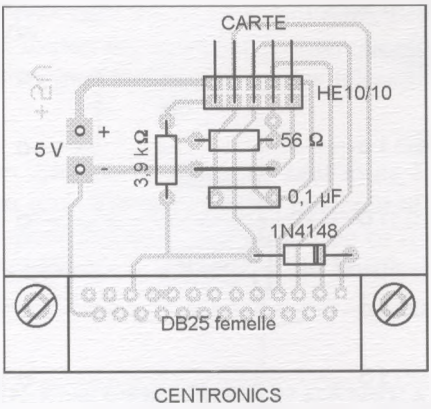
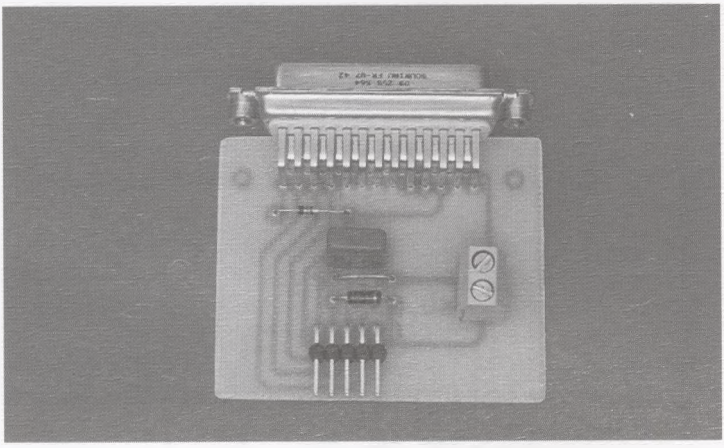



**Figure 4.8.** Plan de câblage du lecteur-encodeur.

Le lecteur-encodeur de 2e génération.



## Un logiciel pour télécartes « européennes »

Le programme MANIPEUR.BAS permet de lire et d'écrire dans la mémoire des cartes dérivées de la « TELEFONKARTE » allemande.

Il s'agit non seulement des cartes connues sous le nom d'EUROCHIP, mais aussi de toutes celles de la génération précédente, encore très largement utilisées dans les applications les plus diverses, y compris par les opérateurs de télécommunications de nombreux pays.

```
10 REM ---- MANIPEUR.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 OUT S,0:KEY OFF :CLS
120 PRINT"Insérer une carte européenne puis presser ENTER"
130 INPUT Z$ :CLS
140 PRINT"   barre d'espace : avance lecture"
150 PRINT"   touche +      : mise à 0 de bit"
160 PRINT"   touche -      : mise à 0 de bit avec retenue"
170 PRINT"   touche ESCape : quitter" :PRINT
180 OUT S,252:OUT S,254
190 OUT S,252:OUT S,248
200 FOR F=1 TO 16
210 FOR G=1 TO 8
220 FOR H=1 TO 4
230 OUT S,248
240 D=INP(E) :GOSUB 360
250 Z$=INKEY$ :IF Z$="" THEN 250
260 IF Z$=CHR$(27) THEN OUT S,0:END
270 IF Z$=CHR$(45) THEN 400
280 IF Z$=CHR$(43) THEN 420
290 IF Z$=CHR$(32) THEN 310
300 GOTO 250
310 OUT S,250
320 NEXT H
330 PRINT" "; :NEXT G
340 PRINT :NEXT F
350 END
360 K= (D AND 128)
370 IF K<>128 THEN PRINT"1";
380 IF K=128  THEN PRINT"0";
390 RETURN
400 OUT S,252:OUT S,248:OUT S,250
410 FOR T=1 TO 50 :NEXT T
420 OUT S,252:OUT S,248:OUT S,250
430 FOR T=1 TO 50 :NEXT T
440 OUT S,248
450 IF INKEY$<>"" THEN 450
460 GOTO 250
470 REM (c)1995 Patrick GUEULLE
```

Ce logiciel s'utilise exactement comme MANIPT1G.BAS mais donne accès, en plus, à la fonction d'écriture avec retenue disponible sur ces cartes.

Cette fois, il est prévu de lire un maximum de 512 bits, chiffre nécessaire à une exploration complète des cartes

© DUNOD - La photocopie non autorisée est un délit.

les plus récentes, mais le compteur d'adresses peut fort bien « faire le tour » beaucoup plus tôt (dès le 128e bit pour les cartes les plus simples).

La figure 4.9. montre ainsi comment la lecture d'une carte européenne à circuit intégré de 3e génération (104 bits) se traduit par l'affichage de quatre répliques d'un même bloc de 128 bits dont les 24 derniers sont invariablement à 1.

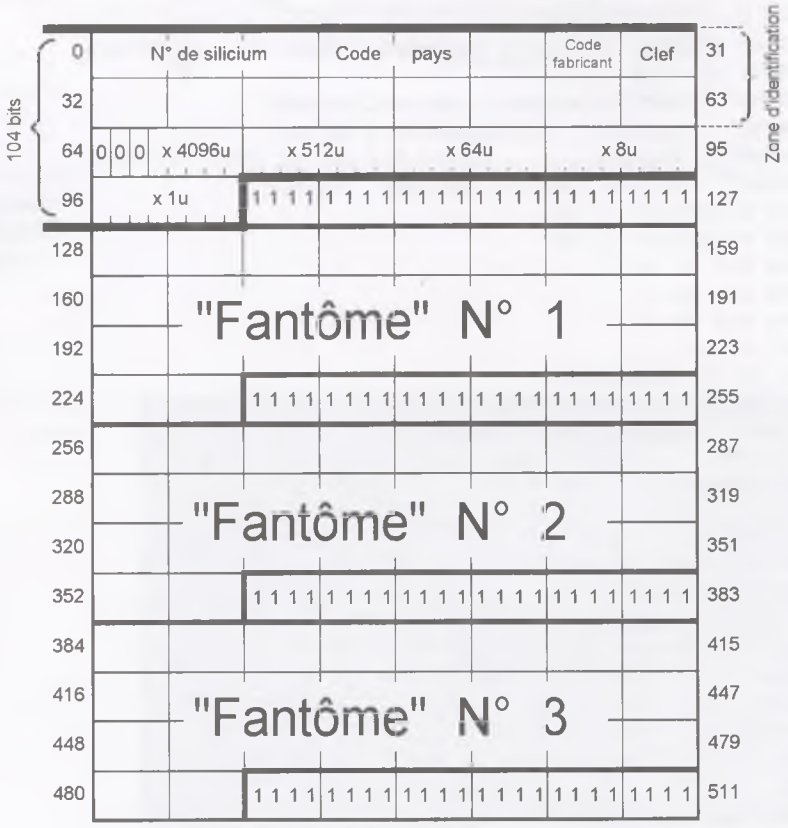



**Figure 4.9.** Plan mémoire des premières cartes européennes.

Ses 64 premiers bits correspondent à une zone accessible uniquement en lecture. Dite « zone d'identification », elle est programmée en usine avec des informations telles que « numéro de silicium » (code du circuit intégré interne), « code pays » propre à l'opérateur de télécommunications qui émet les cartes, et « code fabricant » identifiant l'encarteur qui a fabriqué la carte.

Le reste de cette zone fait office de numéro de série, dont il est parfois possible d'extraire la date de fabrication de la carte.

Viennent ensuite les compteurs d'unités, celui de poids fort (par 4096) en premier.

Les trois premiers bits du compteur de poids fort sont toujours à 0 sur les cartes de cette génération.

Le premier remplace le fusible des GPM 256 et sert à faire basculer la carte du mode « personnalisation » (ou « mode émetteur ») au mode « utilisation » (ou « mode porteur »).

Les deux autres sont également écrits en usine, mais cette fois-ci à des fins de test, un peu comme les dix premiers bits de la zone des unités des T1G.

La lecture de cartes européennes plus récentes donne un résultât proche de ce que représente la figure 4.10.

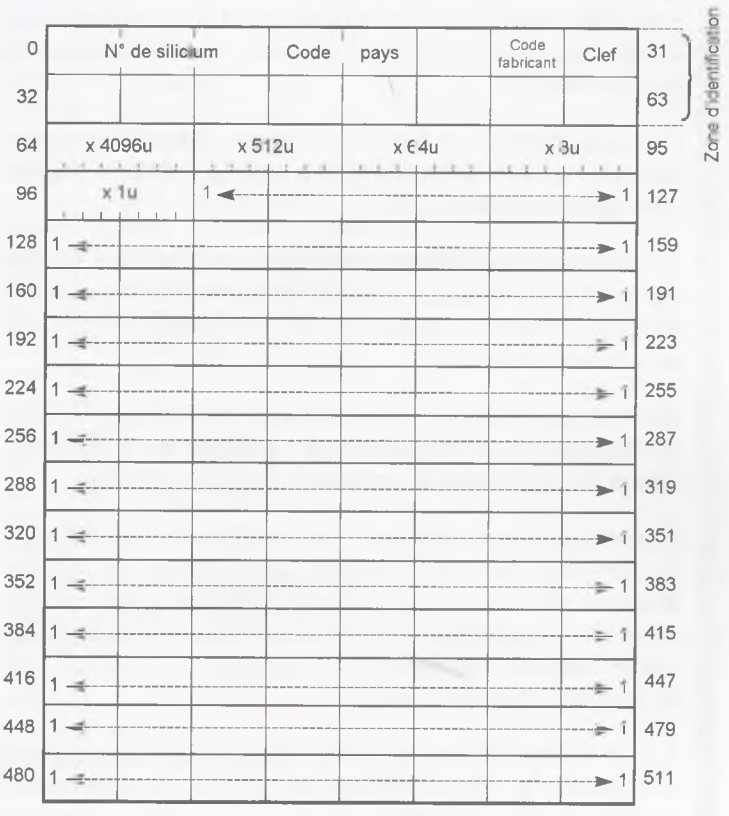



**Figure 4.10.** Plan mémoire simplifié des cartes EUROCHIP.

L'espace adressable s'étend jusqu'à 512 bits, mais dans l'état actuel des choses la plupart de ceux situés au-dessus de l'adresse 103 demeurent à 1.

© DUNOD - La photocopie non autorisée est un délit.

Il y a là des zones dont l'affectation peut varier d'une application à l'autre, et qu'on verra certainement un jour ou l'autre servir à enregistrer, par exemple, un petit répertoire de numéros de téléphone pouvant être appelés par une procédure simplifiée, voire automatiquement.

On parle aussi d'installer ici un « porte-monnaie électronique » rudimentaire.

Enfin, c'est dans ces parages que se situerait l'accès au dispositif cryptographique assurant la sécurité de la carte, et au sujet duquel il ne filtre que bien peu d'informations...

Certaines cartes à 112 bits et plus contiennent un compteur supplémentaire placé à la suite de celui « par un ». Il est parfois utilisé par des applications non téléphoniques comme, par exemple, les distributeurs automatiques de journaux.

Si tous les compteurs ne sont pas encore à 00h, il est possible d'intervenir sur leur contenu pour y consommer des unités mais, en aucun cas, il est facile de le vérifier, pour les « recharger ».

Pour transformer un 1 en 0 (autrement dit pour consommer une unité), il faut appuyer sur la touche + (signe plus) du pavé numérique.

L'affichage n'en sera pas affecté, puisque ce bit avait déjà été lu et qu'il n'est pas possible de faire reculer le compteur d'adresses sans repasser par zéro (par un RESET, ou en « faisant le tour »).

Si on presse la touche – (signe moins) du pavé numérique, on met également le bit courant à 0, mais on remet en même temps à 1 les huit bits du compteur de poids inférieur.

Ce mécanisme de « retenue », auquel on doit une capacité de comptage pouvant atteindre des dizaines de milliers d'unités, ne fonctionne évidemment que si le bit courant se trouve bien dans un compteur autre que celui de poids faible. Dans tous les autres cas, l'action de la touche – est identique à celle de la touche +.

À tout moment, il est possible de quitter le programme en pressant la touche ESCape, auquel cas aucune opération d'écriture n'intervient.

Il suffira alors de relancer le logiciel (RUN) pour reprendre la lecture au début de la mémoire, et voir ainsi l'effet des manœuvres précédentes.

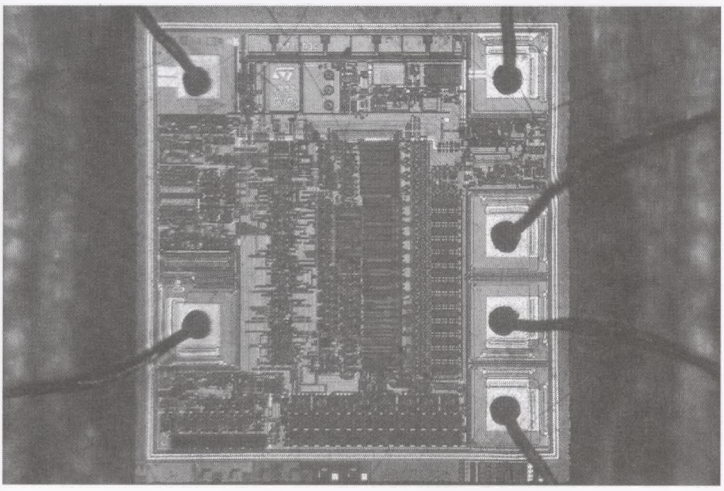
## Un logiciel pour T2G et cartes apparentées

```
10 REM ---- MANIPT2G.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 OUT S,0:KEY OFF :CLS
120 PRINT"Insérer une T2G puis presser ENTER" :PRINT
130 INPUT Z$ :CLS
140 PRINT"   barre d'espace : avance lecture"
150 PRINT"   touche +       : mise à 1 de bit"
160 PRINT"   touche -       : mise à 1 de bit avec retenue"
170 PRINT"   touche ESCape : quitter"
180 PRINT
190 OUT S,250
200 OUT S,248
210 FOR F=1 TO 14
220 FOR G=1 TO 8
230 FOR H=1 TO 4
240 OUT S,249
250 D=INP(E) :GOSUB 370
260 Z$=INKEY$ :IF Z$="" THEN 260
270 IF Z$=CHR$(27) THEN OUT S,0:END
280 IF Z$=CHR$(45) THEN 410
290 IF Z$=CHR$(43) THEN 430
300 IF Z$=CHR$(32) THEN 320
310 GOTO 260
320 OUT S,251
330 NEXT H
340 PRINT" "; :NEXT G
350 PRINT :NEXT F
360 END
370 K= (D AND 128)
380 IF K<>128 THEN PRINT"1";
390 IF K=128  THEN PRINT"0";
400 RETURN
410 OUT S,253
420 OUT S,255
430 OUT S,253
440 FOR T=1 TO 50 :NEXT T
450 OUT S,255
460 OUT S,253
470 OUT S,249
480 IF INKEY$<>"" THEN 480
490 GOTO 260
500 REM (c)1995 Patrick GUEULLE
```

© DUNOD - La photocopie non autorisée est un délit.

Le programme MANIPT2G.BAS est spécifiquement destiné aux « télécartes de 2e génération » françaises (T2G), et aux cartes équipées des circuits intégrés SGS-THOMSON utilisant la même technologie (ST1331, ST1333, etc.) La similitude avec l'EUROCHIP est frappante, puisqu'un mécanisme de « retenue » est également disponible. La principale différence est que, la T2G étant « vierge à 0 » comme la T1G, la touche + servira cette fois à transformer des 0 en 1.

La touche –, pour sa part, permettra de remettre à 0 tous les bits d'un compteur en contrepartie de l'écriture d'un 1 dans le compteur de poids immédiatement supérieur.



La puce d'une T2G de 1993 (ST 1303) (grossie 50 fois).

Il est bien évident que de puissants mécanismes sécuritaires sont prévus pour empêcher que cette manœuvre ne permette de recharger des cartes épuisées !

À l'heure où nous écrivons ces lignes, la T2G est acceptée par tous les publiphones à cartes de France mais n'est encore commercialisée que par séries expérimentales.

Ses caractéristiques n'étant pas définitivement figées, il serait hasardeux de publier des informations précises sur la signification des bits qu'on peut y lire hors de la zone de comptage.

Certaines cartes privatives présentent, pour leur part, une structure très proche de la T2G (figures 2.10 et 2.11), à commencer par les cartes de fidélité « CARTAPLUS » offertes par les stations-service FINA.

Une zone de ces cartes (celle qui comptabilise les points !) présente la particularité d'être librement accessible en lecture et en écriture. C'est la manœuvre d'écriture avec retenue (touche –) qui sert alors à remettre à 0 les 1 inscrits par la manœuvre d'écriture simple (touche +).

Bien entendu, le contenu de cette zone est crypté, ce qui empêche, en principe, toute tentative de modification illicite.

### Lecture des GPM 416

```
10 REM ----- GPM416.BAS -----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1:OUT S,0
110 DIM B$(416)
120 PRINT"Insérer GPM416, puis presser ENTER"
130 INPUT Z$
140 CLS
150 OUT S,4:OUT S,0
160 FOR I=1 TO 416
170 OUT S,0
180 D=INP(E) :D= (D AND 128)
190 IF D=128 THEN B$(I)="0"
200 IF D<>128 THEN B$(I)="1"
210 OUT S,2
220 NEXT I
230 N=1
240 FOR F=1 TO 13
250 FOR G=1 TO 8
260 FOR H=1 TO 4
270 PRINT B$(N) ;:N=N+1
280 NEXT H
290 PRINT " "; :NEXT G
300 PRINT :NEXT F
310 PRINT :PRINT :PRINT"Pour sauvegarder, taper un nom de fichier puis ENTER"
320 PRINT :PRINT"Pas de sauvegarde : changer carte et presser ENTER"
330 PRINT :PRINT :INPUT Z$
340 IF Z$="" THEN 140
350 FOR F=1 TO LEN(Z$)
360 IF MID$(Z$,F,1)="." THEN  390
370 NEXT F
380 Z$=Z$+".CAR"
390 OPEN Z$ FOR OUTPUT AS #1
400 N=1
```

© DUNOD - La photocopie non autorisée est un délit.

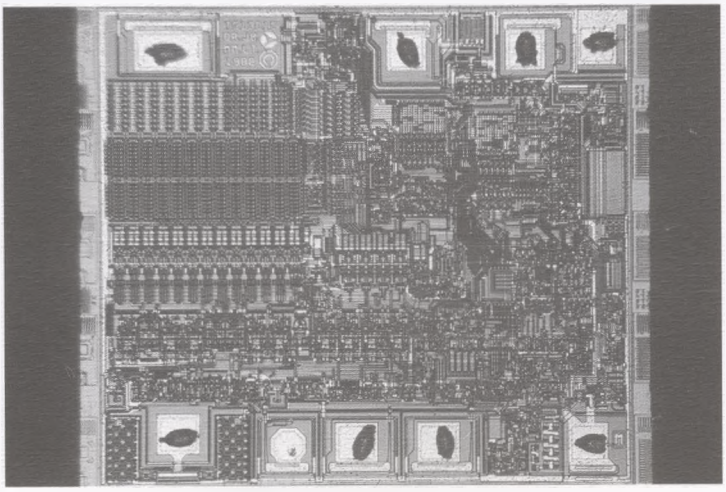
```
410 FOR F=1 TO 13
420 FOR G=1 TO 8
430 FOR H=1 TO 4
440 PRINT#1, B$(N)+" ";:N=N+1
450 NEXT H
460 PRINT#1," "; :NEXT G
470 PRINT#1, :NEXT F
480 CLOSE#1 :PRINT ::GOTO 120
490 REM (c)1993,1995 Patrick GUEULLE
```

Le logiciel GPM416.BAS permet d'afficher 416 bits sur l'écran : ceux-ci correspondent à la capacité totale d'une carte GPM 416. Ce logiciel permet éventuellement de créer le fichier « .CAR » correspondant. S'agissant d'une carte à mémoire sécurisée, certains de ces bits ne sont cependant lisibles que sous le contrôle d'un code secret, généralement inconnu du porteur. Bien souvent, il est présenté de façon automatique par le lecteur-encodeur.

Tant que le bon code n'a pas été présenté, les bits ainsi protégés s'affichent comme des « 1 » quel que soit leur état réel (on dit qu'ils sont « masqués »).

La figure 4.11 résume les règles régissant l'accès aux diverses zones de la mémoire de la carte, en fonction des différents paramètres de sécurité.

La figure 4.12 reproduit le résultat de la lecture d'une télécarte des TAAF (Terres Australes et Antarctiques Françaises) qui, développée par Landis et Gyr à partir de la GPM 416, présente la particularité d'être rechargeable auprès de son émetteur.



La puce ST 1301 d'une GPM 416 (grossie 50 fois).

mode APPLICATIF (fusible claqué)

| | LECTURE | EFFACEMENT | ECRITURE |
|---|---|---|---|
| Zone de Fabrication | oui | non | non |
| Zone émetteur | oui | non | non |
| Code Secret Carte | non | oui si CSC = 1 | oui si CSC = 1 |
| Compteur d'erreurs | oui | oui si CSC = 1 | oui |
| Zone protégée par le Code Secret Carte | oui | oui si CSC = 1 | oui si CSC = 1 |
| Zone Applicative | oui si RDEN = 1 ou CSC = 1 | oui si CSC = 1 et CSE = 1 et EC = 1 | oui si PREN = 1 et CSC = 1 |
| Code Secret Effacement Zone applicative | non | non | non |
| Compteur d'Effacement Zone Applicative | oui | non | oui |

mode PERSONNALISATION (fusible intact)

| | LECTURE | EFFACEMENT | ECRITURE |
|---|---|---|---|
| Zone de Fabrication | oui | non | non |
| Zone émetteur | oui | oui si CSC = 1 | oui si CSC = 1 |
| Code Secret Carte | non si CSC = 1 | oui si CSC = 1 | oui si CSC = 1 |
| Compteur d'erreurs | oui | oui si CSC = 1 | oui |
| Zone protégée par le Code Secret Carte | oui | oui si CSC = 1 | oui si CSC = 1 |
| Zone Applicative | oui si RDEN = 1 ou CSC = 1 | oui si CSC = 1 | oui si CSC = 1 |
| Code Secret Effacement Zone applicative | oui si CSC = 1 | oui si CSC = 1 | oui si CSC = 1 |
| Compteur d'Effacement Zone Applicative | oui | oui si CSC = 1 | oui |

CSC CSC = 1 après une bonne présentation du Code Secret Carte durant la session.

PREN Registre interne positionné par le 1er bit de la Zone Applicative ; verrouille la zone en écriture.

RDEN Registre interne positionné par le 2ème bit de la Zone Applicative ; interdit l'accès en lecture de la Zone Applicative sans présentation préalable du Code Secret Carte.

CSE CSE = 1 après une bonne présentation du Code Secret d'Effacement.

CE CE = 1 tant que le Compteur d'Effacement n'est pas plein (< 64).

**Figure 4.11.** Règles d'accès à la GPM 416.

© DUNOD - La photocopie non autorisée est un délit.

```
0 0 0 1  1 0 0 1  1 1 1 1  1 1 1 1  0 0 0 0  0 0 0 0  0 0 0 0  1 1 1 0
0 0 0 0  1 0 0 0  0 0 0 0  1 1 0 0  0 0 0 0  0 0 0 0  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  0 1 1 1  1 1 1 1  1 1 1 1  1 1 0 0
0 0 0 0  0 0 0 0  0 0 0 1  1 0 0 1  1 1 0 0  0 0 0 0  0 0 0 0  0 0 0 1
1 0 0 1  0 0 1 1  0 1 1 1  0 0 1 0  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
0 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1  1 1 1 1
```

**Figure 4.12.** Contenu d'une télécarte à GPM 416.

```
10 REM ---- DEC416.BAS ----
20 KEY OFF :CLS
30 PRINT"NOM DU FICHIER .CAR à ANALYSER  ";
40 INPUT N$
50 IF N$="" THEN END
60 FOR F=1 TO LEN(N$)
70 IF MID$(N$,F,1)="." THEN 100
80 NEXT F
90 N$=N$+".CAR"
100 OPEN N$ FOR INPUT AS #1
110 DIM M(416)
120 FOR F=0 TO 415
130 INPUT#1,Q :M(F)=Q
140 NEXT F
150 CLS
160 PRINT"ZONE FABRICANT : ";
170 B=0:E=15:GOSUB 520
180 PRINT B$
190 PRINT"ZONE EMETTEUR : ";
200 B=16:E=63:GOSUB 520
210 PRINT B$
220 PRINT"MASQUE DU CODE CONFIDENTIEL : ";
230 B=64:E=79:GOSUB 520
240 PRINT"COMPTEUR D'ERREURS : ";
250 B=80:E=95:GOSUB 520
260 PRINT B$
270 IF LEFT$(H$,1)="F" THEN PRINT"le dernier code présenté était bon"
280 IF LEFT$(H$,1)="7" THEN PRINT"le dernier code présenté était faux"
290  IF  LEFT$(H$,1)="3"  THEN  PRINT"les  2  derniers  codes  présentés
étaient faux"
300  IF  LEFT$(H$,1)="1"  THEN  PRINT"les  3  derniers  codes  présentés
étaient faux"
310  IF  LEFT$(H$,1)="0"  THEN  PRINT"4  codes  faux  ont  été  présentés  :
carte bloquée"
320 PRINT :PRINT"ZONE PROTEGEE : ";
330 B=96:E=111:GOSUB 520
340 PRINT B$
```

```
350 PRINT"ZONE APPLICATIVE : ";
360 B=112:E=319:GOSUB 520
370 PRINT C$;
380 PRINT B$
390 PRINT "PREN =";M(176); " , ";
400 PRINT "RDEN =";M(177)
410 PRINT :PRINT"MASQUE CODE EFFACEMENT : ";
420 B=320:E=351:GOSUB 520
430 PRINT"COMPTEUR D'EFFACEMENT : ";
440 B=352:E=415:GOSUB 520
450 PRINT B$
460 R=0
470 FOR F=352 TO 415
480 IF M(F)=0 THEN R=R+1
490 NEXT F
500  PRINT  "nb  d'effacements  déjà  effectués  :"R ;",  encore  pos-
sibles :";64-R
510 END
520 H=0:B$="":C$="":H$="":K=0:FOR F=B TO E
530 IF M(F)=1 THEN B$=B$+"1" ELSE B$=B$+"0"
540 IF LEN(B$)=255 THEN C$=C$+LEFT$(B$,1):B$=RIGHT$ (B$,254)
550 IF M(F)=1 THEN H=H+2^(3-K)
560 K=K+1
570 IF K<=3 THEN 600
580 H$=H$+HEX$(H)
590 K=0:H=0
600 NEXT F
610 PRINT H$
620 RETURN
630 REM (c)1995 Patrick GUEULLE
```

Il est possible de décrypter sommairement ces 416 bits en utilisant le programme DEC416.BAS sur le fichier « .CAR » préalablement sauvegardé.

La figure 4.13 montre le résultat ; son examen attentif permet de soupçonner que cette carte pourrait bien avoir fait l'objet d'une tentative de présentation d'un code secret qui n'était pas le bon, et que sa zone applicative aurait déjà été effacée une fois (sans doute à l'occasion d'un rechargement).

## Lecture des GPM 896

La carte GPM 896 est apparentée à la GPM 416, mais offre une capacité mémoire supérieure (896 bits) et deux zones applicatives indépendantes comme le montre la figure 4.14.

© DUNOD - La photocopie non autorisée est un délit.

```
ZONE FABRICANT : 19FF
0001100111111111
ZONE EMETTEUR : 000E080C00FF
000000000000111000001000000011000000000011111111
MASQUE DU CODE CONFIDENTIEL : FFFF
COMPTEUR D'ERREURS : 7FFC
0111111111111100
le dernier code présenté était faux
ZONE PROTEGEE : 0019
0000000000011001
ZONE APPLICATIVE: C0019372FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
11000000000000011001001101110010111111111111111111111111111111111111
1111111111
11111111111111111111111111111111111111111111111111111111111111111111
1111111111
11111111111111111111111111111111111111111111
PREN = 1  , RDEN = 1
MASQUE CODE EFFACEMENT : FFFFFFFF
COMPTEUR D'EFFACEMENT : 7FFFFFFFFFFFFFFF
01111111111111111111111111111111111111111111111111111111111111111111
nb d'effacements déjà effectués : 1 , encore possibles : 63
```

**Figure 4.13.** Décryptage sommaire du contenu d'une GPM 416.

| | | |
|---|---|---|
| MANUFACTURING AREA | | (16 BITS) |
| ISSUER AREA | | (64 BITS) |
| CARD SECRET CODE | | (16 BITS) |
| ERROR COUNTER (4 BITS) | | (12 BITS) |
| AREA PROTECTED BY THE CARD SECRET CODE | | (64 BITS) |
| PREN # 1 | RDEN # 1 | |
| APPLICATION DATA AREA # 1 | | 256 BITS |
| ERASE SECRET CODE # 1 | | (48 BITS) |
| PREN # 2 | RDEN # 2 | |
| APPLICATION DATA AREA # 2 | | (256 BITS) |
| ERASE SECRET CODE # 2 | | (32 BITS) |
| ERASE COUNTER FOR AREA # 2 | | (128 BITS) |

TOTAL = 896 BITS

**Figure 4.14.** Plan mémoire de la GPM 896.

C'est sur la GPM 896 qu'est basée la carte de fidélité offerte par le pétrolier SHELL dans ses stations-service.

La figure 4.15 fournit un exemple de ce que peut réellement contenir une telle carte, lue avec GPM896.BAS.

```
00110010 11111111 01100111 01100000 10010001 00010000 00011100 00010010
11100101 10111011 11111111 11111111 11111111 11111111 00000000 01000010
00110000 00000000 00000000 01000010 00110000 00000000 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111
```

**Figure 4.15.** Contenu d'une carte de fidélité à GPM 896.

```
10 REM ----- GPM896.BAS -----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1:OUT S,0
110 DIM B$(896)
120 PRINT"Insérer GPM896, puis presser ENTER"
130 INPUT Z$
140 CLS
150 OUT S,4:OUT S,0
160 FOR I=1 TO 896
170 OUT S,0
180 D=INP(E) :D= (D AND 128)
190 IF D=128 THEN B$(I)="0"
200 IF D<>128 THEN B$(I)="1"
210 OUT S,2
220 NEXT I
230 N=1
240 FOR F=1 TO 14
250 FOR G=1 TO 8
260 FOR H=1 TO 8
270 PRINT B$(N) ;:N=N+1
280 NEXT H
290 PRINT " "; :NEXT G
300 PRINT :NEXT F
310 PRINT :PRINT :PRINT"Pour sauvegarder, taper un nom de fichier puis ENTER"
320 PRINT :PRINT"Pas de sauvegarde : changer carte et presser ENTER"
330 PRINT :PRINT :INPUT Z$
340 IF Z$="" THEN 140
350 FOR F=1 TO LEN(Z$)
```

© DUNOD - La photocopie non autorisée est un délit.

```
360 IF MID$(Z$,F,1)="." THEN  390
370 NEXT F
380 Z$=Z$+".CAR"
390 OPEN Z$ FOR OUTPUT AS #1
400 N=1
410 FOR F=1 TO 28
420 FOR G=1 TO 8
430 FOR H=1 TO 4
440 PRINT#1, B$(N)+" ";:N=N+1
450 NEXT H
460 PRINT#1," "; :NEXT G
470 PRINT#1, :NEXT F
480 CLOSE#1 :PRINT ::GOTO 120
490 REM (c)1993,1995 Patrick GUEULLE
```

Là encore, un logiciel de décryptage (DEC896.BAS) va constituer une aide précieuse.

```
10 REM ---- DEC896.BAS ----
20 KEY OFF :CLS
30 PRINT"NOM DU FICHIER .CAR à ANALYSER  ";
40 INPUT N$
50 IF N$="" THEN END
60 FOR F=1 TO LEN(N$)
70 IF MID$(N$,F,1)="." THEN 100
80 NEXT F
90 N$=N$+".CAR"
100 OPEN N$ FOR INPUT AS #1
110 DIM M(896)
120 FOR F=0 TO 895
130 INPUT#1,Q :M(F)=Q
140 NEXT F
150 CLS
160 PRINT"ZONE FABRICANT : ";
170 B=0:E=15:GOSUB 5000
190 PRINT B$
200 PRINT"ZONE EMETTEUR : ";
210 B=16:E=79:GOSUB 5000
220 PRINT B$
230 PRINT"MASQUE DU CODE CONFIDENTIEL : ";
240 B=80:E=95:GOSUB 5000
260 PRINT"COMPTEUR D'ERREURS : ";
270 B=96:E=111:GOSUB 5000
275 PRINT B$
280 IF LEFT$(H$,1)="F" THEN PRINT"le dernier code présenté était bon"
290 IF LEFT$(H$,1)="7" THEN PRINT"le dernier code présenté était faux"
300  IF  LEFT$(H$,1)="3"  THEN  PRINT"les  2  derniers  codes  présentés
étaient faux"
310  IF  LEFT$(H$,1)="1"  THEN  PRINT"les  3  derniers  codes  présentés
étaient faux"
320  IF  LEFT$(H$,1)="0"  THEN  PRINT"4  codes  faux  ont  été  présentés  :
carte bloquée"
400 PRINT :PRINT"ZONE PROTEGEE : ";
410 B=112:E=175:GOSUB 5000
```

```
420 PRINT B$
500 PRINT"ZONE APPLICATIVE N°1 : ";
510 B=176:E=431:GOSUB 5000
520 PRINT C$;
525 PRINT B$
530 PRINT "PREN#1 =";M(176); " , ";
540 PRINT "RDEN#1 =";M(177)
550 PRINT"MASQUE CODE EFFACEMENT ZONE 1 : ";
560 B=434:E=479:GOSUB 5000
570 PRINT :PRINT"------------- page suivante : presser ENTER ---------
--------"
580 PRINT :INPUT Z$ :CLS
600 PRINT"ZONE APPLICATIVE N°2 : ";
610 B=482:E=735:GOSUB 5000
620 PRINT C$;
625 PRINT B$
630 PRINT :PRINT "PREN#2 =";M(482); " , ";
640 PRINT "RDEN#2 =";M(483)
700 PRINT :PRINT"MASQUE CODE EFFACEMENT ZONE 2 : ";
710 B=740:E=767:GOSUB 5000
800 PRINT :PRINT"COMPTEUR D'EFFACEMENT ZONE 2 : ";
810 B=772:E=895:GOSUB 5000
820 PRINT B$
830 R=0
840 FOR F=772 TO 895
850 IF M(F)=0 THEN R=R+1
860 NEXT F
870 PRINT :PRINT R ;" effacements zone 2 effectués,";128-R"sont encore
possibles"
4999 END
5000 H=0:B$="":C$="":H$="":K=0:FOR F=B TO E
5010 IF M(F)=1 THEN B$=B$+"1" ELSE B$=B$+"0"
5015 IF LEN(B$)=255 THEN C$=C$+LEFT$(B$,1):B$=RIGHT$(B$,254)
5020 IF M(F)=1 THEN H=H+2^(3-K)
5030 K=K+1
5040 IF K<=3 THEN 5100
5050 H$=H$+HEX$(H)
5060 K=0:H=0
5100 NEXT F
5110 PRINT H$
5220 RETURN
6000 REM (c)1995 Patrick GUEULLE
```

Le résultat de ce traitement, qui apparaît sur deux écrans successifs, est reproduit sur la figure 4.16.

## LES CARTES À PUCE I2C

Même si bien d'autres fabricants produisent des cartes à puce I2C ou apparentées, on ne saurait oublier que c'est PHILIPS qui est à l'origine du concept de « bus I2C ».

© DUNOD - La photocopie non autorisée est un délit.

```
ZONE FABRICANT : 32FF
0011001011111111
ZONE EMETTEUR : 676091101C12E5BB
0110011101100000100100010001000000001110000010010111001011011101 1
MASQUE DU CODE CONFIDENTIEL : FFFF
COMPTEUR D'ERREURS : FFFF
1111111111111111
le dernier code présenté était bon
ZONE PROTEGEE : 0042300000423000
0000000001000010001100000000000000000000010000100011000000000000
ZONE APPLICATIVE N°1 :
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
11
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
11111111111111
PREN#1 = 1  , RDEN#1 = 1
MASQUE CODE EFFACEMENT ZONE 1 : FFFFFFFFFF
------------- page suivante : presser ENTER -----------------
ZONE APPLICATIVE N°2 :
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
11111111111111
PREN#2 = 1  , RDEN#2 = 1
MASQUE CODE EFFACEMENT ZONE 2 : FFFFFFF
COMPTEUR D'EFFACEMENT ZONE 2 : FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
1111111111111111111111111111111111111111111111111111111111111111111111
1111111111
11111111111111111111111111111111111111111
0  effacements zone 2 effectués, 128 sont encore possibles
```

**Figure 4.16.** Décryptage sommaire du contenu d'une GPM 896.

Avec ses cartes D2000 (256 octets) et D4000 (512 octets), PHILIPS se conforme enfin au brochage normalisé ISO 7816 après avoir commercialisé pendant plusieurs années des mémoires PCF 8582 « encartées » d'une façon résolument anticonformiste.

On doit donc considérer le brochage de la figure 4.17 comme désormais totalement obsolète, et cela d'autant plus que la carte PCF 8582 MC nécessitait un réseau RC externe relié à son contact PTC selon le schéma de la figure 4.18 !

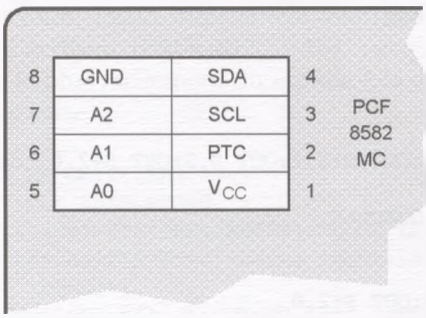



**Figure 4.17.** Brochage (obsolète) de la carte PCF 8582 MC.

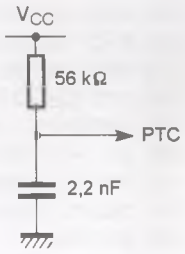



**Figure 4.18.** Réseau RC externe de la PCF 8582 MC.

Il résulte de cette évolution que les lecteurs-encodeurs de ce chapitre se retrouvent parfaitement capables de lire et écrire dans la mémoire de ces cartes disponibles au détail (SELECTRONIC), relativement peu coûteuses, et de grande capacité (2048 et 4096 bits respectivement).

C'est d'autant plus intéressant que ces cartes sont d'un accès totalement libre puisqu'elles ne sont munies d'aucune protection en lecture ni même en écriture.

Contrairement aux cartes synchrones ordinaires, les cartes à puce I2C ne sont pas accessibles bit par bit, mais octet par octet, de façon séquentielle ou aléatoire.

Par conséquent, le logiciel de lecture LECTI2C.BAS opère de façon assez différente de ceux évoqués jusqu'à présent.

```
10 REM ---- LECTI2C.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 OUT S,2:OUT S+2,0
120 CLS :PRINT"Insérer carte I2C à lire, puis presser ENTER"
130 INPUT Z$
140 OUT S,2:OUT S+2,0:OUT S,2:OUT S+2,1:OUT S,0:OUT S+2,1 'cond de DEBUT
150 M=&HA0 :GOSUB 460 :GOSUB 400
160 OPEN "I2C.ROM" FOR OUTPUT AS #1
170 CLS :PRINT"Nombre d'octets à lire ?"
180 INPUT C :CLS
190 M=0:GOSUB 460 :GOSUB 400
200 FOR T=0 TO 300 :NEXT T
210 OUT S,2:OUT S+2,0:OUT S,2:OUT S+2,1:OUT S,0:OUT S+2,1
```

© DUNOD - La photocopie non autorisée est un délit.

```
220 M=&HA1 :GOSUB 460 :GOSUB 400
230 FOR G=1 TO C-1
240 GOSUB 300 :GOSUB 380
250 NEXT G
260 GOSUB 300 :GOSUB 390
270 OUT S,0:OUT S+2,1:OUT S,2:OUT S+2,1:OUT S,2:OUT S+2,0 'cond de FIN
280 END
290 REM (c)1992,1997 Patrick GUEULLE
300 K=0 'réception octet
310 FOR F=0 TO 7
320 OUT S,0:OUT S+2,0:OUT S,2:OUT S+2,0
330 D=INP(E) :D= D AND 128
340 IF D=0 THEN K=K+2^(7-F)
350 OUT S,0:OUT S+2,0:NEXT F
360 PRINT USING "####";K ;:PRINT#1,K ;
370 RETURN
380 OUT S,0:OUT S+2,1:OUT S,2:OUT S+2,1:OUT S,0:OUT S+2,1:RETURN 'tx 0
390 OUT S,0:OUT S+2,0:OUT S,2:OUT S+2,0:OUT S,0:OUT S+2,0:RETURN 'tx 1
400 OUT S,0:OUT S+2,0:OUT S,2:OUT S+2,0 'attente ACK
410 N=0
420 D=INP(E) :D= D AND 128
430 N=N+1:IF N>500 THEN END
440 IF D=0 THEN 420
450 OUT S,0:OUT S+2,0:RETURN
460 D=0 : REM émission octet
470 IF M>127 THEN D=1:M=M-128
480 GOSUB 630
490 IF M>63 THEN D=1:M=M-64
500 GOSUB 630
510 IF M>31 THEN D=1:M=M-32
520 GOSUB 630
530 IF M>15 THEN D=1:M=M-16
540 GOSUB 630
550 IF M>7 THEN D=1:M=M-8
560 GOSUB 630
570 IF M>3 THEN D=1:M=M-4
580 GOSUB 630
590 IF M>1 THEN D=1:M=M-2
600 GOSUB 630
610 D=M :GOSUB 630
620 RETURN
630 IF D=1 THEN GOSUB 390
640 IF D=0 THEN GOSUB 380
650 D=0:RETURN
```

Lisant séquentiellement un nombre spécifié d'octets à partir du premier (en général la totalité du contenu de la carte), il affiche ceux-ci sous la forme d'une suite de valeurs décimales qu'il sauvegarde en même temps dans un fichier texte baptisé I2C.ROM.

Le format de ce fichier (*free format decimal*) est compatible avec de nombreux utilitaires de transcodage, par exemple en binaire ou en hexadécimal.

Il est de toute façon directement réutilisable par notre logiciel d'écriture (PROGRI2C.BAS), ce qui permet de procéder le plus facilement du monde à la duplication de ce type de carte.

```
10 REM ---- PROGRI2C.BAS ----
20 KEY OFF :CLS :DEF SEG=0
30 S1=PEEK(&H408)+256*PEEK(&H409) 'pour LPT1 :
40 S2=PEEK(&H40A)+256*PEEK(&H40B) 'pour LPT2 :
50 OUT S2,0 :E2=S2+1
60 IF (INP(E2) AND 64) <> 0 THEN S=S1 :GOTO 100
70 OUT S2,128
80 IF (INP(E2) AND 64) <> 64 THEN S=S1 :GOTO 100
90 S=S2
100 E=S+1
110 OUT S,2:OUT S+2,0:L=0
120 CLS :PRINT"Nom du fichier .ROM à utiliser ?"
130 INPUT F$ :F$=F$+".ROM"
140 OPEN F$ FOR INPUT AS #1
150 DIM W(4096)
160 CLS :PRINT"---- LECTURE FICHIER EN COURS ----
170 IF EOF(1) THEN 210
180 INPUT#1,W(L)
190 L=L+1
200 GOTO 170
210 CLOSE#1 :CLS
220 CLS :PRINT"Insérer carte I2C à programmer, et presser ENTER"
230 PRINT"ATTENTION ! Capacité mini de la carte : ";L ;" octets"
240 INPUT Z$ :CLS :PRINT"---- PROGRAMMATION EN COURS ----"
250 FOR G=0 TO L-1 :PRINT"*";
260  OUT S,2:OUT S+2,0:OUT S,2:OUT S+2,1:OUT S,0:OUT S+2,1 'cond de
DEBUT
270 M=&HA0 :GOSUB 430 :GOSUB 370
280 M=G :GOSUB 430 :GOSUB 370
290 M=W(G) :GOSUB 430 :GOSUB 370
300 OUT S,0:OUT S+2,1:OUT S,2:OUT S+2,1:OUT S,2:OUT S+2,0 'cond de FIN
310 FOR T=0 TO 2000:NEXT T
320 NEXT G
330 END
340 REM (c)1992,1997 Patrick GUEULLE
350 OUT S,0:OUT S+2,1:OUT S,2:OUT S+2,1:OUT S,0:OUT S+2,1:RETURN 'tx 0
360 OUT S,0:OUT S+2,0:OUT S,2:OUT S+2,0:OUT S,0:OUT S+2,0:RETURN 'tx 1
370 OUT S,0:OUT S+2,0:OUT S,2:OUT S+2,0 : REM attente ACK
380 N=0
390 D=INP(E) :D= D AND 128
400 N=N+1:IF N>500 THEN END
410 IF D=0 THEN 390
420 OUT S,0:OUT S+2,0:RETURN
430 D=0 : REM émission octet
440 IF M>127 THEN D=1:M=M-128
450 GOSUB 600
460 IF M>63 THEN D=1:M=M-64
470 GOSUB 600
480 IF M>31 THEN D=1:M=M-32
```

© DUNOD - La photocopie non autorisée est un délit.

```
490 GOSUB 600
500 IF M>15 THEN D=1:M=M-16
510 GOSUB 600
520 IF M>7 THEN D=1:M=M-8
530 GOSUB 600
540 IF M>3 THEN D=1:M=M-4
550 GOSUB 600
560 IF M>1 THEN D=1:M=M-2
570 GOSUB 600
580 D=M :GOSUB 600
590 RETURN
600 IF D=1 THEN GOSUB 360
610 IF D=0 THEN GOSUB 350
620 D=0:RETURN
```

Il est intéressant de remarquer que ces cartes sont « vierges à 1 » (remplies d'octets FFh ou 255d lorsqu'elles sont neuves), et qu'elles acceptent indifféremment la transformation de 1 en 0 ou de 0 en 1.

## Réalisation d'une « fausse carte » à puce I2C

Notre concept de « fausse carte » gravée sur un circuit imprimé de 8/10 mm peut facilement être étendu aux cartes à puce I2C, dans la mesure où des mémoires très semblables sont disponibles à peu de frais en boîtier DIP à 8 broches.

La 24C02 (256 octets) est ainsi comparable à la D2000, et la 24C04 (512 octets) à la D4000, moyennant un branchement selon les indications de la figure 4.19.

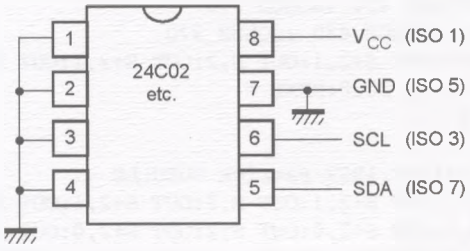



**Figure 4.19.** Comment transformer une 24C02 en carte à puce.

Il n'est d'ailleurs pas interdit d'expérimenter avec des mémoires de capacité inférieure (24C01) ou supérieure (24C08 et 24C16), voire avec les composants plus « spéciaux » que proposent certaines marques (X76041 de XICOR, par exemple).

Plutôt que de faire appel aux « fausses cartes » plus ou moins universelles de la figure 2.13, on pourra préférer graver la version spécialisée dont la figure 4.20 fournit le tracé.

La figure 4.21, quant à elle, précise l'orientation selon laquelle doit être montée la mémoire en boîtier DIP (de préférence sur un support « tulipe »), et rappelle à toutes fins utiles la numérotation des contacts ISO.

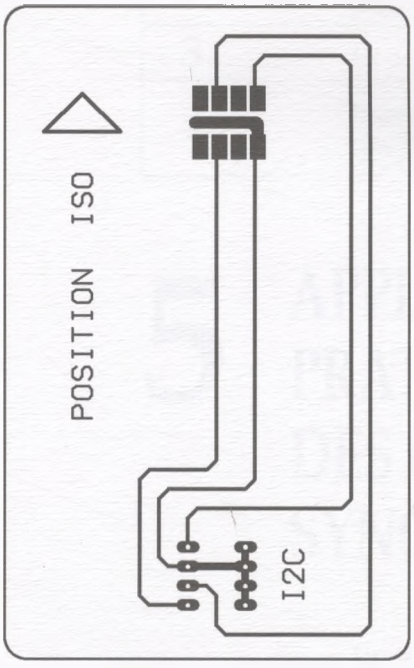



**Figure 4.20.** Tracé du circuit imprimé de la « fausse carte » I2C.

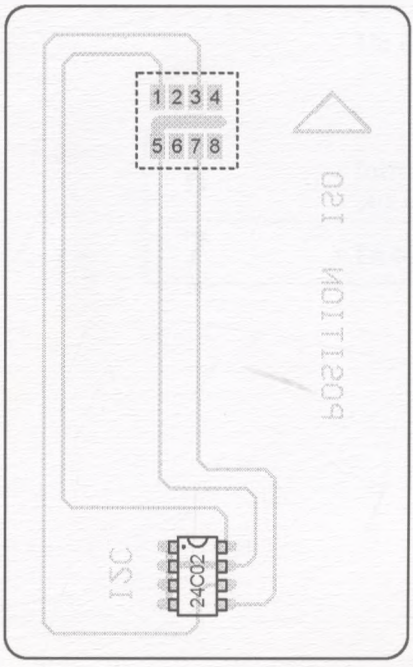



**Figure 4.21.** Plan de câblage de la « fausse carte » I2C.

© DUNOD - La photocopie non autorisée est un délit.



CHAPITRE PAGE

| | | |
|---|---|---|
| 1 | Vocabulaire et normalisation | 1 |
| 2 | Les circuits intégrés pour cartes à puce | 13 |
| 3 | La périphérie des cartes | 37 |
| 4 | Mise en œuvre des cartes synchrones | 67 |

# 5 APPLICATIONS PRATIQUES DES CARTES SYNCHRONES

**Un testeur autonome de télécartes** 106
**Une serrure de sûreté à télécarte** 113
**Un destructeur de cartes à puce** 118

| | | |
|---|---|---|
| 6 | Introduction aux cartes asynchrones | 125 |
| 7 | Le cédérom du livre | 157 |

Savoir lire et écrire dans toutes sortes de cartes à puce synchrones permet d'envisager la mise sur pied d'applications pratiques parfois assez étonnantes.

Même si le recours à un micro-ordinateur compatible PC reste nécessaire pour personnaliser les composants programmables utilisés par les montages qui vont être décrits, ceux-ci seront, par la suite, entièrement autonomes.

Nous espérons ainsi faire entrevoir à nos lecteurs la voie à suivre pour développer leurs propres applications à base de cartes à puce, basées ou non sur l'utilisation d'un PC.

## UN TESTEUR AUTONOME DE TÉLÉCARTES

Notre logiciel GPM256.BAS permet de faire subir une « expertise » en règle à n'importe quelle télécarte « T1G », mais uniquement à l'aide d'un lecteur connecté à un micro-ordinateur compatible PC.

Un testeur autonome, au format de poche, trouvera son utilité à chaque fois que l'on souhaitera tester sommairement une télécarte « sur le terrain », et en particulier savoir si elle est authentique et si elle contient encore des unités. Ce sera ainsi un bon outil de collectionneur.

Le schéma de la figure 5.1 est basé sur un principe que nous avons imaginé à l'origine pour réaliser des serrures électroniques à cartes ou clefs à mémoire (et nous allons y venir !)

Un petit automate simplifié est programmé par le biais d'une EPROM qui contient à la fois la séquence des signaux nécessaires à la lecture de la carte, et la description des états que doit prendre sa sortie. Si au cours du cycle un état de sortie n'est pas conforme à ce qui est attendu, tout s'arrête sur ce « pas de programme » précis.

Nous avons inclus dans le programme des « instructions » commandant l'allumage de voyants à LED lorsque certaines étapes importantes sont franchies avec succès :

- détection d'un « code famille » correspondant aux télécartes T1G ;
- reconnaissance du type de carte attendu (50 ou 120 unités) ;
- comptage d'un nombre de bits à 1 indiquant que le crédit est épuisé.

© DUNOD - La photocopie non autorisée est un délit.





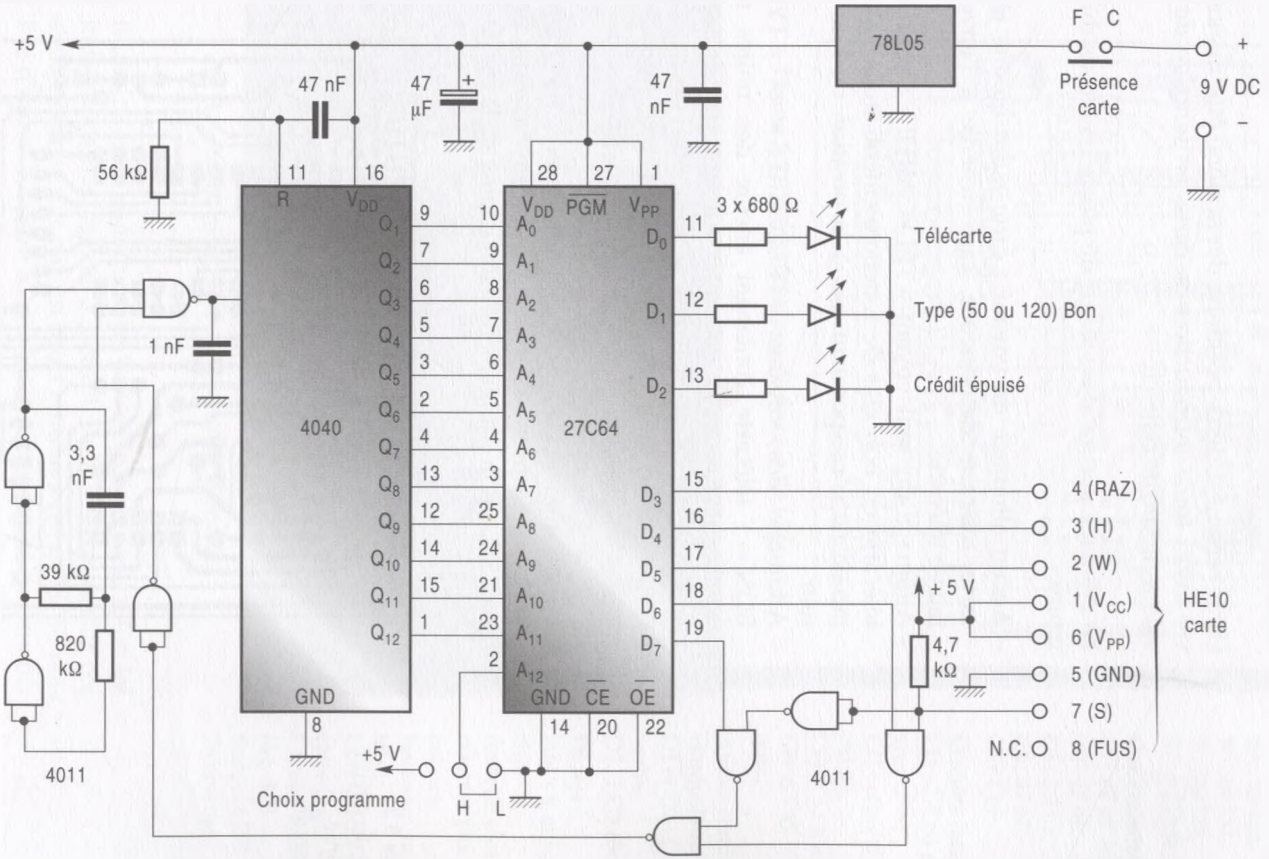



**Figure 5.1.** Schéma du testeur de télécartes

Deux « programmes » distincts sont donc prévus, l'un pour les cartes de 50 unités, et l'autre pour celles de 120 (les 40, véritables pièces de collection, méritent de toute façon un traitement à part).

Un inverseur à deux positions devra donc être manœuvré avant toute introduction de carte, en fonction de la valeur faciale de celle-ci.

Le montage pourra alors réagir de plusieurs façons différentes.

- Aucun allumage de voyant : carte autre qu'une télécarte, télécarte défectueuse, carte insérée à l'envers, fausse télécarte.
- Allumage du seul voyant « TÉLÉCARTE » : véritable télécarte en bon état de fonctionnement, mais valeur faciale ne correspondant pas à la position de l'inverseur.
- Allumage des voyants « TÉLÉCARTE » et « TYPE BON » : télécarte contenant encore des unités (en nombre quelconque), ou unités consommées de façon anormale. Une expertise plus poussée s'impose !
- Allumage des trois voyants (cas hélas le plus fréquent) : télécarte épuisée.

La réalisation de ce petit appareil suppose la gravure d'un circuit imprimé simple face, conforme au tracé de la figure 5.2, et son équipement selon le plan de la figure 5.3.

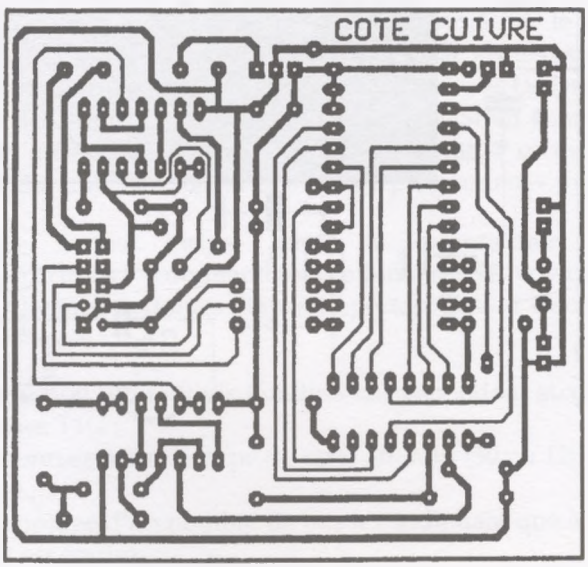



**Figure 5.2.**
Tracé du circuit imprimé du testeur

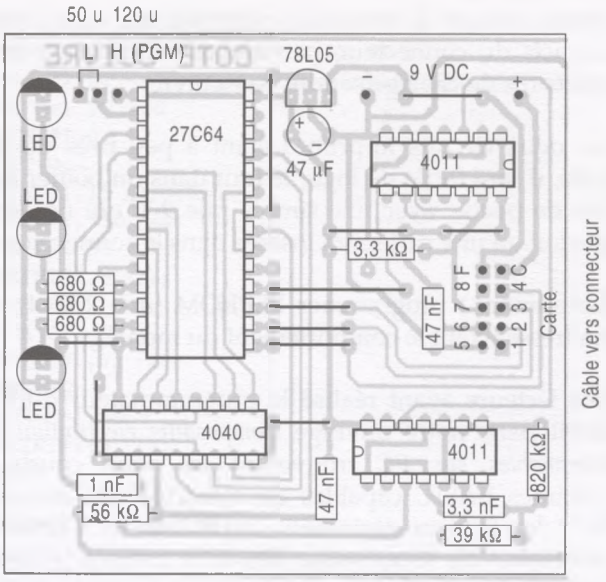
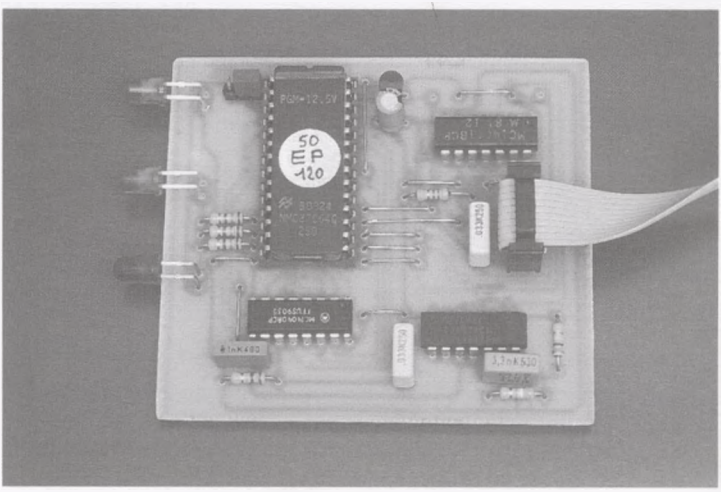



**Figure 5.3.** Plan de câblage du testeur de télécartes.



La platine principale du testeur de télécartes.

*Liste des composants*

**Résistances (5 % 1/4W) :**
R1 à R3 : 680 Ω,
R4 : 3,3 kΩ,
R5 : 56 kΩ,
R6 : 39 kΩ,
R7 : 820 kΩ.

**Condensateurs :**
C1 : 47 µF 16 V,
C2 : 47 nF,
C3 : 3,3 nF,
C4 : 47 nF,
C5 : 1 nF.

**Circuits intégrés :**
CI1 : 27C64 programmée,
CI2 : régulateur 78L05,
CI3 : CD 4040,
CI4 et CI5 : CD 4011.

**Autres semi-conducteurs :**
D1 et D2 : LED vertes,
D3 : LED rouge.

**Divers :**
Pile 9 V et son clip,
Barrette sécable à doubles picots coudés,
Inverseur unipolaire,
Connecteur de carte (fig. 3.4),
Cordon de liaison (fig. 3.2),
Support DIL 28 broches.

Il faudra aussi construire un connecteur de carte selon les indications des figures 3.3 et 3.4, puis interconnecter ces deux platines soit par un court cordon à fiches HE10 réalisé d'après la figure 3.2, soit tout simplement par dix fils souples soudés aux points correspondants des deux platines.

Compte tenu du fait que les T1G existent avec des micromodules en position ISO aussi bien qu'AFNOR, on

© DUNOD - La photocopie non autorisée est un délit.

pourra songer à réunir en parallèle les deux jeux de contacts du connecteur, par exemple au moyen de huit courts fils de câblage soudés côté cuivre.

Les deux circuits imprimés étant à peu près de même taille, il sera facile de loger le tout dans un boîtier au format de poche, avec une simple pile 9 V qui ne débitera que lorsqu'une carte sera insérée dans le connecteur.

Reste enfin à programmer l'EPROM (une 27C64), pièce maîtresse fixant le comportement du montage.

Nos lecteurs ayant réalisé le programmateur d'EPROM décrit dans notre ouvrage *Composants électroniques programmables sur PC* trouveront ici deux courts programmes BASIC capables de construire sur un simple RUN les fichiers décimaux « 50.ROM » et « 120.ROM » nécessaires au remplissage des deux moitiés (A12 à 0 et A12 à 1) de la mémoire.

```
10 REM ----- CRED50.BAS -----
20 OPEN "50.rom" FOR OUTPUT AS #1
30 CLS :PRINT"----- Création fichier 50.ROM en cours -----"
40 FOR G=1 TO 100
50 PRINT#1,0 ;
60 NEXT G
70 PRINT#1,16 ;0;0;0;
80 PRINT#1,136 ;24;
90 FOR G=1 TO 7
100 PRINT#1,8 ;24;
110 NEXT G
120 FOR G=1 TO 4
130 PRINT#1,72 ;24;
140 NEXT G
150 FOR G=1 TO 4
160 PRINT#1,8 ;24;
170 NEXT G
180 FOR G=1 TO 72
190 PRINT#1,9 ;25;
200 NEXT G
210 FOR G=1 TO 5
220 PRINT#1,73 ;25;
230 NEXT G
240 PRINT#1,137 ;25;137;25;73;25;
250 FOR G=1 TO 60
260 PRINT#1,139 ;27;
270 NEXT G
280 PRINT#1,199 ;
290 CLOSE
300 CLS :PRINT"----- LE FICHIER 50.ROM EST DISPONIBLE -----
310 END
320 REM (c)1993,1995 Patrick GUEULLE
```

```
10 REM ----- CRED120.BAS -----
20 OPEN "120.rom" FOR OUTPUT AS #1
30 CLS :PRINT"----- Création fichier 120.ROM en cours -----"
40 FOR G=1 TO 100
50 PRINT#1,0 ;
60 NEXT G
70 PRINT#1,16 ;0;0;0;
80 PRINT#1,136 ;24;
90 FOR G=1 TO 7
100 PRINT#1,8 ;24;
110 NEXT G
120 FOR G=1 TO 4
130 PRINT#1,72 ;24;
140 NEXT G
150 FOR G=1 TO 4
160 PRINT#1,8 ;24;
170 NEXT G
180 FOR G=1 TO 72
190 PRINT#1,9 ;25;
200 NEXT G
210 PRINT#1,73 ;25;73;25;73;25;137;25;
220 PRINT#1,73 ;25;73;25;137;25;137;25;
230 FOR G=1 TO 130
240 PRINT#1,139 ;27;
250 NEXT G
260 PRINT#1,199 ;
270 CLOSE
280 CLS :PRINT"----- LE FICHIER 120.ROM EST DISPONIBLE -----
290 END
300 REM (c)1993, 1995 Patrick GUEULLE
```

Ceux qui possèdent un programmateur différent pourront se tourner vers les fichiers au format « INTEL HEX" correspondants (50.HEX et 120.HEX).

Fichier 50.HEX :

```
:10000000000000000000000000000000000000F0
:10001000000000000000000000000000000000E0
:10002000000000000000000000000000000000D0
:10003000000000000000000000000000000000C0
:10004000000000000000000000000000000000B0
:10005000000000000000000000000000000000A0
:1000600000000000100000008818081808180818 80
:1000700008180818081808184818481848184818 80
:1000800008180818081808180919091909190919 68
:1000900009190919091909190919091909190919 50
:1000A0000919091909190919091909190919091940
:1000B0000919091909190919091909190919091930
:1000C0000919091909190919091909190919091920
:1000D0000919091909190919091909190919091910
:1000E0000919091909190919091909190919091900
:1000F0000919091909190919091909190919 0F0
:1001000009190919091909190919091909190919DF
:1001100009190919091909194919491949194919CF
```

© DUNOD - La photocopie non autorisée est un délit.

```
:10012000491989198919491988B1B8B1B8B1B8B1B2F
:100130008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8F
:100140008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B7F
:100150008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B6F
:100160008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B5F
:100170008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B4F
:100180008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B3F
:100190008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B2F
:0101A000C797
:00000001FF
```

Fichier 120.HEX :

```
:10000000000000000000000000000000000000000F0
:10001000000000000000000000000000000000000E0
:10002000000000000000000000000000000000000D0
:10003000000000000000000000000000000000000C0
:10004000000000000000000000000000000000000B0
:10005000000000000000000000000000000000000A0
:10006000000000001000000088180818081880
:10007000081808180818081848184818481880
:10008000081808180818081809190919091968
:10009000091909190919091909190919091950
:1000A000091909190919091909190919091940
:1000B000091909190919091909190919091930
:1000C000091909190919091909190919091920
:1000D000091909190919091909190919091910
:1000E000091909190919091909190919091900
:1000F0000919091909190919091909190919F0
:10010000091909190919091909190919DF
:10011000091909190919491949194914989198F
:1001200049194919891989198B1B8B1B8B1B8B1B2F
:100130008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8F
:100140008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B7F
:100150008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B6F
:100160008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B5F
:100170008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B4F
:100180008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B3F
:100190008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B2F
:1001A0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B1F
:1001B0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B0F
:1001C0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BFF
:1001D0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BEF
:1001E0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BDF
:1001F0008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BCF
:100200008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BBE
:100210008B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1B8B1BAE
:0D0220008B1B8B1B8B1B8B1B8B1B8B1BC726
:00000001FF
```

À défaut, de nombreux revendeurs sont capables de programmer ou faire programmer une EPROM à partir de ces données.

## UNE SERRURE DE SÛRETÉ À TÉLÉCARTE

La serrure électronique est une application très populaire des cartes à puce, dont il existe d'ailleurs des réalisations commerciales basées le plus souvent sur l'emploi d'un microcontrôleur.

Le schéma de la figure 5.4 est basé, pour sa part, sur le même principe que le testeur que nous venons d'étudier, mais la programmation de l'EPROM est totalement différente. Elle devra en effet être personnalisée en fonction du contenu des cartes habilitées à déclencher le relais pilotant la gâche électrique (ou ce que chacun voudra).

Deux relais cohabitent cependant sur la platine, dont l'un ne devra en principe jamais coller. Si cela devait arriver, cela signifierait que la serrure est en défaut, et l'ouverture du contact « repos » du relais de sécurité empêcherait la gâche d'être commandée.

Trois voyants à LED visualisent les principaux états de l'automate, ce qui sera précieux en cas d'anomalie.

Deux variantes de fonctionnement sont possibles, selon que l'on câblera ou non la diode de remise à zéro anticipée du compteur 4040. Sans diode, le collage du relais durera tant que la (bonne) carte sera présente dans le connecteur, tandis qu'avec la diode ce collage sera intermittent.

Cette seconde option renforce la sécurité du système, car à la moindre anomalie dans le cycle, celui-ci repart à zéro au lieu de rester en attente d'un événement qui pourrait lui permettre de se poursuivre normalement.

Là encore, les deux moitiés de la 2764 peuvent héberger deux programmes différents. L'un pour le jour et l'autre pour la nuit, par exemple, ou encore l'un pour la semaine et l'autre pour le week-end.

Le circuit imprimé du module principal sera gravé selon le tracé de la figure 5.5, puis câblé (sans oublier les straps !) d'après la figure 5.6.

La disposition des pastilles a été prévue pour que des borniers à vis puissent équiper l'alimentation et le contact de sortie, facilitant ainsi l'installation.

© DUNOD - La photocopie non autorisée est un délit.

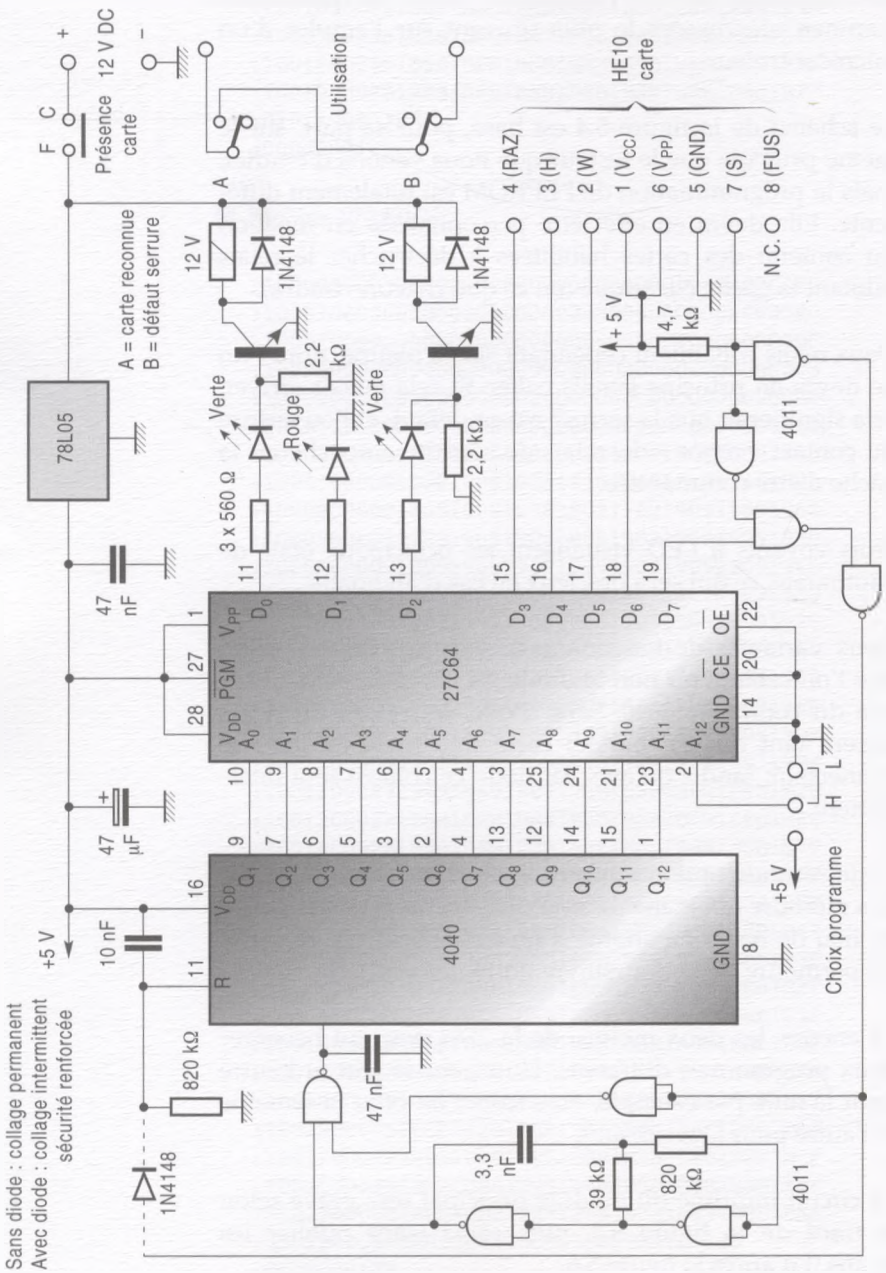



**Figure 5.4.** Schéma de la serrure à télécarte.

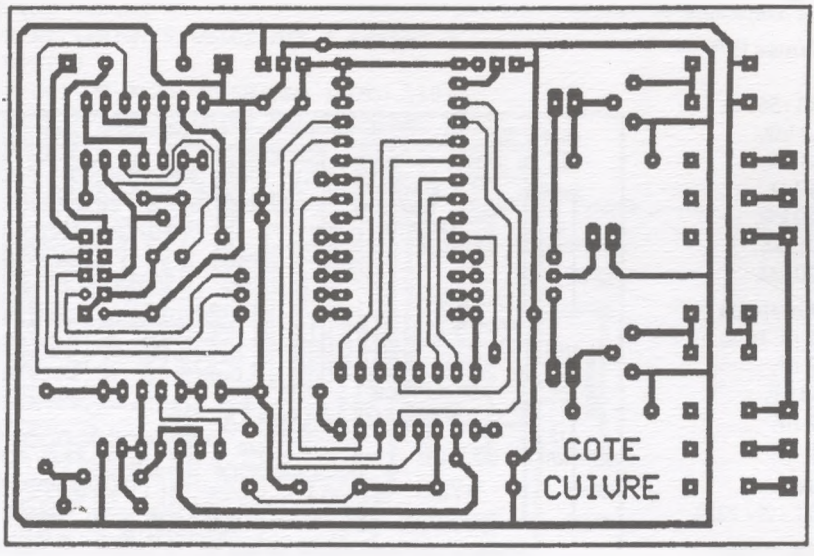



**Figure 5.5.** Tracé du circuit imprimé de la serrure.

On ne saurait trop insister sur la nécessité impérative de monter ce module en lieu sûr. Nous avons vu beaucoup trop de prétendus systèmes de sécurité entièrement installés dans un boîtier extérieur, qu'il suffit de forcer pour accéder à deux fils qui, mis en court-circuit, déclenchent l'ouverture de la porte...

Pour les essais, le connecteur de carte pourra être relié à la serrure par notre habituel cordon HE10, mais sur le terrain, on préfèrera en général employer du câble téléphonique à 5 paires raccordé par wrapping sur les barrettes à picots carrés équipant les deux platines.

La longueur de ce câble devra rester raisonnable, et en tout cas inférieure à un mètre, le plus court étant évidemment le mieux.

Reste une fois encore à programmer l'EPROM en fonction du comportement souhaité pour l'ensemble.

```
10 REM ----- SERRURE.BAS -----
20 CLS :PRINT"Nom du fichier .CAR à utiliser ?"
30 INPUT N$ :C$=N$+".CAR" :R$=N$+".ROM"
40 CLS :PRINT"La carte contient 256 bits : 1 à 256"
50 OPEN C$ FOR INPUT AS #1
60 PRINT :PRINT"----------------------------------------"
70 PRINT :PRINT"        Zone  fabricant : 1 à 96"
80 OPEN R$ FOR OUTPUT AS #2
90 PRINT :PRINT"        Zone des unités : 97 à 256"
```

© DUNOD - La photocopie non autorisée est un délit.

*Liste des composants*

**Résistances (5 % 1/4W) :**
R1 à R3 : 560 Ω,
R4 : 2,2 kΩ,
R5 : 3,3 kΩ,
R6 : 39 kΩ,
R7 : 820 kΩ,
R8 : 2,2 kΩ,
R9 : 820 kΩ.

**Condensateurs :**
C1 : 47 µF 16 V,
C2 : 47 nF,
C3 : 3,3 nF,
C4 : 47 nF,
C5 : 10 nF.

**Transistors :**
T1 et T2 : 2N 2222.

**Circuits intégrés :**
CI1 : 27C64 programmée,
CI2 : régulateur 78L05,
CI3 : CD 4040,
CI4 et CI5 : CD 4011.

**Autres semi-conducteurs :**
D1 et D2 : LED vertes,
D3 : LED rouge,
D4 à D6 : 1N 4148.

**Divers :**
2 relais 12 V DIL 2RT,
Barrette sécable à doubles picots coudés,
4 borniers à vis à 2 circuits,
Connecteur de carte (fig. 3.4),
Cordon de liaison (fig. 3.2),
Support DIL 28 broches,
Barrette sécable à picots droits,
1 cavalier de court-circuit 2,54 mm,
Alimentation 12 V continu.

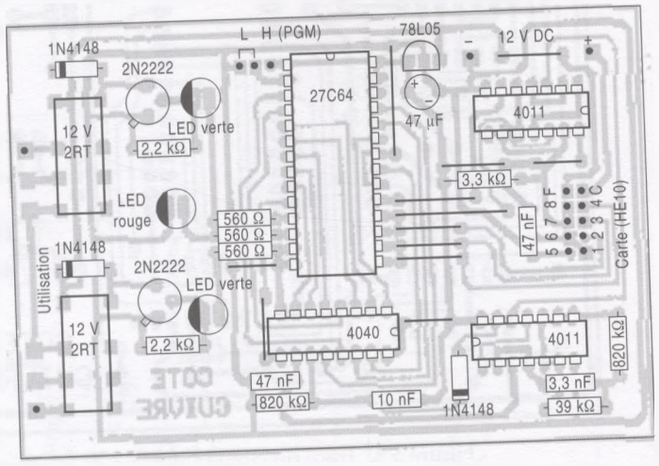
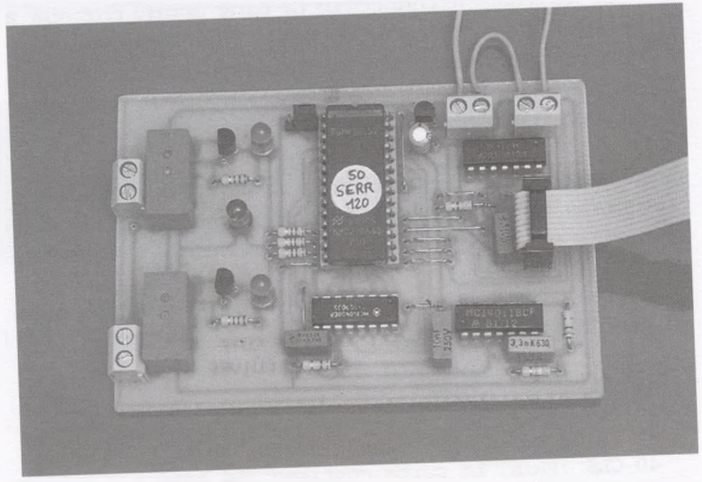



**Figure 5.6.** Plan de câblage de la serrure.




La platine principale de la serrure à carte à puce.





```
100 PRINT :PRINT"-----------------------------------------"
110 PRINT :PRINT"Premier bit à tester ?"
120 INPUT D
130 IF D<1 OR D>255 THEN CLS :GOTO 110
140 PRINT :PRINT"Dernier bit à tester ?"
150 INPUT F
160 IF F<=D OR F>256 THEN CLS :GOTO 110
170 CLS :PRINT"----- Création fichier ";R$;" en cours -----"
180 FOR G=1 TO 100
190 PRINT#2,0 ;
200 NEXT G
210 PRINT#2,16 ;0;0;0;
220 FOR G=1 TO D-1
230 INPUT#1,B
240 PRINT#2,10 ;26;
250 NEXT G
260 FOR G=D TO F
270 INPUT#1,B
280 IF B=0 THEN PRINT#2,74 ;26;
290 IF B=1 THEN PRINT#2,138 ;26;
300 NEXT G
310 FOR G=1 TO 3000
320 PRINT#2,1 ;
330 NEXT G
340 PRINT#2,193 ;
350 CLOSE
360 CLS :PRINT"----- LE FICHIER ";R$;" EST DISPONIBLE -----
370 END
380 REM (c)1993 Patrick GUEULLE
```

Le logiciel SERRURE.BAS permet de construire le fichier « .ROM » nécessaire, à partir du fichier « .CAR » qui reproduit le contenu de la carte devant servir de clef. Celle-ci aura par conséquent été tout d'abord lue avec GPM256.BAS.

Il suffit de préciser la zone de la carte que devra contrôler la serrure, pour que le contenu de l'EPROM soit automatiquement préparé en conséquence.

Si on demande la lecture des bits 1 à 96 (autrement dit de la « zone fabricant » dans son intégralité), alors une seule et unique télécarte (incopiable) pourra déclencher la serrure. Il importera de ne pas la perdre...

En revanche, la même procédure appliquée à une « carte lavage » BP ou MOBIL permettrait à toutes les cartes de même valeur faciale d'être reconnues puisqu'elles sont strictement identiques.

© DUNOD - La photocopie non autorisée est un délit.

L'approche la plus souple possible nous paraît être la suivante :

- à l'aide du logiciel GPM256.BAS et d'un des lecteurs décrits au chapitre 4, lire une télécarte de 50 unités ou une « carte lavage », évidemment épuisée ;
- sauvegarder le résultat de cette lecture dans un fichier « .CAR » ;
- au moyen d'un éditeur de texte, y écrire un code composé d'une suite quelconque de « 1 » et de « 0 » dans la zone inutilisée de la carte, remplie pour le moment de « 0 » (une douzaine de bits fera amplement l'affaire) ;
- recharger le fichier ainsi modifié dans GPM256.BAS ;
- programmer avec ce fichier toutes les cartes (du même type) devant pouvoir déclencher la serrure ;
- utiliser ce même fichier « .CAR » avec le logiciel SERRURE.BAS pour construire le fichier « .ROM » de programmation de l'EPROM de la serrure.

Cette fois, les cartes ainsi personnalisées sont copiables. En revanche, on peut aussi enregistrer, dans différentes zones de chaque carte, plusieurs codes correspondant à différentes serrures.

## UN DESTRUCTEUR DE CARTES À PUCE

Les cartes à puce ont cela de particulier que même celles qui sont considérées comme parfaitement anonymes (télécartes, porte-monnaie électroniques, etc.) peuvent fort bien contenir, en général à l'insu de leur porteur, des informations personnelles parfois embarrassantes pour celui-ci...

Sans aller jusqu'à brûler ou découper en menus morceaux des cartes potentiellement « compromettantes » mais possédant peut-être une valeur de collection, on pourra souhaiter faire disparaître radicalement le contenu de certaines puces soupçonnées d'indiscrétion.

Après tout, il existe bien des « destructeurs de documents », alors pourquoi pas des « destructeurs de cartes à puce » ?

Le plus sûr moyen de rendre inutilisable une carte à puce, sans l'abîmer extérieurement, consiste à appliquer des tensions excessives entre certains de ses contacts.

L'immunité aux surtensions des circuits de cartes à puce a cependant fait de tels progrès ces derniers temps qu'il faut vraiment « frapper fort ».

En effet, il faut savoir qu'un test normalisé des plus courants consiste à relier au composant testé un condensateur de 150 pF chargé sous 4000 à 8000 V, cela à travers une résistance de 330 Ω.

Il en résulte, tout de même, un courant de crête pouvant atteindre une bonne vingtaine d'ampères (A), qui ne doit avoir aucun effet destructeur, ni même fragilisateur...

Après tout, une carte à puce manipulée par un porteur de vêtements en textiles synthétiques subit couramment ce genre d'agression, surtout par temps sec.

Pour obtenir de véritables effets dévastateurs, il faut augmenter massivement l'énergie injectée dans la puce, ce qui ne passe pas nécessairement par la mise en œuvre de très hautes tensions : il suffit tout simplement d'utiliser un condensateur de valeur beaucoup plus forte.

Parallèlement, l'augmentation du courant de crête (facile à obtenir en réduisant la valeur de la résistance de limitation du courant) donne aussi de bons résultats (fusion des très fins fils de raccordement de la puce).

Le schéma de la figure 5.7 utilise ainsi un condensateur de 0,47 à 0,68 µF (ou éventuellement davantage) chargé à la tension de crête du secteur 220 V, c'est-à-dire un bon 300 V.

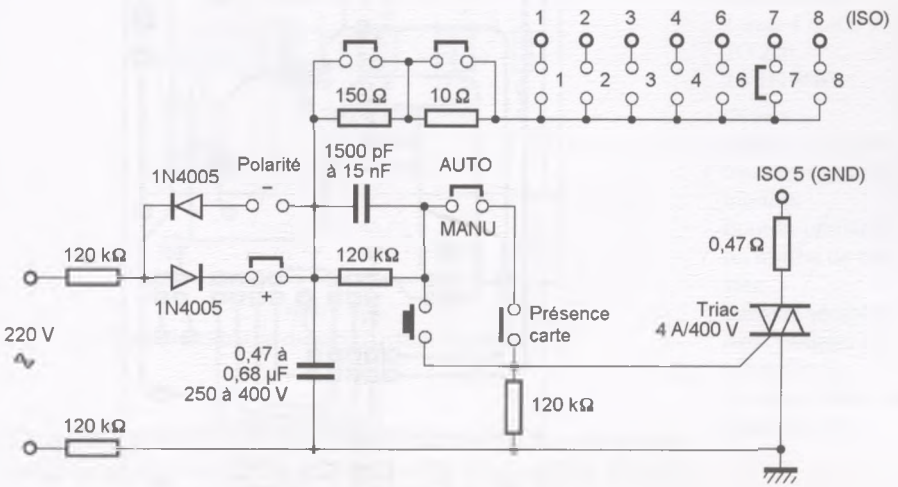



**Figure 5.7.** Schéma du destructeur de cartes à puce.

© DUNOD - La photocopie non autorisée est un délit.

Nous avons prévu une possibilité d'inversion de la polarité de cette tension, et de choix de la valeur de la résistance série (de 0,47 à 160 Ω).

Un système de commutation très simple permet par ailleurs de « torturer » séparément chaque contact de la puce, selon le type de défaut qu'on souhaite faire apparaître.

Enfin, le « tir » peut être soit manuel (quand on veut appliquer plusieurs « coups » successifs), soit automatique par simple insertion de la carte dans son connecteur.

Afin d'éviter tout risque d'endommagement des contacts par des courants aussi élevés (jusqu'à plusieurs centaines d'ampères en pointe), il a été choisi d'utiliser un robuste triac comme élément de commutation.

Celui-ci peut être déclenché soit par un bouton-poussoir, soit par le contact de « présence carte » du connecteur.

La réalisation pratique du montage suppose la gravure d'un circuit imprimé conforme au tracé de la figure 5.8.

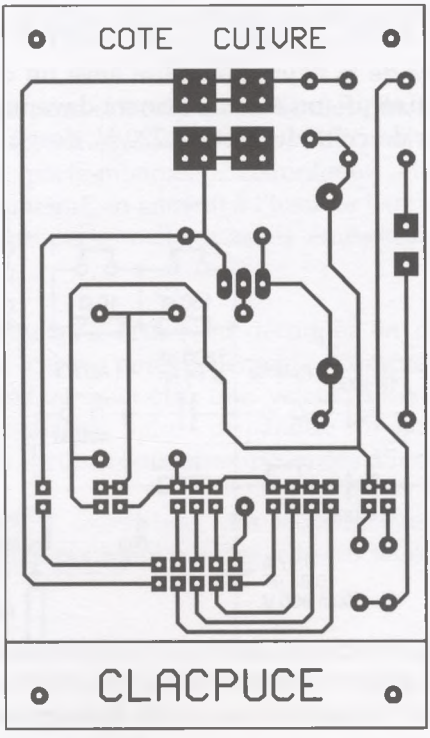



**Figure 5.8.**
Tracé du circuit imprimé du destructeur de cartes.

Celui-ci a été spécialement étudié pour prendre place dans un boîtier « prise de courant » (grand modèle) servant habituellement à la construction de blocs secteur.

Le connecteur de carte à puce sera raccordé par l'habituel câble méplat équipé de deux fiches HE10 à dix contacts, venant se brancher sur un tronçon de barrette sécable à double rangée de picots carrés droits.

D'autres morceaux de la même barrette serviront de supports à des cavaliers de court-circuit au pas de 2,54 mm, servant à établir les commutations qui permettent le réglage de l'appareil.

Le reste des composants, c'est-à-dire assez peu de chose, sera enfin monté en accord avec le plan de la figure 5.9.

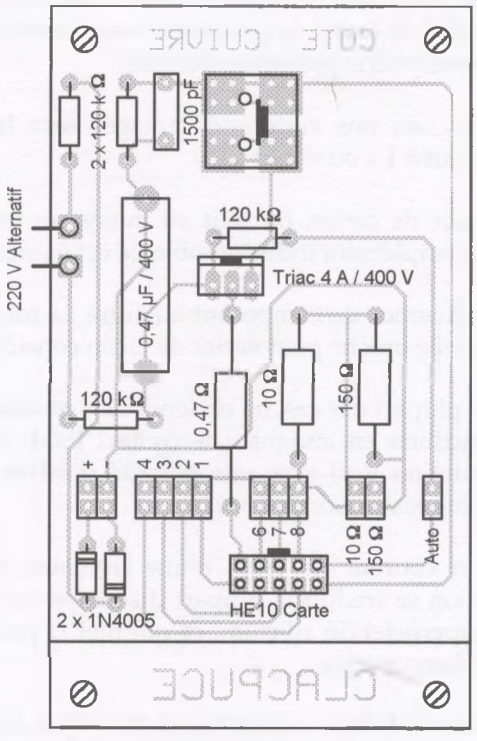



**Figure 5.9.**
Plan de câblage du destructeur de cartes.

*Liste des composants*

**Résistances :**
4 x 120 kΩ 1/4 W,
0,47 Ω vitrifiée 1 W,
10 Ω vitrifiée 1 W,
150 Ω vitrifiée 1 W.

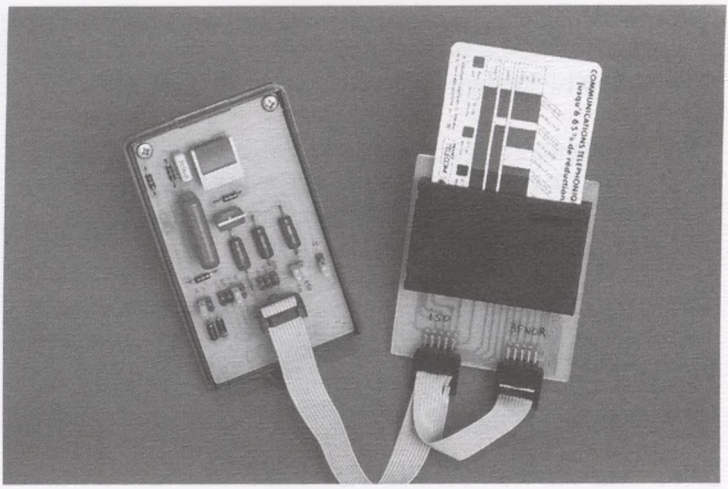
**Condensateurs :**
0,47 à 0,68 µF 400 V,
1500 pF à 15 nF 400 V (selon triac).

**Semi conducteurs :**
1 triac 4 A 400 V TO 220,
2 x 1N 4005.

**Divers :**
Boîtier « prise de courant » grand modèle,
Bouton-poussoir ou touche de clavier,
Barrette sécable à deux rangées de picots carrés,
Lot de cavaliers de court-circuit.

On remarquera qu'un pastillage « universel » a été prévu pour la touche ou le bouton-poussoir, permettant d'utiliser quasiment n'importe quel modèle disponible.

© DUNOD - La photocopie non autorisée est un délit.



Le destructeur de cartes à puce équipé de son connecteur.

L'exploitation efficace de ce destructeur de cartes à puce suppose l'acquisition d'un minimum de savoir-faire, et, en tout état de cause, la possibilité de contrôler immédiatement toute carte présumée détruite.

Selon les cas, une carte endommagée sera lue comme étant « tout à 1 » ou « tout à 0 ».

Un lecteur de cartes, ou tout au moins un testeur, sera ainsi le complément indispensable de cet équipement.

D'une référence de composant à l'autre, la robustesse de telle ou telle broche peut varier de façon considérable.

Dans la plupart des cas, on obtiendra les résultats les plus reproductibles en attaquant le contact ISO1 (c'est-à-dire l'alimentation Vcc) avec une polarité positive et au travers d'une résistance de 10 Ω.

Avec un courant de crête d'une trentaine d'ampères, l'opération se traduit la plupart du temps par un percement superficiel du silicium, ce qui met la puce définitivement hors service.

En présence de la seule résistance de 0,47 Ω, surtout destinée à protéger le triac, on obtient bien souvent la rupture du fil d'alimentation Vcc, ou parfois de celui de masse. N'étant plus alimentée, la puce est, là encore, inutilisable.

Avec 150 Ω, il n'est pas rare que la puce résiste. On pourra évaluer sa robustesse en renouvelant plusieurs

fois la sollicitation, qu'on fera systématiquement suivre d'une lecture de contrôle. Le nombre d'opérations nécessaires à la destruction de la puce (ou à la perturbation plus ou moins sévère de son fonctionnement) renseignera assez fidèlement sur son degré d'endurance.

Qu'il nous soit permis, pour conclure, de préciser que ce montage n'a nullement été conçu pour rendre défectueuses (et par conséquent remboursables...) des télécartes usagées, ou pour perturber la mise en place, par exemple, de la « carte santé » !

© DUNOD - La photocopie non autorisée est un délit.

| CHAPITRE | | PAGE |
|---|---|---|
| 1 | Vocabulaire et normalisation | 1 |
| 2 | Les circuits intégrés pour cartes à puce | 13 |
| 3 | La périphérie des cartes | 37 |
| 4 | Mise en œuvre des cartes synchrones | 67 |
| 5 | Applications pratiques des cartes synchrones | 105 |


# 6 INTRODUCTION AUX CARTES ASYNCHRONES


**La structure des cartes asynchrones** 127
**Un lecteur-encodeur simplifié** 128
**Lecture de la réponse au reset** 137
**Décodage de la réponse au reset** 143
**Le dialogue avec les cartes** 146
**Exemples pratiques** 154

| | | |
|---|---|---|
| 7 | Le cédérom du livre | 157 |

Si la mise en œuvre des cartes à puce les plus simples se limite, comme nous venons de le voir, à y lire ou y écrire des bits de données, le cas des cartes à microprocesseur (autrement dit asynchrones) est beaucoup plus complexe.

Authentiques micro-calculateurs subminiatures, ces cartes dialoguent véritablement avec leur lecteur-encodeur en échangeant des octets sur une liaison série asynchrone et bidirectionnelle.

Beaucoup moins coûteux que les « kits de développement » du commerce, le lecteur-encodeur simplifié dont nous allons décrire la réalisation va pourtant vous permettre de lire et écrire dans la plupart des cartes asynchrones actuellement en circulation !

## LA STRUCTURE DES CARTES ASYNCHRONES

Nettement plus chères que les cartes synchrones, les cartes à microprocesseur sont réservées à des applications exigeant soit des fonctionnalités complexes, soit une très haute sécurité, soit les deux : monétique, télévision à péage, téléphone cellulaire, etc.

La figure 6.1 dévoile l'architecture interne selon laquelle sont réalisées quasiment toutes les cartes asynchrones, au coeur desquelles se trouve un microprocesseur spécial mais souvent dérivé d'une famille courante (68HC705 chez MOTOROLA ou SGS-THOMSON, TMS 370 chez TEXAS INSTRUMENTS, 8051 chez PHILIPS, etc.)

Comme toutes les cartes à puce, une carte asynchrone a pour principale mission d'assurer la sécurité des données qui sont enregistrées dans sa mémoire non volatile.

Cette sécurité est obtenue en interdisant tout accès direct, depuis l'extérieur, au contenu de la mémoire. Toute opération de lecture, d'écriture, ou d'authentification transite obligatoirement par le microprocesseur embarqué qui, seul, peut accéder physiquement à la mémoire.

En pratique, on enverra un ordre à la carte, et c'est le microprocesseur qui décidera de l'exécuter ou non selon les règles de sécurité qu'il est programmé pour appliquer.

La réponse de la carte se composera donc d'un « compte-rendu » précisant la suite qui a pu être donnée à l'ordre ainsi « filtré », et s'il y a lieu d'un bloc de données, éventuellement crypté.

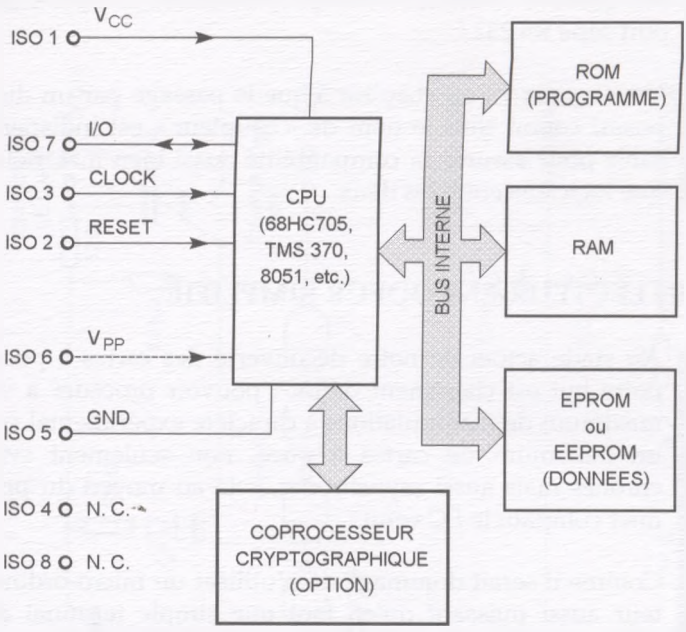
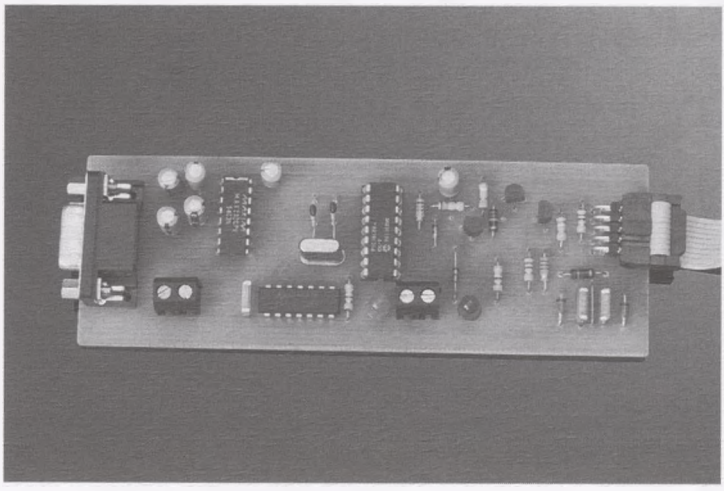



**Figure 6.1.** Structure type d'une carte asynchrone.



La platine principale du lecteur-encodeur de cartes asynchrones.

Dans l'état actuel de la technique, tous ces échanges de « questions et réponses » se font en « *half-duplex* », sur une seule ligne d'entrée-sortie série (le contact ISO 7 de la carte).

La norme ISO 7816 prévoit différents protocoles de communication, mais le dialogue se fait bien souvent à 9 600 bits par seconde avec huit bits de données, un bit de parité paire, et l'équivalent d'au moins deux bits de stop.

© DUNOD - La photocopie non autorisée est un délit.

Pas question toutefois de relier directement la carte à un port série RS 232 !

Nous avons vu au chapitre 3 que le passage par un dispositif connu sous le nom de « coupleur » est indispensable pour assurer la compatibilité aussi bien matérielle que logicielle entre les deux.

## UN LECTEUR-ENCODEUR SIMPLIFIÉ

Au stade actuel de notre découverte des cartes à puce, notre but est clairement défini : pouvoir procéder à un maximum de manipulations à caractère expérimental sur un maximum de cartes à puce, non seulement synchrones mais aussi asynchrones, cela au moyen du premier compatible PC venu.

Comme il serait dommage de n'utiliser un micro-ordinateur aussi puissant qu'en tant que simple terminal de communication, nous avons pris le parti de simplifier au maximum le coupleur et d'intégrer une partie de ses fonctions dans des logiciels exécutables par le PC. Cela facilitera l'évolution de l'ensemble sans remise en cause de la partie « *firmware* ».

Le microcontrôleur du coupleur (un PIC 16C84) sera ainsi chargé de la délicate question de la mise sous tension et hors tension des contacts de la carte de façon « propre », de la fourniture du signal d'horloge, et enfin de l'adaptation entre la ligne de données bidirectionnelle de la carte à puce et les lignes TXD/RXD « à sens unique » de la RS 232.

Plutôt que d'employer un circuit intégré spécifique risquant de poser tôt ou tard des problèmes d'approvisionnement, nous avons confié les fonctions d'interface électrique à une poignée de composants discrets qui s'en tirent finalement fort bien dans notre contexte.

Tous ces choix, résolument originaux, se traduisent par le schéma de la figure 6.2 qui appelle les précisions suivantes.

Normalement prévu pour être alimenté sous une tension unique de + 5 V (disponible sur la broche N° 1 de la prise DB15 « joystick » du PC), le montage possède une entrée auxiliaire pour une éventuelle alimentation Vpp.

© DUNOD - La photocopie non autorisée est un délit.





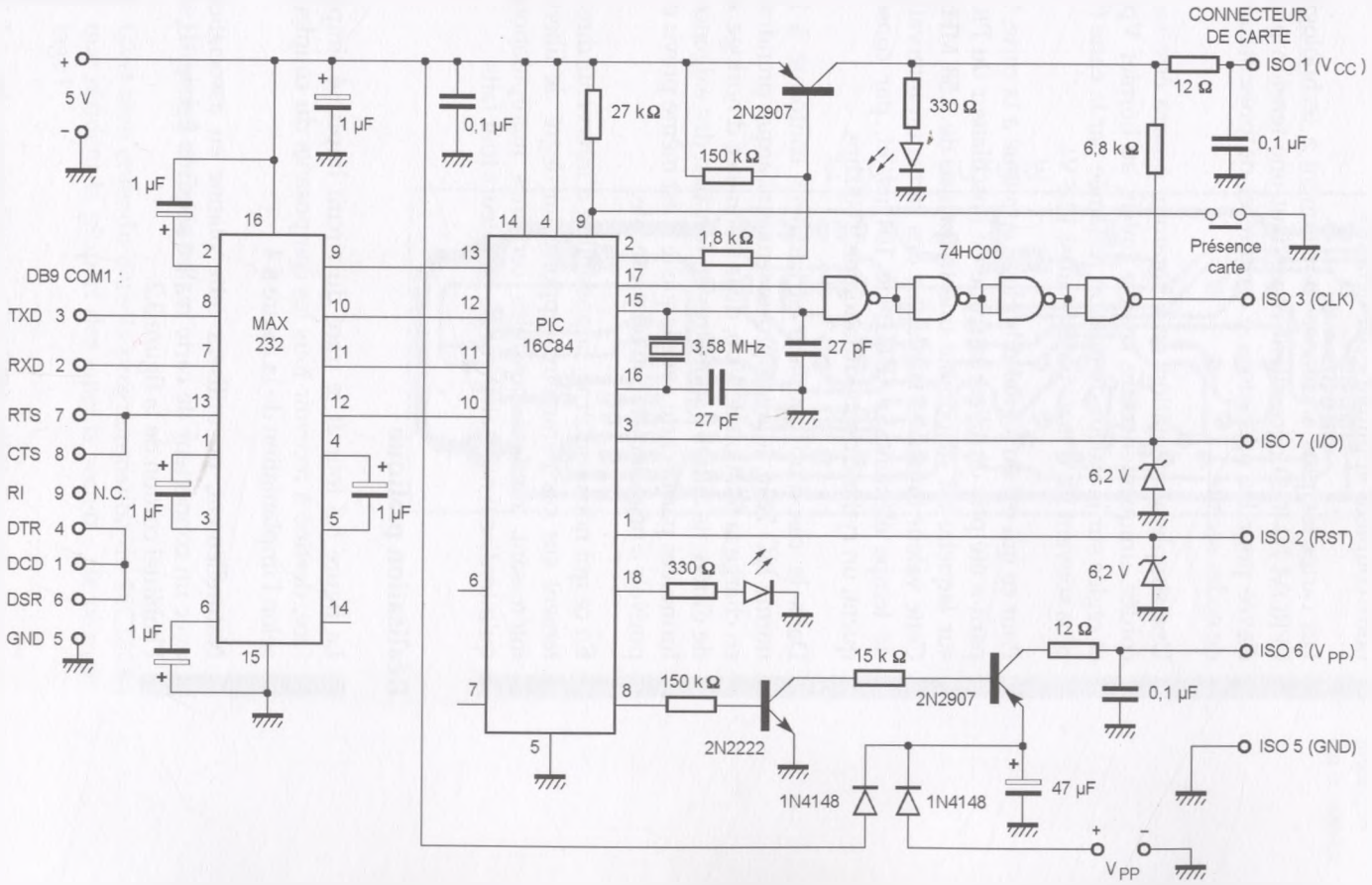



**Figure 6.2.** Schéma du coupleur simplifié.

Il faut savoir que toutes les cartes asynchrones sont en principe lisibles en présence d'un Vpp de 5 V, valeur que notre coupleur applique « par défaut ».

Les cartes les plus anciennes (notamment à technologie EPROM NMOS) nécessitent cependant une tension plus élevée pour les opérations d'écriture et de présentation de codes secrets.

Une simple alimentation de laboratoire pourra être raccordée, uniquement dans ces cas précis, au bornier Vpp et réglée sur la valeur de tension réclamée par la carte (le plus souvent 21 V, mais parfois aussi 12,5 V).

Pour ce qui est du signal d'horloge appliqué à la carte, le parti a été pris d'utiliser la sortie de l'oscillateur du PIC, sur laquelle est disponible une fréquence de 3,58 MHz. Cette valeur impose à la plupart des cartes un intervalle de temps élémentaire (ETU) de 104 µs, et, par conséquent, un rythme de modulation de 9 600 bps.

Dans le cas d'un coupleur strictement conforme à la norme ISO 7816, le microprocesseur embarqué prendrait en charge la fixation de Vpp, de la fréquence d'horloge, et de différents autres paramètres en fonction des exigences formulées par la carte avec laquelle il est même prévu de pouvoir « négocier » tel ou tel protocole.

En ce qui nous concerne, la possibilité d'intervenir directement sur ces paramètres apporte un degré de liberté intéressant, rendant possibles certaines manipulations qu'interdisent normalement les coupleurs tout faits.

## Réalisation pratique

La figure 6.3 fournit le tracé du circuit imprimé simple face, destiné à recevoir tous les composants du coupleur selon l'implantation de la figure 6.4.

Naturellement, on utilisera cette platine en association avec un connecteur de carte réalisé selon la figure 3.3, et l'habituel cordon de la figure 3.2.

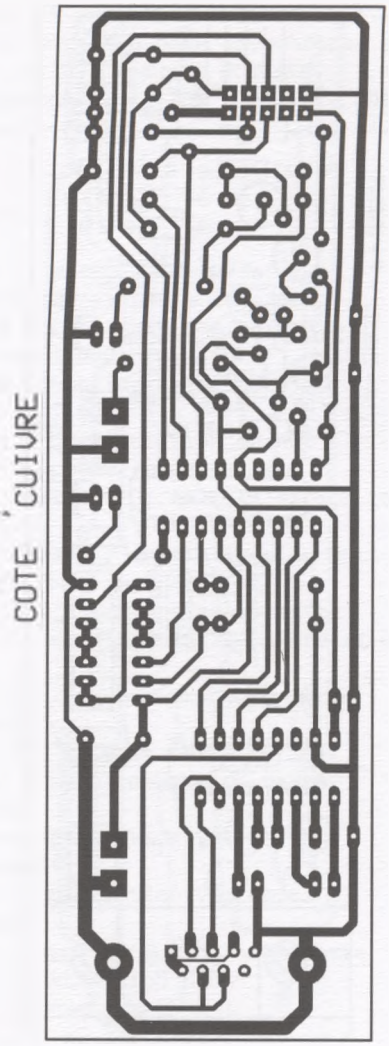



**Figure 6.3.**
Tracé du circuit imprimé du coupleur.

## Le logiciel embarqué

C'est bien entendu dans la programmation du PIC16C84 que résident la plupart des « petits secrets » de ce montage !

Le code source (fichier COUP84.ASM) n'est pourtant pas très long, et n'a absolument aucun rapport avec ce que serait celui d'un coupleur « professionnel ».

© DUNOD - La photocopie non autorisée est un délit.

*Liste des composants*

**Résistances (5 % 1/4 W) :**
R1 : 330 Ω,
R2 : 27 kΩ,
R3 : 150 kΩ,
R4 : 390 kΩ,
R5 : 15 kΩ,
R6 : 330 Ω,
R7 : 12 Ω,
R8 : 1,8 kΩ,
R9 : 150 kΩ,
R10 : 6,8 kΩ,
R11 : 12 Ω.

**Condensateurs :**
C1 à C5 : 1 µF 16 V radial ou tantale goutte,
C6 et C7 : 27 pF,
C8 : 47 µF 10 V radial ou tantale goutte.
C9 à C11 : 0,1 µF.

**Circuits intégrés :**
CI1 : MAX 232,
CI2 : PIC16C84 programmé.
CI3 : 74HC00

**Transistors :**
T1 et T2 : 2N 2907,
T3 : 2N 2222.

**Diodes :**
D1 : LED verte,
D2 : LED rouge,
D3 et D4 : zeners 6,2 V 1/2 W,
D5 et D6 : 1N 4148.

**Divers :**
Q1 : quartz 3,579 MHz,
Barrette sécable à doubles picots carrés coudés,
Embase DB9 femelle coudée pour CI,
Bornier à 2 circuits (5,08 mm),
Connecteur de carte (figure 3.3),
Cordon de liaison (figure 3.2).

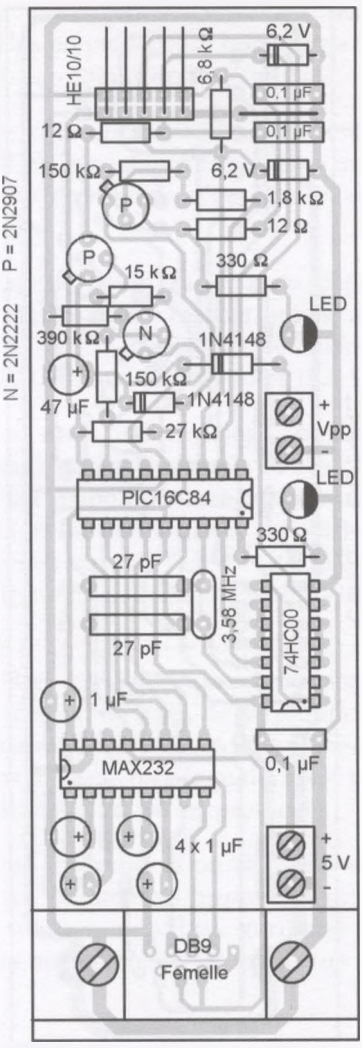



**Figure 6.4.** Plan de câblage du coupleur.

```
; ---------------------- COUP84.ASM ---------------------------------
; Coupleur de cartes à puce asynchrones avec un PIC16C84
; copyright (c)1997 Patrick GUEULLE
; fusibles de configuration : osc XT, WDT ON
; -------------------------------------------------------------
;
org 0
     goto init
org 4
init bsf 3,5  ; accès page 1
     movlw b'10000' ; RA4 en entrée
     movwf 85 ; configuration port A
     movlw b'10011000'
     movwf 86 ; configuration port B
     movlw b'11111000'
     movwf 81 ; configuration du WDT
     bcf 3,5  ; retour page 0
     movlw b'11111000' ; initialisation port B
     movwf 06
     movlw b'11010' ; initialisation port A
     movwf 05
deja btfss 6,3 ; attente absence carte
     goto err ; désalimentation carte si déjà insérée
wait clrwdt
     btfsc 6,3 ; attente présence carte
     goto wait
     btfsc 6,4 ; si port série fermé
     goto err ; désalimentation carte
     call tempo
     bcf 5,3 ; application Vcc carte
     call tempo
     bsf 6,2 ; application Vpp carte
     call tempo
     bsf 5,0 ; application horloge carte
     bcf 5,1 ; extinction LED
     bsf 5,2 ; reset carte à 1
loop btfss 6,3 ; si carte présente
     clrwdt ; reset du WDT
     btfsc 6,4 ; si port série fermé
     goto err ; désalimentation carte
     bsf 3,5 ; accès page 1
     movlw b'10000' ; RA4 en entrée, I/O carte à 1 (libre)
     movwf 85 ; configuration port A
     bcf 3,5 ; retour page 0
testio    btfsc 5,4 ; si I/O carte à 1
     goto testrs ; on lit la RS232
     bcf 6,6 ; si I/O carte à 0, on recopie 0 sur la RS 232
     goto testio
zeroca    bsf 3,5 ; accès page 1
     movlw b'00000' ; RA4 en sortie
     movwf 85 ; configuration port A
     bcf 3,5 ; retour page 0
     bcf 5,4 ; on envoie le 0 à la carte
     btfsc 6,7 ; si RS232 à 1
```

© DUNOD - La photocopie non autorisée est un délit.

```
      goto loop ; on libère I/O carte
      goto zeroca ; on prolonge le 0 carte
testrs    bsf 6,6 ; on maintient la RS232 à 1
      btfss 6,3 ; si carte présente
      clrwdt ; reset du WDT
      btfss 6,7 ; si RS232 à 0
      goto zeroca ; on envoie le 0 à la carte
      goto loop ; si RS232 à 1 on libère I/O carte
      goto loop
tempo     movlw .200 ; temporisation de 200 etu
     movwf 10
loopa     call bit
      btfss 6,3 ; si carte présente
      clrwdt ; reset du WDT
      decfsz 10,1
      goto loopa
      return
bit   movlw .28 ; etu de 104 µs
time movwf 0F
redo decfsz 0F,1
      goto redo
      return
err   goto err ; désalimentation carte par hors-temps WDT
   end
```

Le résultat de son assemblage au moyen des outils du « kit » PICSTART 16B de MICROCHIP est le fichier objet COUP84.OBJ, qui pourrait directement servir à la programmation du microcontrôleur, à condition de configurer manuellement les « fusibles » de l'oscillateur (mode XT) et du chien de garde (WDT ON).

Fichier COUP84.OBJ :

```
:020000000428D2
:10000800831610308500983086000F83081008312FE
:10001800F83086001A308500861D47286400861946
:100028001228061A47283A2085113A2006153A2040
:10003800051485100515861D6400061A47288316C1
:10004800103085008312051A3328061327288316D3
:10005800003085008312051286 1B1F282B280617DF
:10006800861D6400861F2B281F281F28C830900073
:10007800422086 1D6400900B3C2808001C308F002D
:080088008F0B442808004728F3
:00000001FF
```

Plus riche, le fichier COUP84.HEX permet de programmer le PIC16C84 au moyen du très simple programmateur décrit dans notre ouvrage *Composants électroniques programmables sur PC*, paru dans cette même collection.

La configuration des fusibles est alors automatiquement prise en charge par le logiciel de programmation, fourni sur la disquette du livre précité.

Fichier COUP84.HEX :

```
:100000000428FF3FFF3FFF3F8316103085009830E4
:100010008600F83081008312F83086001A3085009F
:10002000861D4728640086191228061A47283A2098
:1000300085113A2006153A20051485100515861DF0
:100040006400061A472883161030850083120512AB
:10005000332806132728831600308500831205 12E3
:10006000861B1F282B280617861D6400861F2B2839
:100070001F281F28C83090004220861D6400900B66
:100080003C2808001C308F008F0B442808004728AC
:10009000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F70
:1000A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F60
:1000B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F50
:1000C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F40
:1000D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F30
:1000E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F20
:1000F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F10
:10010000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFF
:10011000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FEF
:10012000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDF
:10013000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCF
:10014000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBF
:10015000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAF
:10016000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9F
:10017000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8F
:10018000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7F
:10019000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6F
:1001A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5F
:1001B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4F
:1001C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3F
:1001D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2F
:1001E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1F
:1001F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0F
:10020000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFE
:10021000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FEE
:10022000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDE
:10023000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCE
:10024000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBE
:10025000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAE
:10026000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9E
:10027000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8E
:10028000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7E
:10029000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6E
:1002A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5E
:1002B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4E
:1002C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3E
:1002D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2E
:1002E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1E
:1002F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0E
:10030000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFD
:10031000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FED
:10032000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDD
:10033000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCD
```

© DUNOD - La photocopie non autorisée est un délit.

```
:10034000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBD
:10035000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAD
:10036000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9D
:10037000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8D
:10038000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7D
:10039000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6D
:1003A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5D
:1003B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4D
:1003C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3D
:1003D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2D
:1003E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1D
:1003F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0D
:10040000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFC
:10041000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FEC
:10042000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDC
:10043000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCC
:10044000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBC
:10045000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAC
:10046000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9C
:10047000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8C
:10048000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7C
:10049000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6C
:1004A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5C
:1004B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4C
:1004C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3C
:1004D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2C
:1004E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1C
:1004F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0C
:10050000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFB
:10051000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FEB
:10052000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDB
:10053000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCB
:10054000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBB
:10055000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAB
:10056000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9B
:10057000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8B
:10058000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7B
:10059000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6B
:1005A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5B
:1005B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4B
:1005C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3B
:1005D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2B
:1005E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1B
:1005F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0B
:10060000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FFA
:10061000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FEA
:10062000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FDA
:10063000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FCA
:10064000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FBA
:10065000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FAA
:10066000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F9A
:10067000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F8A
:10068000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F7A
:10069000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F6A
```

```
:1006A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F5A
:1006B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F4A
:1006C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F3A
:1006D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F2A
:1006E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F1A
:1006F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F0A
:10070000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FF9
:10071000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FE9
:10072000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FD9
:10073000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FC9
:10074000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FB9
:10075000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3FA9
:10076000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F99
:10077000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F89
:10078000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F79
:10079000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F69
:1007A000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F59
:1007B000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F49
:1007C000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F39
:1007D000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F29
:1007E000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F19
:1007F000FF3FFF3FFF3FFF3FFF3FFF3FFF3FFF3F09
:08400000FF3FFF3FFF3FFC0
:02400E00ED3F84
:10420000FF00FF00FF00FF00FF00FF00FF00FF00B6
:10421000FF00FF00FF00FF00FF00FF00FF00FF00A6
:10422000FF00FF00FF00FF00FF00FF00FF00FF0096
:10423000FF00FF00FF00FF00FF00FF00FF00FF0086
:10424000FF00FF00FF00FF00FF00FF00FF00FF0076
:10425000FF00FF00FF00FF00FF00FF00FF00FF0066
:10426000FF00FF00FF00FF00FF00FF00FF00FF0056
:10427000FF00FF00FF00FF00FF00FF00FF00FF0046
:00000001FF
```

## LECTURE DE LA RÉPONSE AU RESET

L'essentiel de la norme ISO 7816 applicable aux cartes à puce se compose, en ce qui nous concerne, de ses trois premières parties :

– ISO 7816-1 (caractéristiques physiques des cartes) ;
– ISO 7816-2 (dimensions et positionnement des contacts) ;
– ISO 7816-3 (signaux et protocoles de transmission).

Cette troisième partie prévoit que les cartes asynchrones conformes à la norme doivent émettre spontanément un message particulier de 33 octets au maximum, dès qu'elles font l'objet d'une remise à zéro (reset).

Cette opération est réputée intervenir au moins lors de leur mise sous tension, mais peut aussi être déclenchée à volonté.

© DUNOD - La photocopie non autorisée est un délit.

L'émission de cette « réponse au reset » ou ATR (*answer to reset*) est subordonnée à la présence du signal d'horloge, et sa nature diffère selon le type de carte considéré.

Véritable « signature » de la carte, ce message contient un nombre variable d'informations dont certaines sont normalisées et décrivent ses principales caractéristiques : tension et courant de programmation, fréquence d'horloge, codage des bits de données…

La lecture de la réponse au reset permet donc de savoir, dans une certaine mesure, à quel type de carte on a affaire. C'est par ailleurs une bonne occasion pour se familiariser avec le protocole de communication utilisé, et découvrir qu'il n'est finalement pas si compliqué qu'on pourrait le croire.

Seule la norme ISO 7816-3 doit être considérée comme référence pour le décryptage de la réponse au reset d'une carte, mais nous fournirons tout de même quelques exemples de ce que l'on peut tirer d'un décodage succinct.

Le tout premier caractère de l'ATR revêt une importance particulière puisqu'il indique si la suite des échanges se fera en « convention ISO » directe ou inverse.

En convention directe, les octets se succèdent sur ISO7 avec leur bit de poids faible en premier, tandis que le 1 logique est représenté par un état « haute impédance ».

En convention inverse, le bit de poids fort est en tête et le 1 logique est codé sous la forme d'un niveau bas (0 V).

Si on note « Z » l'état « haute impédance » et « A » le niveau bas, alors le premier caractère de l'ATR (avec son bit de start et son bit de parité) se présentera comme suit :

– AZZAAAAAAZ pour les cartes à convention inverse ;
– AZZAZZZAAZ pour les cartes à convention directe.

Après conversion en hexadécimal, dans la convention applicable, cela correspond respectivement aux octets 3Fh et 3Bh.

Tout autre caractère en tête de l'ATR, ou bien l'absence pure et simple de réponse au reset, signaleraient une carte non conforme à la norme, synchrone, ou défectueuse.

```
10 REM ---- ATR.BAS ----
20 KEY OFF :CLS
30 PRINT"Lecteur de réponse au reset" :PRINT :PRINT
40 OPEN "com1 :9600,e,8,2" AS #1
50 ON ERROR GOTO 410
60 PRINT"--- INSERER UNE CARTE ASYNCHRONE DANS LE LECTEUR ---" :PRINT
70 IF LOC(1)<>0 THEN GOTO 100
80 IF INKEY$=CHR$(27) THEN END
90 GOTO 70
100 T$=TIME$ :BEEP
110 IF T$=TIME$ THEN 110
120 A$=""
130 WHILE NOT EOF(1)
140 A$=A$+INPUT$(1,#1)
150 WEND
160 CLOSE#1
170 C$=LEFT$(A$,1)
180 C=ASC(C$)
190 CLS
200 IF C=59 THEN PRINT"CARTE A CONVENTION ISO DIRECTE" :GOTO 420
210 IF C=3 THEN PRINT "CARTE A CONVENTION ISO INVERSE" :GOTO 230
220 PRINT"CARTE ASYNCHRONE ISO NON RECONNUE" :END
230 T$="":D$="":PRINT :PRINT"Réponse au reset (ATR) :" :PRINT :
240 FOR F=1 TO LEN(A$)
250 N$=MID$(A$,F,1)
260 N=ASC(N$)
270 M=255
280 IF N>127 THEN N=N-128 :M=M-1
290 IF N>63 THEN N=N-64 :M=M-2
300 IF N>31 THEN N=N-32 :M=M-4
310 IF N>15 THEN N=N-16 :M=M-8
320 IF N>7 THEN N=N-8 :M=M-16
330 IF N>3 THEN N=N-4 :M=M-32
340 IF N>1 THEN N=N-2 :M=M-64
350 IF N>0 THEN M=M-128
360 M$=HEX$(M) :D$=D$+CHR$(M)
370 IF LEN(M$)=1 THEN M$="0"+M$
380 PRINT M$;" "; :T$=T$+M$
390 NEXT F
400 GOTO 500
410 RESUME
420 T$="":D$="":PRINT :PRINT"Réponse au reset (ATR) :" :PRINT :
430 FOR F=1 TO LEN(A$)
440 N$=MID$(A$,F,1)
450 N=ASC(N$) :D$=D$+N$
460 M$=HEX$(N)
470 IF LEN(M$)=1 THEN M$="0"+M$
480 PRINT M$;" "; :T$=T$+M$
490 NEXT F
500 OPEN"atr.car" FOR OUTPUT AS #1
510 K=0
520 FOR F=1 TO LEN(D$)
530 B$=MID$(D$,F,1)
540 B=ASC(B$)
```

© DUNOD - La photocopie non autorisée est un délit.

```
550 IF(B AND 128)= 128 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
560 IF(B AND 64)= 64 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
570 IF(B AND 32)= 32 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
580 IF(B AND 16)= 16 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
590 IF(B AND 8)= 8 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
600 IF(B AND 4)= 4 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
610 IF(B AND 2)= 2 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
620 IF(B AND 1)= 1 THEN PRINT#1,"1 "; ELSE PRINT#1,"0 ";
630 K=K+1
640 IF K>3 THEN PRINT#1, : K=0
650 NEXT F
660 PRINT :PRINT :END
670 REM (c)1997 Patrick GUEULLE
```

Le logiciel ATR.BAS a été écrit dans le but d'intercepter l'ATR de toute carte asynchrone insérée dans le lecteur, de déterminer sa convention, et de construire un fichier disque (ATR.CAR) reproduisant intégralement son contenu.

Comme tous les autres programmes de pilotage de notre coupleur, il est muni d'une fonction de sécurité évitant tout risque d'application intempestive de tensions à la carte, et dont le principe est le suivant :

- tant que le programme n'est pas lancé, le coupleur ne peut appliquer aucune tension à la carte même si on l'introduit à plusieurs reprises dans le lecteur ;
- une fois le programme lancé, il faut introduire vraiment la carte dans le lecteur pour déclencher sa mise sous tension. Si une carte est déjà présente dans le lecteur lors du lancement du programme, il est nécessaire de la retirer puis de l'insérer à nouveau ;
- dès que le programme a terminé sa tâche (ou si on l'interrompt), il commande une désalimentation complète et « propre » de la carte ;
- Si la carte est « arrachée » du lecteur avant la fin des opérations, le coupleur s'efforce de la désalimenter tout de même « proprement ».

Il est important de savoir que tous les logiciels opérant en liaison directe avec le coupleur doivent impérativement être compilés en fichiers « .EXE » avant leur exécution (qui se fera ainsi directement à partir de l'invite du DOS).

En effet, le mode de fonctionnement du port série dont nous avons besoin (8 bits de données plus un bit de parité) n'est pas reconnu par l'interpréteur GWBASIC.

Tenter d'exécuter directement les « sources » BASIC déclencherait immanquablement un arrêt sur message d'erreur.

La disquette jointe à cet ouvrage contient donc les versions compilées des logiciels concernés, à commencer par ATR.EXE.

Dans le cas où certains de nos lecteurs souhaiteraient apporter des modifications de leur cru à ces programmes (ne serait-ce que pour changer de port série si COM1 : n'était pas libre), il conviendrait qu'ils se procurent un compilateur tel que TURBO-BASIC afin de recompiler les sources ainsi transformées.

Cela étant posé, dès que la carte a terminé d'émettre sa réponse au reset, le programme affiche la convention applicable et la totalité de l'ATR sous sa forme hexadécimale.

Dans le cas d'une carte bancaire française datant déjà de quelques années, le résultat pourrait être :

3F 65 25 08 31 04 6C 90 00.

En revanche, une carte de téléphone cellulaire GSM à convention directe donnerait un résultat pouvant ressembler à :

3B 7B 11 00 00 29 C1 01 05 00 1E 55 00 00 90 00.

Une DOSCARD de GEMPLUS (carte de la famille COS programmée pour pouvoir être utilisée comme une simple disquette) pourrait répondre :

3F 6C 00 00 24 A0 13 00 FF D0 CA 01 00 0C 90 00.

La figure 6.5 donne quelques éléments permettant de décrypter partiellement l'ATR, mais on se réfèrera bien sûr à la norme ISO 7816-3 pour toute étude sérieuse.

Le caractère qui suit TS (baptisé TO) est un « caractère de format » dont le rôle est double :

– Préciser lesquels des caractères TA1, TB1, TC1, et TD1 vont être transmis ensuite. Ces caractères dits « d'interface » déclarent un certain nombre de caractéristiques importantes de la carte ;

© DUNOD - La photocopie non autorisée est un délit.

– *Préciser le nombre des « caractères historiques » placés en fin de message. La signification de ces caractères n'est pas normalisée et peut donc varier d'un fabricant à l'autre. Il s'agit souvent d'un numéro ou d'une date de version, voire d'indications sur la vie de la carte depuis son émission.*

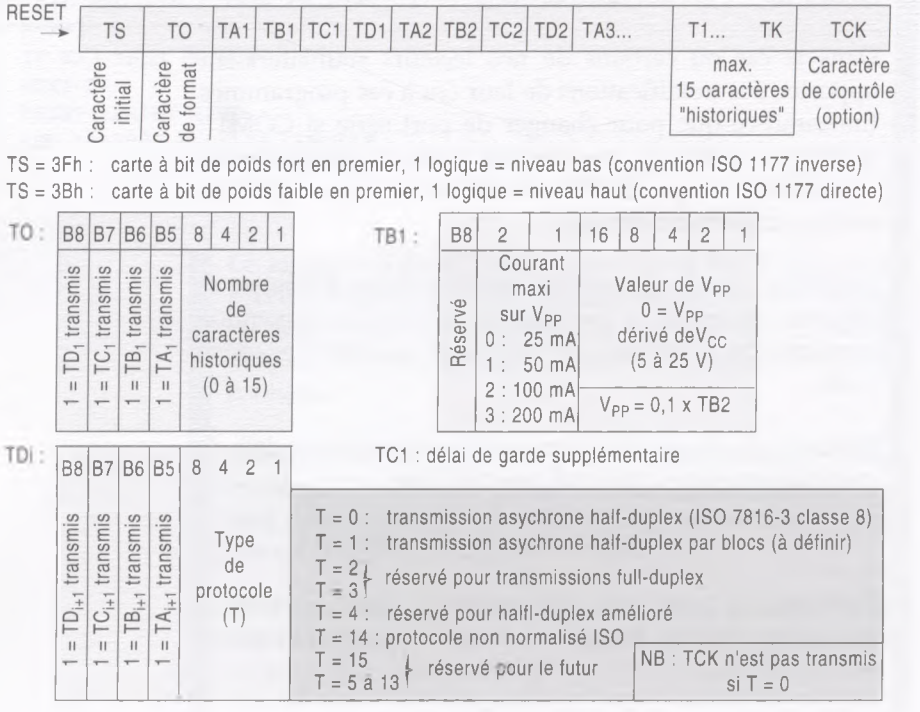



**Figure 6.5.** Éléments d'interprétation de la réponse au reset.

Bien souvent (mais pas toujours !), les deux derniers caractères historiques sont 90 00, paire d'octets qui, nous le verrons bientôt, signifie à peu près « tout va bien à bord ».

Les caractères TD, pour leur part, renseignent sur le type de protocole qui devra être appliqué pour la suite du dialogue.

TCK, enfin, est un caractère de contrôle pas toujours présent, calculé de telle sorte que le résultat d'un OU exclusif entre les caractères TO à TCK inclus soit égal à zéro.

À titre d'illustration, la figure 6.6 donne les résultats du décryptage partiel de la réponse de deux cartes courantes : une carte « DOSCARD » et une simple carte bancaire périmée depuis déjà plusieurs années.

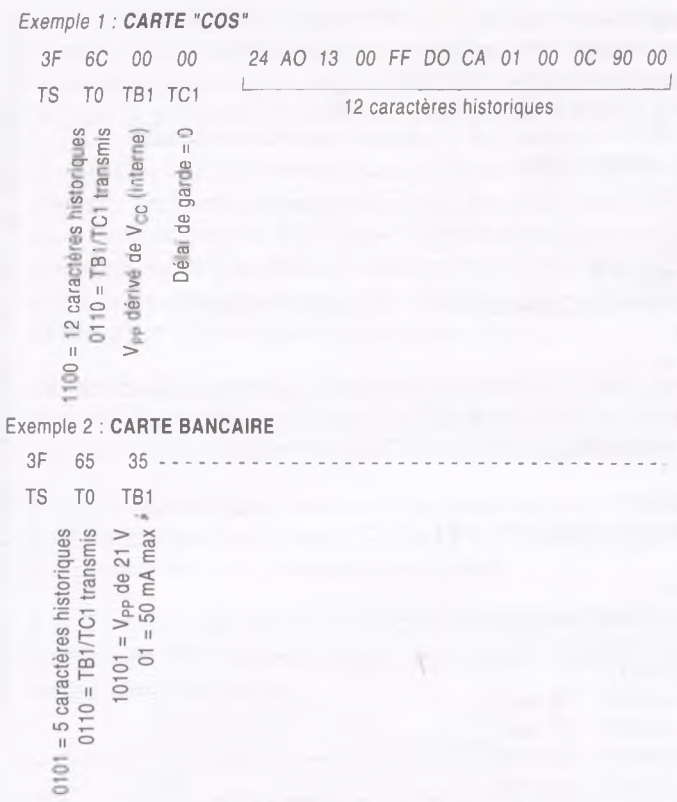



*Figure 6.6.* Exemples de décryptage de réponses au reset.

## DÉCODAGE DE LA RÉPONSE AU RESET

```
10 REM ----- DECATR.BAS -----
20 KEY OFF :CLS
30 PRINT"Décryptage de réponse au reset (ATR.CAR)"
40 OPEN "ATR.CAR" FOR INPUT AS #1
50 DIM B(LOF(1)/2)
60 F=1:PRINT :PRINT
70 WHILE NOT EOF(1)
80 INPUT#1,N :B(F)=N
90 F=F+1
100 WEND
110 V=0
120 FOR F=1 TO 8
130 IF B(F)=1 THEN V=V+2^(8-F)
140 NEXT F
150 IF V=&H3F THEN PRINT"CARTE A CONVENTION INVERSE (3Fh)" :GOTO 180
160 IF V=&H3B THEN PRINT"CARTE A CONVENTION DIRECTE (3Bh)" :GOTO 180
170 PRINT"FICHIER NON CONFORME A ISO7816" :BEEP :PRINT :PRINT :END
180 PRINT :K=0
190 FOR F=0 TO 3
200 IF B(13+F)=1 THEN K=K+2^(3-F)
210 NEXT F
220 Z=17
```

© DUNOD - La photocopie non autorisée est un délit.

```
230 IF B(12)=1 THEN GOSUB 290
240 IF B(11)=1 THEN GOSUB 350
250 IF B(10)=1 THEN GOSUB 520
260 IF B(9)=1 THEN GOSUB 580 ELSE GOSUB 680
270 PRINT :PRINT"ATR contient";K ;"caractères historiques"
280 PRINT :PRINT :PRINT :END
290 REM --- TA1 ---
300 PRINT"TA1 =";
310 FOR F=Z TO Z+7
320 PRINT B(F) ;:NEXT F
330 PRINT"   (variations possibles : horloge, bauds)"
340 Z=Z+8:RETURN
350 REM --- TB1 ---
360 PRINT"TB1 =";
370 FOR F=Z TO Z+7
380 PRINT B(F) ;:NEXT F
390 PP=0
400 FOR F=Z+3 TO Z+7
410 IF B(F)=1 THEN PP=PP+2^(Z+7-F)
420 NEXT F
430 PRINT"   (Vpp ";
440 IF PP=0 THEN PRINT"interne)" :GOTO 510
450 PRINT"=";PP ;"volts";
460 I=B(Z+2)+8*B(Z+1)
470 IF I=0 THEN PRINT" 25 mA)"
480 IF I=1 THEN PRINT" 50 mA)"
490 IF I=2 THEN PRINT" 100 mA)"
500 IF I=3 THEN PRINT" 200 mA)"
510 Z=Z+8:RETURN
520 REM --- TC1 ---
530 PRINT"TC1 =";
540 FOR F=Z TO Z+7
550 PRINT B(F) ;:NEXT F
560 PRINT"   (Délai de garde éventuel)
570 Z=Z+8:RETURN
580 REM --- TD1 ---
590 PRINT"TD1 =";
600 FOR F=Z TO Z+7
610 PRINT B(F) ;:NEXT F
620 T=0
630 FOR F=Z+4 TO Z+7
640 IF B(F)=1 THEN T=T+2^(Z+7-F)
650 NEXT F
660 PRINT"   (Protocole principal : T =";T ;")"
670 Z=Z+8:RETURN
680 PRINT :PRINT"Protocole T=0"
690 RETURN
700 REM (c)1997 Patrick GUEULLE
```

Le décodage automatisé du contenu utile de l'ATR peut être confié à un second logiciel, baptisé DECATR.BAS, qui exploite les données enregistrées dans le fichier ATR.CAR (un texte ASCII reproduisant l'ATR sous sa forme binaire).

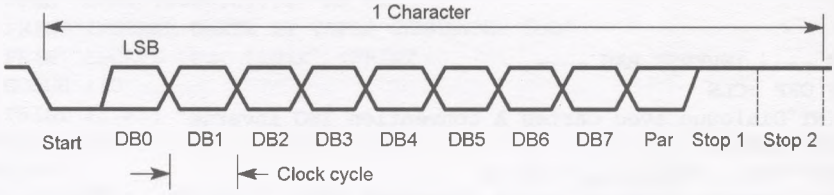
On découvrira ainsi (dans TB1) la valeur de l'éventuelle tension Vpp externe dont peut avoir besoin la carte pour les opérations nécessitant une écriture en mémoire, mais aussi le type de protocole (T) à utiliser pour la suite du dialogue.

T = 0 est le cas le plus commun, et de loin, car c'est le tout premier protocole *half-duplex* à avoir été défini avec précision dans la norme ISO 7816-3 (clause 8). C'est le protocole applicable par défaut si aucun autre n'est spécifié, et aussi celui que supportent nos logiciels. Sa particularité est de gérer la transmission octet par octet.

Certaines applications récentes commencent à faire timidement usage du protocole T=1, basé sur une transmission par blocs et donc potentiellement plus rapide.

T = 4 est réservé pour un futur protocole *half-duplex* amélioré, tandis que les valeurs T = 2 et T = 3 correspondent à des protocoles *full-duplex* encore à définir.

T = 14 rassemble pour sa part tous les protocoles non normalisés ISO, dont la figure 6.7. décrit l'un des très rares exemples connus.



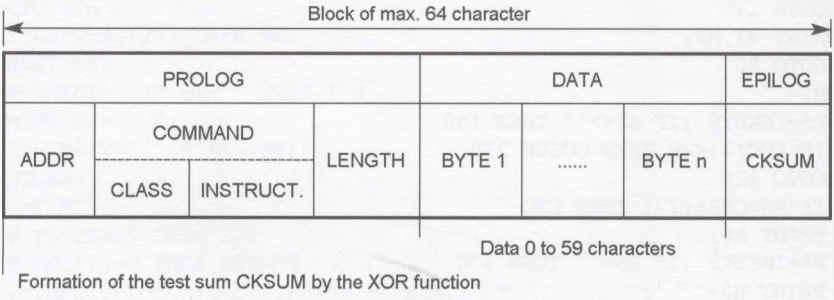




**Figure 6.7.** Exemple de protocole T = 14.

L'existence d'un caractère TA1 peut signaler que la carte réclame une fréquence d'horloge particulière, et/ou un rythme de modulation différent de 9 600 bps. En pareil cas, il conviendrait de consulter la norme ISO 7816 pour déterminer s'il y a ou non compatibilité avec les caractéristiques par défaut du lecteur.

© DUNOD - La photocopie non autorisée est un délit.

Éventuellement, un caractère TC1 peut imposer un « délai de garde », c'est-à-dire un temps d'attente à respecter entre la transmission de deux octets successifs.

## LE DIALOGUE AVEC LES CARTES

Pour pousser nos investigations au-delà du simple décodage de l'ATR, nous allons avoir besoin de logiciels permettant de nouer un véritable dialogue avec la carte insérée dans le lecteur.

INVERSE.EXE sera utilisé avec les cartes à convention inverse, et DIRECT.EXE avec celles à convention directe, le type de carte ayant été préalablement identifié avec ATR.EXE et DECATR.BAS.

*Insistons bien sur le fait que INVERSE.BAS et DIRECT.BAS ne représentent que les codes source de ces deux programmes, qui doivent obligatoirement être exécutés* dans leurs versions compilées (fichiers .EXE).

```
10 REM ---- INVERSE.BAS ----
20 KEY OFF :CLS
30 PRINT"Dialogue avec cartes à convention ISO inverse"
40 PRINT :PRINT
50 OPEN "COM1 :9600,o,8,2" AS #1
60 PRINT"INSERER CARTE ET TAPER COMMANDES ISO"
70 PRINT"ESCAPE pour finir" :PRINT
80 GOSUB 110
90 PRINT #1,M$;
100 GOTO 80
110 M$=""
120 A$=INKEY$ :IF A$<>"" THEN 150
130 IF LOC(1)<>0 THEN GOSUB 230
140 GOTO 120
150 IF A$=CHR$(27) THEN END
160 PRINT A$;
170 B$=INKEY$ :IF B$="" THEN 170
180 PRINT B$+"  ";
190 N=VAL("&H"+A$+B$)
200 GOSUB 370
210 M$=CHR$(M)
220 RETURN
230 T$=TIME$
240 IF T$=TIME$ THEN 240
250 IF LOC(1)=0 THEN RETURN
260 C$=INPUT$(LOC(1),#1): PRINT : PRINT " * ";
270 FOR K=1 TO LEN(C$)
```

```
280 N=ASC(MID$(C$,K,1))
290 GOSUB 370
300 D$=HEX$(M)+" "
310 IF LEN(D$)<3 THEN D$="0"+D$
320 PRINT D$;
330 NEXT K
340 IF LOC(1)<>0 THEN C$=INPUT$(LOC(1),#1):GOTO 270
350 PRINT "*"
360 RETURN
370 M=255
380 IF N>127 THEN N=N-128 :M=M-1
390 IF N>63 THEN N=N-64 :M=M-2
400 IF N>31 THEN N=N-32 :M=M-4
410 IF N>15 THEN N=N-16 :M=M-8
420 IF N>7 THEN N=N-8 :M=M-16
430 IF N>3 THEN N=N-4 :M=M-32
440 IF N>1 THEN N=N-2 :M=M-64
450 IF N>0 THEN M=M-128
460 RETURN
470 REM (c)1997 Patrick GUEULLE
```

```
10 REM ---- DIRECT.BAS ----
20 KEY OFF :CLS
30 PRINT"Dialogue avec cartes à convention ISO directe"
40 PRINT :PRINT
50 OPEN "COM1 :9600,e,8,2" AS #1
60 PRINT"INSERER CARTE ET TAPER COMMANDES ISO"
70 PRINT"ESCAPE pour finir" :PRINT
80 GOSUB 110
90 PRINT #1,M$;
100 GOTO 80
110 M$=""
120 A$=INKEY$ :IF A$<>"" THEN 150
130 IF LOC(1)<>0 THEN GOSUB 210
140 GOTO 120
150 IF A$=CHR$(27) THEN END
160 PRINT A$;
170 B$=INKEY$ :IF B$="" THEN 170
180 PRINT B$+"  ";
190 M$=CHR$(VAL("&H"+A$+B$))
200 RETURN
210 T$=TIME$
220 IF T$=TIME$ THEN 220
230 IF LOC(1)=0 THEN RETURN
240 C$=INPUT$(LOC(1),#1): PRINT : PRINT " * ";
250 FOR K=1 TO LEN(C$)
260 D$=HEX$(ASC(MID$(C$,K,1)))+" "
270 IF LEN(D$)<3 THEN D$="0"+D$
280 PRINT D$;
290 NEXT K
300 IF LOC(1)<>0 THEN C$=INPUT$(LOC(1),#1):GOTO 250
310 PRINT "*"
320 RETURN
330 REM (c)1997 Patrick GUEULLE
```

© EDITIONS - La photocopie non autorisée est un délit.

*Le mode opératoire est très simple : tous les octets qu'émet la carte (à commencer par son ATR) s'affichent en hexadécimal dès qu'ils sont reçus par le lecteur.*

*Les blocs d'octets provenant de la carte sont encadrés par des étoiles afin de faciliter leur repérage ultérieur (par exemple, sur des recopies d'écran).*

*À tout moment, il est possible d'envoyer des octets à la carte en les frappant tout simplement au clavier, en hexadécimal pur. La transmission se fait immédiatement, octet par octet, sans qu'il soit nécessaire d'appuyer sur une quelconque touche de validation.*

C'est en principe le lecteur qui est maître du dialogue : il doit envoyer des commandes à la carte, qui peut y répondre ou non selon les règles de sécurité qu'elle applique (son mutisme serait ici un signe de protestation).

Les commandes peuvent être « entrantes » ou « sortantes ». Une commande « entrante » sert à envoyer un bloc de données à la carte, et une commande « sortante » à lui en réclamer un.

En protocole « T=0 », toutes les commandes doivent faire usage d'un bloc de cinq octets appelé « en-tête » ou « *header* », construit selon les indications de la figure 6.8.

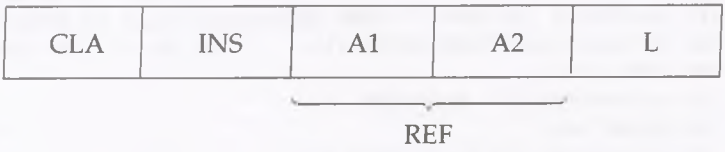



**Figure 6.8.** Structure d'une commande ISO.

Son premier octet (CLA) est ce qu'on appelle la « classe ISO » de la commande. C'est un code compris entre 00h et FEh, propre à la carte.

Ce pourra être BCh pour une carte BULL CP8 (actuelles cartes bancaires françaises) ou TB100 PHILIPS, ou A0h pour une carte de téléphone GSM.

Une valeur « par défaut » de 00h est également assez fréquente, tandis que la spécification « EMV » (Europay Mastercard Visa) préconise la valeur 80h pour certaines cartes financières de demain.

*CLASSINV.EXE et CLASSDIR.EXE permettent en principe d'effectuer, sur une carte complètement inconnue, une recherche systématique de classe ISO en essayant toutes les combinaisons possibles.*

*Rappelons qu'il s'agit respectivement des versions compilées de CLASSINV.BAS (pour les cartes à convention inverse) et de CLASSDIR.BAS (pour les cartes à convention directe) et qu'il ne faut pas chercher à exécuter les codes source suivants sous GWBASIC.*

```
10 REM ---- CLASSINV.BAS ----
20 KEY OFF :CLS
30 PRINT"Recherche classe ISO carte à convention inverse"
40 PRINT :PRINT
50 OPEN "COM1 :9600,o,8,2" AS #1
60 PRINT"INSERER LA CARTE DANS LE LECTEUR"
70 IF LOC(1)<>0 THEN 100
80 IF INKEY$=CHR$(27) THEN 570
90 GOTO 70
100 T$=TIME$ :BEEP
110 IF T$=TIME$ THEN 110
120 A$=""
130 WHILE NOT EOF(1)
140 A$=A$+INPUT$(1,#1)
150 WEND
160 IF LEFT$(A$,1) = CHR$(3) THEN 180
170 CLS :PRINT"CARTE NON RECONNUE" :GOTO 570
180 FOR R=0 TO 254
190 IF INKEY$=CHR$(27) THEN 570
200 C$=HEX$(R)
210 IF LEN(C$)=1 THEN C$="0"+C$
220 B$=C$+"B008E090"
230 CLS :PRINT C$,
240 FOR F=1 TO 9 STEP 2
250 K$=MID$(B$,F,2)
260 N$="&h"+K$
270 N=VAL(N$)
280 GOSUB 580
290 PRINT#1,CHR$(M) ;
300 FOR T=0 TO 20 :NEXT T
310 NEXT F
320 T$=TIME$
330 IF T$=TIME$ THEN 330
340 IF LOC(1)<>0 THEN 370
350 IF INKEY$=CHR$(27) THEN 570
360 GOTO 340
370 A$=INPUT$(LOC(1),#1)
380 D$=""
390 FOR F=1 TO LEN(A$)
400 N$=MID$(A$,F,1)
410 N=ASC(N$)
420 GOSUB 580
```

© DUNOD - La photocopie non autorisée est un délit.

```
430 M$=HEX$(M)
440 IF LEN(M$)=1 THEN M$="0"+M$
450 D$=D$+M$
460 NEXT F
470 IF LOC(1)<>0 THEN A$=INPUT$(LOC(1),#1):GOTO 390
480 IF LEFT$(D$,2)<>"6E" THEN 510
490 NEXT R
500 GOTO 570
510 PRINT"Classe reconnue" :PRINT :PRINT :BEEP
520 PRINT"Poursuivre recherche : ENTER"
530 PRINT"Quitter : ESCape"
540 IF INKEY$=CHR$(27) THEN 570
550 IF INKEY$=CHR$(13) THEN 490
560 GOTO 540
570 PRINT :PRINT :END
580 M=255
590 IF N>127 THEN N=N-128 :M=M-1
600 IF N>63 THEN N=N-64 :M=M-2
610 IF N>31 THEN N=N-32 :M=M-4
620 IF N>15 THEN N=N-16 :M=M-8
630 IF N>7 THEN N=N-8 :M=M-16
640 IF N>3 THEN N=N-4 :M=M-32
650 IF N>1 THEN N=N-2 :M=M-64
660 IF N>0 THEN M=M-128
670 RETURN
680 REM (c)1997 Patrick GUEULLE

10 REM ---- CLASSDIR.BAS ----
20 KEY OFF :CLS
30 PRINT"Recherche classe ISO carte à convention directe"
40 PRINT :PRINT
50 OPEN "COM1 :9600,e,8,2" AS #1
60 PRINT"INSERER LA CARTE DANS LE LECTEUR"
70 IF LOC(1)<>0 THEN 100
80 IF INKEY$=CHR$(27) THEN 550
90 GOTO 70
100 T$=TIME$ :BEEP
110 IF T$=TIME$ THEN 110
120 A$=""
130 WHILE NOT EOF(1)
140 A$=A$+INPUT$(1,#1)
150 WEND
160 IF LEFT$(A$,1) = CHR$(59) THEN 180
170 CLS :PRINT"CARTE NON RECONNUE" :GOTO 550
180 FOR R=0 TO 254
190 IF INKEY$=CHR$(27) THEN 550
200 C$=HEX$(R)
210 IF LEN(C$)=1 THEN C$="0"+C$
220 B$=C$+"B008E090"
230 CLS :PRINT C$,
240 FOR F=1 TO 9 STEP 2
250 K$=MID$(B$,F,2)
260 N$="&h"+K$
270 M=VAL(N$)
```

```
280 PRINT#1,CHR$(M) ;
290 FOR T=0 TO 20 :NEXT T
300 NEXT F
310 T$=TIME$
320 IF T$=TIME$ THEN 320
330 IF LOC(1)<>0 THEN 360
340 IF INKEY$=CHR$(27) THEN 550
350 GOTO 330
360 A$=INPUT$(LOC(1),#1)
370 D$=""
380 FOR F=1 TO LEN(A$)
390 N$=MID$(A$,F,1)
400 M=ASC(N$)
410 M$=HEX$(M)
420 IF LEN(M$)=1 THEN M$="0"+M$
430 D$=D$+M$
440 NEXT F
450 IF LOC(1)<>0 THEN A$=INPUT$(LOC(1),#1):GOTO 380
460 IF LEFT$(D$,2)<>"6E" THEN 490
470 NEXT R
480 GOTO 550
490 PRINT"Classe reconnue" :PRINT :PRINT :BEEP
500 PRINT"Poursuivre recherche : ENTER"
510 PRINT"Quitter : ESCape"
520 IF INKEY$=CHR$(27) THEN 550
530 IF INKEY$=CHR$(13) THEN 470
540 GOTO 520
550 PRINT :PRINT :END
560 REM (c)1997 Patrick GUEULLE
```

Bien entendu, il ne faudrait pas espérer pouvoir employer le même artifice pour découvrir un code confidentiel, toute carte correctement protégée se bloquant définitivement après trois tentatives malheureuses...

L'octet suivant (INS) identifie l'instruction envoyée à la carte ou « code opération » (*opcode*). Les codes opération suivants sont de grands classiques, reconnus par de nombreuses cartes asynchrones.

B0h : lecture d'octets ;
D0h : écriture d'octets ;
20h : présentation de code.

Ils permettent déjà de procéder à des manipulations intéressantes, mais il est toujours avantageux de se procurer le « dictionnaire » complet des instructions de chaque carte sur laquelle on se propose d'opérer.

© DUNOD - La photocopie non autorisée est un délit.

Voici par exemple, « en anglais dans le texte », les commandes habituellement supportées par les cartes GSM :

24h : change CHV ;
26h : disable CHV ;
28h : enable CHV ;
C0h : get response ;
32h : increase ;
04h : invalidate ;
B0h : read binary ;
B2h : read record
44h : rehabilitate ;
88h : run GSM algorithm ;
A2h : seek ;
A4h : select ;
FAh : sleep ;
F2h : status ;
2Ch : unblock CHV ;
D6h : update binary ;
CDh : update record ;
20h : verify CHV.

À défaut, il n'est nullement interdit d'expérimenter avec des opcodes « empruntés » à d'autres cartes, et de prendre note de ceux qui sont acceptés.

Les octets A1 et A2 qui suivent INS constituent ce qu'on appelle la « référence » de la commande. Ce peut être l'adresse physique d'une zone de mémoire à lire ou à écrire, le numéro d'un code ou d'une clef…

Le cinquième octet (L) précise la longueur du bloc de données associé à la commande : données qui vont être transmises à la carte si la commande est « entrante », données attendues de la carte si elle est « sortante ».

Une longueur de 00h est affectée aux commandes qui ne sont ni entrantes ni sortantes : invalidation, réhabilitation, mise « en sommeil », ratification de code…

Dès qu'elle reconnaît l'en-tête d'une commande valide, la carte répond par un « octet de procédure ». Celui-ci précède immédiatement le bloc de données renvoyé par la carte si la commande est « sortante », ou bien constitue une « invitation à transmettre » pour le lecteur si elle est « entrante ».

Dans ce dernier cas, il est évident que le lecteur devra envoyer très exactement le nombre d'octets déclaré dans l'octet L.

La plupart du temps, l'octet de procédure est identique au code opération (INS), mais il peut être égal à INS+1 pour indiquer que la carte réclame l'application d'une tension Vpp (commandes d'écriture ou de présentation de codes).

La fin du traitement de la commande est signalée par la carte, sous la forme de deux octets SW1 et SW2 (ou exceptionnellement un seul) transmis au lecteur soit en queue du bloc de donnés sortantes, soit après réception du dernier octet de données entrantes.

Si tout s'est bien passé, ce « compte-rendu » est 90 00. Une valeur différente signale un incident dont l'interprétation de SW1 et/ou SW2 permet de préciser la nature.

*Un compte-rendu commençant par 6Eh ou 6Dh indique que la commande n'est pas supportée par la carte. 6Eh* signifie que l'octet CLA ne correspond pas à la classe de la carte, tandis que 6Dh signale que INS ne correspond pas à un code opération connu.

Les autres compte-rendus commençant par 6 indiquent que la carte supporte la commande, mais que celle-ci est mal formulée : référence incorrecte pour 6Bh (par exemple, tentative de lecture à une adresse qui n'existe pas), ou longueur incorrecte pour 67h (par exemple, tentative de présentation d'un code trop long ou trop court).

En pareil cas, l'octet SW2 fournit souvent le « corrigé » de la valeur erronée, ce qui est une aubaine pour les explorateurs impénitents que devraient bientôt devenir nos lecteurs...

6Fh est pour sa part réservé aux incidents sur la nature desquels aucune précision n'est donnée.

La signification des compte-rendus commençant par 9, ainsi que des octets SW2, n'est pas imposée par la norme mais relève de chaque application, avec toutefois un certain consensus en faveur des affectations suivantes :

9010h : présentation d'un code faux (1er essai) ;
9020h : présentation d'un code faux (2e essai) ;
9040h : présentation d'un code faux (3e essai) ;
9080h : présentation d'un code faux (carte bloquée) ;
9001h : échec d'écriture en EPROM ;
9202h : échec d'écriture en EEPROM ;

© DUNOD - La photocopie non autorisée est un délit.

9802h : code secret invalide ;
9804h : mauvaise présentation de code ;
9806h : code annulé ;
9810h : condition de sécurité non satisfaite ;
9820h : code secret inactif.

Beaucoup d'opérations nécessitent, on s'en doute, la présentation de l'un ou l'autre des codes qui protègent la sécurité de la carte, et il faut savoir que la façon de procéder varie d'une famille de cartes à l'autre.

Dans le cas des cartes BULL CP8, par exemple, un code « porteur » à quatre chiffres doit être transcodé en un mot de quatre octets, selon un algorithme nullement secret. Le code 4950 doit ainsi être présenté (avec la référence 0000h) sous la forme 12543FFFh !

Une fois présenté, ce code doit encore être « ratifié » par une commande BC 40 00 00 00.

Pour ce qui est des cartes « COS » de GEMPLUS, les codes de quatre octets doivent être étendus à huit avant leur présentation. L'opération consiste à ajouter, à chaque quartet, quatre bits de poids fort qui peuvent être absolument quelconques.

Le code 45343F45h pourrait ainsi être présenté aussi bien sous la forme 04050304030F0405h que sous celle, plus commode, de 54455354434F4445h (TESTCODE en ASCII), souvent reconnue d'ailleurs par les cartes « échantillon ».

## EXEMPLES PRATIQUES

Il serait évidemment plus que présomptueux de prétendre percer tous les mystères d'une carte asynchrone totalement inconnue sans disposer d'un minimum d'informations à son sujet.

Cependant, beaucoup de renseignements peuvent assez facilement être réunis sur les applications pourtant « sensibles » que sont, par exemple, la carte bancaire et la carte FRANCE TELECOM.

*Notre ouvrage PC et cartes à puces, paru dans cette même collection,* propose ainsi un grand nombre d'expériences intéressantes à mener autour de ces cartes qui dérivent de la famille BULL CP8.

Pour l'heure, on pourra se contenter d'essayer le très simple ordre de lecture BC B0 09 E0 02 (lecture de deux octets à l'adresse 09E0h, située dans une « zone à lecture libre »).

Le résultat doit être B0 3F E5 90 00 dans le cas d'une carte bancaire, et B0 3F E2 90 00 en présence d'une carte FRANCE TELECOM (anciennement PASTEL).

On reconnaît facilement un « octet de procédure » B0, les deux octets de données 3FE5h ou 3FE2h, et le compte-rendu 9000h.

© DUNOD - La photocopie non autorisée est un délit.

| CHAPITRE | | PAGE |
|---|---|---|
| 1 | Vocabulaire et normalisation | 1 |
| 2 | Les circuits intégrés pour cartes à puce | 13 |
| 3 | La périphérie des cartes | 37 |
| 4 | Mise en œuvre des cartes synchrones | 67 |
| 5 | Applications pratiques des cartes synchrones | 105 |
| 6 | Introduction aux cartes asynchrones | 125 |


# 7 LE CÉDÉROM DU LIVRE

Le cédérom joint à cet ouvrage remplace avantageusement la disquette qui accompagnait ses précédentes éditions.

On retrouvera ainsi le contenu intégral de cette disquette dans le répertoire CARPUCE, qui rassemble les fichiers suivants :

| | | |
|---|---|---|
| ATR | BAS | 2 052 |
| CLASSDIR | BAS | 1 393 |
| CLASSINV | BAS | 1 686 |
| DECATR | BAS | 1 850 |
| DIRECT | BAS | 860 |
| INVERSE | BAS | 1 173 |
| MANIPT1G | BAS | 1 304 |
| MANIPEUR | BAS | 1 301 |
| GPM256 | BAS | 4 220 |
| MANIPT2G | BAS | 1 258 |
| GPM416 | BAS | 1 240 |
| GPM896 | BAS | 1 240 |
| LECTI2C | BAS | 1 921 |
| PROGRI2C | BAS | 1 884 |
| CRED50 | BAS | 683 |
| CRED120 | BAS | 684 |
| SERRURE | BAS | 1 125 |
| CARTOROM | BAS | 447 |
| ROMTOCAR | BAS | 817 |
| ROMTOBIN | BAS | 426 |
| BINTOROM | BAS | 394 |
| DEC416 | BAS | 1 824 |
| DEC896 | BAS | 2 224 |
| ATR | EXE | 40 691 |
| CLASSDIR | EXE | 39 136 |
| CLASSINV | EXE | 39 584 |
| DECATR | EXE | 42 518 |
| DIRECT | EXE | 38 320 |
| INVERSE | EXE | 38 768 |
| COUP84 | ASM | 2 722 |
| COUP84 | OBJ | 420 |
| COUP84 | HEX | 6 179 |
| 50 | HEX | 1 198 |
| 120 | HEX | 1 582 |
| 50 | ROM | 1 547 |
| 120 | ROM | 2 178 |
| COUP | PCB | 3 242 |
| FD2000 | PCB | 890 |
| AFNOR | PCB | 884 |
| 10TO21 | PCB | 534 |
| BITT | PCB | 1 225 |
| 12TO21 | PCB | 877 |
| CARTEISO | PCB | 841 |
| CLACPUCE | PCB | 1 341 |
| DEVCARTE | PCB | 2 366 |
| DIPCARTE | PCB | 1 137 |

```
NANOLECT    PCB        1 074
SERRURE     PCB        3 612
SIMCARDA    PCB          713
SIMLOCK     PCB          618
256         PCB        1 273
DIPISO      PCB        1 183
CREDIT      PCB        3 006
MATRIX      PCB          682

            54 fichier(s)     312 347 octets
```

Il s'agit notamment de tous les programmes passés en revue au fil des chapitres.

Ils sont écrits en GWBASIC, langage longtemps fourni d'origine avec la plupart des compatibles PC, auquel on peut maintenant substituer QBASIC (version interprétée de QUICK BASIC, livrée notamment avec Windows 95).

Certains logiciels du chapitre 6, qui ne doivent pas être utilisés sous cette forme ne constituant que leur « code source », sont également fournis sous la forme d'exécutables compilés (ATR.EXE, INVERSE.EXE, DIRECT.EXE, CLASSINV.EXE, CLASSDIR.EXE). On les lancera directement à partir de l'invite du DOS, ou dans une fenêtre « MS-DOS » de WINDOWS 95 ou supérieur.

Par souci de commodité, nous avons également prévu une version compilée de DECATR.BAS (DECATR.EXE), qui épargnera de fréquents allers-retours entre le DOS et l'interpréteur BASIC.

Quatre petits utilitaires BASIC ont été ajoutés pour faciliter les éventuelles conversions entre les formats de fichiers couramment utilisés dans le courant de cet ouvrage : CARTOROM.BAS, ROMTOCAR.BAS, ROMTOBIN.BAS, et BINTOROM.BAS.

Le logiciel destiné au PIC16C84 du coupleur décrit au chapitre 6 est fourni sous la forme d'un code source (COUP84.ASM) et d'un code objet directement compatible avec les programmateurs courants (COUP84.OBJ et COUP84.HEX).

Les fichiers de programmation de l'EPROM du testeur de télécartes décrit au chapitre 5 sont, pour leur part, offerts sous deux formats distincts : « free format decimal » (50.ROM et 120.ROM), et « INTEL HEX » (50.HEX et 120.HEX).

© DUNOD - La photocopie non autorisée est un délit.

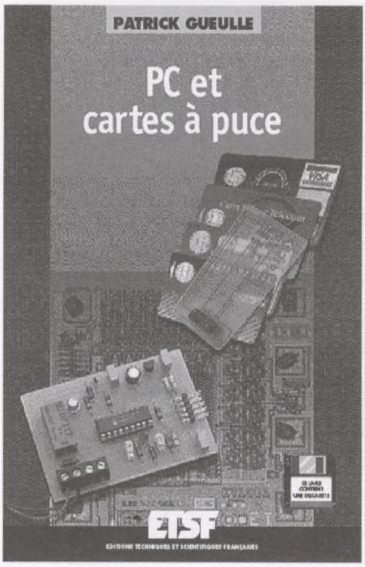
Le disque contient enfin les tracés de tous les circuits imprimés reproduits dans le livre, sous la forme des fichiers «.PCB » produits par le logiciel BOARDMAKER.

Une version limitée de BOARDMAKER 1, très suffisante pour modifier et réimprimer ces tracés (sur une simple imprimante matricielle), est disponible dans le répertoire « BMAKER ». Notons qu'une présentation détaillée de ce puissant outil figure dans nos ouvrages *Circuits imprimés – conception et réalisation* et *Logiciels PC pour l'électronique*, tous deux parus dans cette même collection.

Le présent cédérom contient également, dans son répertoire PCPUCE, tous les fichiers de la disquette d'accompagnement de notre ouvrage *PC et cartes à puce*.

Suite logique du livre que vous avez entre les mains, il explique comment aller encore bien plus loin dans la voie que nous venons de tracer, en mettant tout particulièrement l'accent sur les cartes « asynchrones », notamment bancaires...

Le répertoire ACROBAT réunit, enfin, différentes versions du logiciel gratuit Acrobat Reader, nécessaire pour visualiser ou imprimer les documents fournis sous la forme d'un fichier «.PDF ».




- Les microprocesseurs des cartes à puces
- À la découverte de la carte bancaire
- Un mini-système de développement
- Les télécartes ou cartes synchrones

Code 045205

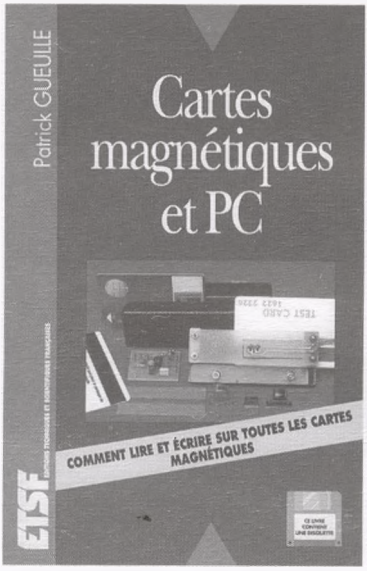



- Le système GSM
- Les réseaux
- Le poste mobile
- Une boîte à outils GSM
- La carte SIM

Code 045184

EN VENTE CHEZ VOTRE LIBRAIRE HABITUEL

DUNOD

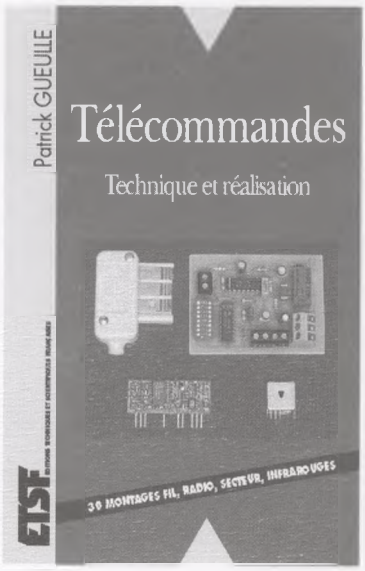



- Supports magnétiques de données
- Cartes magnétiques normalisées
- Lecture et vérification
- Copie, encodage, effacement

Code 023984

- Techniques de télécommande
- Quelques montages de base
- Télécommande par infrarouges
- Télécommandes par radio
- Télécommandes « secteur »
- Télécommandes par téléphone
- Télécommandes sur voies « audios »
- Les nouvelles techniques

Code 044637




EN VENTE CHEZ VOTRE LIBRAIRE HABITUEL

DUNOD

045736 - (I) - (3) - OSB 100° - IMN - GDE

Imprimerie Nouvelle
45800 Saint-Jean-de-Braye
N° d'imprimeur : 2001 03 0244
Dépôt légal : mai 2001

045736 - (I) - (3) - OSB 100° - IMN - GDE

Imprimerie Nouvelle
45800 Saint-Jean-de-Braye
N° d'imprimeur : 2001 03 0244
Dépôt légal : mai 2001

PATRICK GUEULLE

# Cartes à puce




ETSF
EDITIONS TECHNIQUES ET SCIENTIFIQUES FRANÇAISES

# Cartes à puce

## INITIATION ET APPLICATIONS

*Cartes à puce* va tout simplement vous permettre d'apprendre à lire et à écrire dans la plupart des cartes à puce, avec l'aide d'un micro-ordinateur compatible PC ; le cédérom inclus dans le livre contient tous les logiciels et autres fichiers nécessaires.

Vous commencerez par réaliser une « boîte à outils » complète : lecteurs, encodeurs, connecteurs, « fausses cartes » en circuit imprimé, alimentations spéciales, etc.

Après une découverte progressive des possibilités de ces composants fascinants et d'une bonne partie de leurs petits secrets, vous pourrez monter vos propres applications pratiques : testeur de poche pour télécartes, serrures de sûreté à carte, et même destructeur de cartes « compromettantes ».

| CONFIGURATION | MINIMALE | RECOMMANDÉE |
|---|---|---|
| Processeur<br>Vitesse | 8086<br>8 MHz | 386 SX<br>25 MHz |
| RAM/Disque dur | 640 Ko / – | 8 Mo / 100 Mo ou + |
| Système<br>• MS-DOS<br>• Windows | <br>3.30<br>– | <br>3.30 ou supérieur<br>Windows 3.X ou 95 |
| Carte vidéo/moniteur | CGA/14" | VGA/14" ou + |
| Lecteur de CD-ROM | 2x | > 12x |
| Périphériques<br>• Imprimante<br>• Programmateur | <br>Matricielle 9 aiguilles<br>– | <br>Jet d'encre<br>PIC 16C84 |
| Langages programmation | GWBASIC | GWBASIC, TURBOBASIC<br>Assembleur PIC 16C84 |
| Logiciels installés | – | Acrobat Reader 3.0 |

9 782100 057368

http://www.dunod.com

Code 045736

ISBN 2 10 005736 7