



PC

Programmation

Système

*R*essources
D'EXPERTS

Frank van Gilluwe

Des codes sources, de nombreux
utilitaires et des outils à télécharger
à partir de www.ssm.fr

- Architecture PC : contrôleurs disque, claviers, vidéo, ports série, etc.
- Microprocesseurs Pentium, Cyrix, AMD, NexGen
- Détection du matériel et du système
- Fonctions BIOS et zones de données fixes
- Mémoire CMOS et horloge temps réel
- Contrôle des interruptions et services DMA




CAMPUSPRESS

Chapitre 1. Introduction	1	Les instructions non documentées	66
Sources d'information	3	Récapitulatif des instructions non documentées	67
Types de systèmes	4	Description des instructions non documentées	68
Diagramme système du programmeur	5	Mode interruption	74
Chapitre 2. La partie non documentée du PC	9	Mode ICE (In-Circuit-Emulator)	74
Trouver les documents source originaux	10	Mode enregistrement des registres	75
Ce travail a-t-il déjà été réalisé ?	11	Description du port d'E/S du processeur Cyrix	77
Etudier comment ce travail a déjà été réalisé	11	LOADALL sur le 80286	91
Désassemblage	12	LOADALL sur le 386/486	92
Options de désassemblage	12	Utilisation de LOADALL	96
Pourquoi est-il si difficile de désassembler ?	13	Utilisation de LOADALL pour la pagination en mode réel	98
Désassemblage commenté	14	Reprendre depuis le mode gestion du système	98
Désassemblage du BIOS	25	Récapitulation des registres	107
IOSPY : le superviseur de port d'E/S résident	28	Description détaillée des registres	109
UNPC : l'observateur de port d'E/S	31	Espace d'adressage caché	131
Chapitre 3. L'unité centrale et les instructions non documentées	33	Les modes suspendre et reprendre	132
Les entrées/sorties	34	386SXLC, 386DXLC, 486DXLC d'AMD	134
Adressage des E/S	35	486SLC, 486DLC de TI et Cyrix	135
Instructions d'E/S	36	486SLC/e de Cyrix et TI	135
Entrée à partir du port	36	6x86 de Cyrix	137
Exemples de code	37	386SLC et 486SLC d'IBM	137
Chaîne en entrée	37	80386SL, 80486SL, Pentium, Pentium Pro d'Intel, 5k86 d'AMD	138
Exemples de code	38	ICE (In-Circuit-Emulation)	142
Sortie vers le port	39	Réinitialisation du processeur	142
Exemples de code	39	Comment réinitialiser le processeur	143
Chaîne en sortie	39	Prendre le contrôle avant la réinitialisation	145
Exemples de code	41	Chapitre 4. Détection du matériel et du système	147
Synchronisation des instructions	42	La partie facile	148
Problèmes de synchronisation	43	Détection du système	151
Exemple de code 3.1 : Délai d'E/S	44	Exemple de code 4.1 : Détection du système	151
Les modes d'UC liés aux E/S	46	Informations relatives à l'unité centrale	161
Accès matériel via C et C++	47	Exemple de code 4.2 : Identification du processeur	163
Les registres	48		
Les interruptions	49		
Contrôle des interruptions	50		
Les ports d'E/S	50		
Exemples de code en assembleur et en C	51		
Les processeurs	54		

Exemple de code 4.3 : Identification du processeur simple	172	Méthode n°1 : fournir la mémoire RAM sur la carte	224
Exemple de code 4.4 : Détection du processeur virgule flottante	174	Méthode n°2 : récupérer la RAM dans la partie supérieure de la zone mémoire principale du DOS	225
Exemple de code 4.5 : Emplacement du processeur virgule flottante	176	Méthode n°3 : utiliser quelques octets dans le BIOS ou les zones de données d'interruption	226
Exemple de code 4.6 : Détection de la taille de la file d'attente de préextraction (prefetch)	178	Méthode n°4 : utiliser la mémoire accessible depuis les E/S	226
Exemple de code 4.7 : Détection de la version du processeur	184	Méthode n°5 : utiliser un pilote pour réserver la mémoire RAM nécessaire	227
Exemple de code 4.8 : Détection du mode du processeur	192	Méthode n°6 : utiliser l'accès direct à la mémoire (DMA)	227
Exemple de code 4.9 : Identification du vendeur	193	Méthode n°7 : utiliser des adresses de RAM très hautes dans la mémoire ...	228
Exemple de code 4.10 : Mesure de la vitesse du processeur	197	Méthode n°8 : la mémoire RAM est-elle réellement nécessaire ?	228
Exemple de code 4.11 : Détection de la mémoire cache du processeur	201	Sélection des numéros de ports d'E/S	229
Exemple de code 4.12 : Analyse de la taille de la mémoire cache données du processeur ...	203	Multiplicité des ports d'E/S	229
Exemple de code 4.13 : Tests des instructions non documentées	207	Escamotage des mémoires ROM et RAM ..	232
Exemple de code 4.14 : Recherche de nouvelles instructions non documentées ...	215	Connecteurs et cavaliers	232
Exemple de code 4.15 : Recherche et affichage des registres spécifiques au modèle	216	Plug and Play	233
Exemple de code 4.16 : Affichage du compteur de l'horodateur	218	Chapitre 6. Les données du BIOS et autres zones de données fixes	235
Chapitre 5. Le développement des cartes ..	219	Zone de données du BIOS	236
Initialisation et en-tête de la ROM	220	Description détaillée de la zone des données du BIOS	239
Analyse d'une ROM MCA	221	Zone de données du BIOS étendue	277
Définition de l'adresse de début et de la taille de la ROM	221	Résumé de l'utilisation de la zone de données étendue du BIOS	278
Code de la ROM	223	Description détaillée de la zone de données étendue du BIOS	279
Règle 1 : éviter les écritures dans la ROM	223	Mémoire vidéo	286
Règle 2 : éviter les segments fixes dans la ROM	223	Les mémoires ROM de carte et la mémoire UMB	287
Comment obtenir la mémoire RAM nécessaire	224	Chapitre 7. Table des vecteurs d'interruption	289
		Descriptions des données et des vecteurs d'interruption	294

Chapitre 8. Le système clavier	323	Description détaillée des ports	380
Introduction	324	Résumé des commandes	381
Fonctionnement de base	325	Description détaillée des commandes	382
Traitement typique d'une touche sur un système AT	326	Résumé des commandes	393
Traitement typique d'une touche sur un système PC/XT	327	Description détaillée des commandes	394
Communications avec le contrôleur	328	Chapitre 9. Le système vidéo	407
Transmissions clavier vers carte mère	329	Introduction	408
Transmission clavier vers carte mère sur le système AT	331	Standards des cartes vidéo	409
Service BIOS du clavier – niveau bas	331	CGA – Color Graphics Adapter	409
Services BIOS du clavier – niveau intermédiaire	334	MDA – Monochrome Display Adapter ..	409
Zones de données du BIOS pour le clavier	346	HGA – Hercules Graphics Adapter	410
Les touches d'accès rapide et l'accès aux touches indéfinies	349	PGA – Professional Graphics Adapter ...	410
Codes de balayage	350	EGA – Enhanced Graphics Adapter	410
Claviers non américains	357	MCGA	410
Accès A20 à la mémoire étendue	360	VGA – Video Graphics Array	411
Adressage au-delà du premier segment 1 Mo	360	SVGA – Super VGA	411
Porte A20	360	XGA – Extended Graphics Adapter	411
Etat de la porte A20	361	JEGA, AX-VGA – Les cartes japonaises ..	412
Exemple de code 8.1 : Lecture de l'état courant de la porte A20	362	Convention des noms de cartes	412
Contrôle de l'état de la porte A20	363	Services BIOS	413
Exemple de code 8.2 : Contrôle de A20	363	Description détaillée des sous-fonctions de la fonction 10h	429
Avertissements	364	Autres interruptions relatives au système vidéo	499
Connexion et transmissions du clavier	365	Spécification de l'interface d'écran repositionnée (RSIS)	499
Exemple de code 8.3 : Accès au contrôleur ..	366	Considérations matérielles et logicielles ..	500
Exemple de code 8.4 : Réinitialisation du système	370	Comment obtenir la conformité RSIS ...	500
Exemple de code 8.5 : Affichage des codes de balayage et Kscan	370	L'appel de fonction RSIS	501
Exemple de code 8.6 : Programme résident d'échange de touches	375	Considérations particulières	501
Exemple de code 8.7 : Analyse de fonctionnalité	378	Exemples de code 9.1 : Lecture de l'adresse d'écran repositionné, code C	502
Résumé des ports	380	Exemple de code 9.2 : Lecture de l'adresse d'écran repositionné, code assembleur	503
Confusion à propos des commandes	380	Aucun changement du mode vidéo (type texte)	503
		Programmes qui modifient les modes vidéo (texte et graphique)	504

Exemple de code 9.3 : Ecriture en mémoire vidéo	506	Chapitre 11. Les systèmes disque dur	591
Fonction de mise à jour de l'écran pour DOS/V	507	Introduction	592
Pages multiples	507	Comment connaître la taille réelle d'un disque dur ?	595
Le support RSIS et les environnements	508	Standards d'interface et contrôleurs	596
Les responsabilités	508	Fonctionnement du lecteur	599
Les environnements RSIS	508	Lecteurs de type ST-506	599
Les environnements utilisant RSIS	509	Lecteurs utilisés avec les standards IDE, EIDE, ESDI et SCSI	600
Exemple de code 9.4 : Détection de la carte vidéo	509	Lecteurs IDE à grande capacité	600
Résumé des ports	514	Table de paramètres du disque	601
Description détaillée des ports d'E/S vidéo non documentés	517	Table du type de lecteur	604
Chapitre 10. Système disquette	521	Initialisation du BIOS	607
Introduction	522	BIOS du disque dur	608
Caractéristiques du lecteur de disquettes ...	524	Remarques sur les fonctions BIOS	612
Format des données sur la disquette	524	Détail des sous-fonctions	637
Table des paramètres de disquette	525	Détails sur les sous-fonctions	652
Initialisation du BIOS	529	Données du BIOS disque	662
Services BIOS de disquette	530	Envoyer des commandes au contrôleur de disque	663
Données BIOS pour la disquette	541	Fonctionnement de la lecture de secteur	663
Parties communes du contrôleur de disquettes	545	Informations générales	664
Envoi de commandes vers le contrôleur de disquettes	546	Détail des commandes du port 320h	718
Avertissements	547	Détail des commandes du port 3510h	732
Les limites du secteur BIOS	547	Chapitre 12. Les ports série	751
Problème du transfert de données au-delà de la limite de 64 Ko	547	Introduction	752
Problèmes de synchronisation du logiciel	548	Initialisation du BIOS	754
Exemple de code 10.1 : Détection du lecteur de disquettes	549	Services série du BIOS	755
Résumé des ports	551	La trame série	762
Description détaillée des ports	552	Les signaux contrôle/modem	763
Etats et paramètres de commandes standards	561	Séquence d'événements — Transmission série	764
Résumé des commandes du port 3F5h ..	565	Séquence d'événements — Réception série .	765
Description détaillée des commandes ...	566	Fonctionnement du bouclage (loopback) ...	765
		Débits en bauds	766
		Contrôle d'interruption	767
		Mode FIFO	770
		Zones de données du BIOS	771
		Débogage	773
		Récapitulatif du composant UART	774

Ressources d'experts

Connecteur du port série	775	Services BIOS d'imprimante	931
Avertissements	776	Impression d'écran	934
Exemple de code 12.1 : Débit lent pour le débogage	778	Zones de données du BIOS	935
Exemple de code 12.2 : Détecteur de port série	779	Synchronisation du port parallèle	938
Exemple de code 12.3 : Analyseur de débit maximal en bauds	784	Connecteur du port parallèle	939
Récapitulatif des ports	795	Port parallèle Fast	940
Détails des registres UART	797	Avertissements	941
Chapitre 13. Fonctions système	811	Exemple de code 14.1 : Imprimer uniquement en code ASCII	942
Services BIOS	812	Exemple de code 14.2 : Changer d'imprimante	944
Récapitulatif des ports	876	Exemple de code 14.3 : Détection du support du mode étendu	945
Détails sur les ports	878	Récapitulatif des ports	948
Récapitulatif des registres (Contrôleur DRAM EISA 82359 d'Intel, registres généraux)	880	Détail des ports	948
Récapitulatif des registres (Contrôleur DRAM EISA 82359 d'Intel, registres EMS)	882	Chapitre 15. Mémoire CMOS et horloge temps réel	955
Récapitulatif des registres (support E/S local EISA 82351 d'Intel)	882	Introduction	956
Récapitulatif des registres (Périphérique de gestion de l'énergie 82347 d'Intel) ...	883	Informations générales sur la RTC (horloge temps réel)	956
Codes POST du BIOS XT IBM fréquemment utilisés	885	Service BIOS de la RTC	957
Codes POST du BIOS AMI fréquemment utilisés	891	Différences du système EISA	964
Codes POST du BIOS AWARD fréquemment utilisés	893	Informations sur le type ASCII	966
Codes POST du BIOS AT IBM fréquemment utilisés	897	Sous-fonction 0, portion secondaire de la mémoire tampon	968
Codes POST du BIOS ISA/EISA Phoenix fréquemment utilisés	900	Sous-fonction 1, portion secondaire de la mémoire tampon	969
Codes POST du BIOS MCA IBM fréquemment utilisés	920	Sous-fonction 2, portion secondaire de la mémoire tampon	969
Chapitre 14. Les ports parallèle et l'impression d'écran	927	Sous-fonction 3, portion secondaire de la mémoire tampon	970
Introduction	928	Zones de données système	974
Initialisation du BIOS	929	Registres de la CMOS étendue	974
Un système peut-il avoir un quatrième port parallèle ?	930	Mémoire CMOS étendue sur AT	974
		Mémoire CMOS étendue sur MCA	974
		Mémoire CMOS étendue sur EISA	974
		Avertissement	975
		Interruptions	975
		Total de contrôle CMOS	975
		Registres d'horloge	976
		Exemple de code 15.1 : Lire la CMOS	976

Exemple de code 15.2 : Ecrire dans la CMOS	977	Timer 5 — Contrôle de vitesse de l'unité centrale (EISA uniquement)	1068
Exemple de code 15.3 : Afficher la CMOS AT	977	Installation du timer et fonctionnement	1068
Exemple de code 15.4 : Afficher la CMOS MCA étendue	979	Utilisations types	1069
Exemple de code 15.5 : Afficher la CMOS EISA étendue	980	Accès	1070
Récapitulatif des ports	982	Avertissements	1070
Détails sur les ports	982	Exemple de code 16.1 : Synchronisation précise d'événement	1070
Récapitulatif des registres — Heure et date	983	Exemple de code 16.2 : Mode timer 0	1073
Récapitulatif des registres — Mémoire CMOS	984	Exemple de code 16.3 : Gestionnaire d'interruptions rapides	1076
Détails sur les registres	986	Récapitulatif des ports	1080
Mémoire CMOS	993	Détails des ports	1081
Détails des registres	1050	Récapitulatif des commandes	1084
Chapitre 16. Les timers système	1057	Détails des commandes	1085
Introduction	1058	Récapitulatif des commandes	1094
Modes de fonctionnement	1059	Détails des commandes	1094
Mode 0 : Délai d'attente unique	1060	Récapitulatif des commandes	1097
Mode 1 : Durée fixe, déclenchements multiples	1060	Détails des commandes	1097
Mode 2 : Générateur de débit	1061	Chapitre 17. Contrôle des interruptions et NMI	1105
Mode 3 : Onde carrée	1062	Introduction	1106
Mode 4 : Stroboscope déclenché par voie logicielle	1063	Description du processus d'interruption	1107
Mode 5 : Stroboscope redéclenchable par voie matérielle	1063	Contrôle par le front ou par la position	1108
Opérations communes — Tous modes ..	1064	Déclenchement par le front	1109
Timer 0 — Synchronisation du système ...	1065	Déclenchement par la position	1109
Timer 1 — Rafraîchissement DRAM	1066	NMI (Non-Maskable Interrupt)	1110
Timer 2 — Utilisation générique et haut-parleur	1066	Coprocasseur à virgule flottante et NMI ...	1110
Timer 3 — Timer de surveillance (watchdog) (MCA uniquement)	1066	Particularités des systèmes MCA	1111
Timer 3 — Timer de surveillance (watchdog) (EISA uniquement)	1067	Particularités des systèmes EISA	1112
Timer 4 — Non mis en œuvre (EISA uniquement)	1068	Particularités des systèmes PCI	1112
		Utilisations types	1112
		Zones de données des interruptions	1115
		Avertissements	1115
		Interférences	1115
		Niveaux de priorité des interruptions ...	1116
		COM 2, IRQ 3	1116
		Chevauchements d'UC et IRQ 5	1116
		Exemple de code 17.1 : Redirection IRQ ...	1118
		Récapitulatif des ports	1120

Détails des ports	1121	VDS (Services DMA virtuels)	1159
Récapitulatif des commandes	1124	Utilisations types	1161
Détails des commandes	1125	Zone de données du BIOS DMA	1161
Récapitulatif des commandes	1135	Avertissements	1162
Détails des commandes	1136	Exemple de code 18.1 : Installation du transfert DMA	1163
Chapitre 18. Services DMA et actualisation de la DRAM	1145	Récapitulatif des ports	1164
Introduction	1146	Détails des ports	1167
Mise au point	1149	Récapitulatif des commandes étendues ..	1176
Transfert type de la mémoire à l'E/S	1149	Détails des commandes étendues	1177
Transferts DMA de mémoire à mémoire ...	1151	Annexe A. Sur le site Web	1205
Modes de fonctionnement	1152	Programmes	1206
Auto-initialisation	1152	Programmes exécutables	1206
Mode de transfert simple	1152	Sous-routines	1207
Mode de transfert par bloc	1152	Explications détaillées des programmes exécutables	1208
Mode de transfert sur demande	1152	Annexe B. Glossaire	1213
Mode mise en cascade	1153	Abréviations générales	1214
Particularités des systèmes MCA	1153	Références des composants et fonctions courantes	1218
Particularités des systèmes EISA	1154	Index	1221
Modes de synchronisation de cycle	1155		
Transferts FIFO sur EISA	1157		
Transferts chaînés sur EISA	1158		



Le guide du programmeur sur les E/S, les microprocesseurs et les zones de mémoire fixes

- Les réponses aux problèmes les plus complexes
- L'optimisation du temps d'exécution des programmes
- Les fonctions BIOS et instructions des microprocesseurs non documentées

TABLE DES MATIÈRES

- | | |
|--|--|
| • La partie non documentée du PC | • Les systèmes disque dur |
| • L'unité centrale et les instructions non documentées | • Les ports série |
| • La détection du matériel et du système | • Les fonctions système |
| • Le développement des cartes | • Les ports parallèle et l'impression d'écran |
| • Les données du BIOS et autres zones de données fixes | • La mémoire CMOS et l'horloge temps réel |
| • La table des vecteurs d'interruption | • Les timers système |
| • Le système clavier | • Le contrôle des interruptions et NMI |
| • Le système vidéo | • Les services DMA et l'actualisation de la DRAM |
| • Le système disquette | |

Cet ouvrage dévoile des caractéristiques du matériel PC encore jamais publiées. L'architecture du PC y est décortiquée de manière systématique, et les instructions non documentées des principaux microprocesseurs traitées de manière exhaustive. Les principaux sous-systèmes du PC sont abordés dans le détail et d'importantes sections de référence montrent et expliquent les fonctions du BIOS, qu'elles soient ou non documentées. De nombreux exemples de codes assembleurs permettent de mettre en pratique les points abordés.

En téléchargement à partir de www.ssm.fr :

- Des outils d'analyse et de diagnostic, des routines de détection de matériel, des routines de détection de l'unité centrale, un programme de détection des registres, et des utilitaires permettant d'accéder à la mémoire CMOS, au contrôleur de clavier, ainsi qu'à d'autres sous-systèmes.
- Le code source documenté complet des utilitaires.


CAMPUSPRESS

CAMPUSPRESS FRANCE
19, rue Michel le Comte
75003 Paris
Tél. : 01 44 54 51 10
Fax : 01 48 04 53 61
Web : <http://www.ssm.fr>

ISBN : 2-7440-0559-2

0559 0199 369 FF



Niveau

Expert

Catégorie : Matériel
et Programmation
Titre original :
The Undocumented PC