

## **Rozszerzenia architektury x86 w procesorach firmy INTEL**

Architektura procesorów rodziny x86 ewoluuje od czasów powstania pierwszego układu, który ją zapoczątkował. Procesor 8086 pojawił się na rynku w 1978 roku. Jego model programowy przejawiał silny wpływ poprzednich (8 bitowych) konstrukcji firmy INTEL.

Rozszerzenia wprowadzone w kolejnych generacjach x86 (procesory 286 i 386) dostarczyły podstawowych mechanizmów potrzebnych do realizacji oraz efektywnej implementacji współczesnych systemów operacyjnych. Są to przede wszystkim tryb chroniony oraz stronicowanie.

W procesorach 486 oraz następnych INTEL (a także inni producenci) skupił się na modyfikacji mikroarchitektury celem zwiększenia mocy obliczeniowej tych układów. Nie zabrakło jednak nowych mechanizmów i rozszerzeń modelu programowego pojawiających się w kolejnych generacjach procesorów. Zostaną one krótko opisane w niniejszym dokumencie.

Architektura 486 różni się od 386 w nieznaczny sposób. Pojawiły się nowe rejestry testowe (TR3, TR4, TR5), kilka rozkazów, wbudowano koprocesor i pamięć podręczną (cache) pierwszego poziomu oraz dodano pewne mechanizmy (opisane dalej).

Nowe rozkazy (BSWAP, XADD, CMPXCHG, INVLPG, INVD, WBINVD) dotyczą zmiany kolejności bajtów w dwusłowie (konwersja formatów little-endian i big-endian), funkcji z zamianą argumentów, unieważnienia zawartości bufora TLB oraz pamięci cache.

Wbudowany koprocesor jest zgodny z układami 8087, 287 i 387. Jednak fakt jego zintegrowania uprościł komunikację, a w szczególności zgłaszanie wyjątków koprocesora (INT 16). Dla zachowania pełnej zgodności z powyższymi układami udostępniono alternatywną metodę zgłaszania wyjątków za pomocą zewnętrznego przerwania. Wyborem metody steruje znacznik NE z rejestru CR0 (rys. 1).

31	30	29	28	19	18	16	15	6	5	4	3	2	1	0
PG	CD	NW	R	AM	R	WP	R	NE	1	TS	EM	MP	PE	
R	pole zarezerwowane (reserved)													
CD	wyłączenie pamięci podręcznej (cache disable)													
NW	nie przepisywanie pamięci podręcznej (not write through)													
AM	wyrównanie adresów (alignment mask)													
WP	pisanie do zabezpieczonej strony (write protect)													
NE	błędy numeryczne (numerics exception)													

Rys. 1. Rejestr CR0 procesora 486

Nowością procesora 486 jest pamięć podręczna pierwszego poziomu i mechanizm jej sterowania. Globalne znaczniki CD i NW znajdują się w rejestrze CR0 a służą do dezaktywacji wypełniania pamięci podręcznej (alokacji wierszy) i modyfikowania jej zawartości (z zapisem zwrotnym). Sterowanie może odbywać się również na poziomie stronicowania (każda strona niezależnie) za pomocą analogicznych znaczników PCD i PWT (bity 4 i 3) w rejestrze CR3 oraz rekordach katalogów i tablic stron (każdy odpowiednio dla strony którą opisuje). Układy zewnętrzne mogą wyłączyć funkcje pamięci podręcznej niezależnie dla każdego odwołania (sygnał #KEN).

Nowe rejestry TR3, TR4 i TR5 dają możliwość przetestowania pamięci podręcznej w analogiczny sposób jak mechanizm testowania buforów TLB.

Udostępniono mechanizm sprawdzania wyrównania argumentów w pamięci (alignment check). Dostęp do danych o nie wyrównanym adresie sygnalizowany jest za pomocą wyjątku (o charakterze pułapki). Włączenie tego mechanizmu następuje poprzez ustawienie bitów AC (bit 18) w rejestrze EFLAGS oraz AM w rejestrze CR0.

Dodatkowy znacznik WP w rejestrze CR0 steruje nowym elementem mechanizmu ochrony wbudowanym w stronicowanie, który blokuje możliwość zapisu stron (bez atrybutu zapisu) na wszystkich poziomach ochrony (również systemowych).

## PENTIUM i PENTIUM MMX

Rozszerzenie architektury procesorów klasy PENTIUM i PENTIUM MMX (V generacja) polega na dodaniu wielu drobnych mechanizmów. Nowy rejestr sterujący CR4 (rys. 2.) zawiera znaczniki włączające te dodatkowe mechanizmy.

31		9	8	7	6	5	4	3	2	1	0
	R		PCE	R	MCE	R	PSE	DE	TSD	PVI	VME

  

R	zarezerwowane (reserved)
PCE	liczniki zdarzeń (performance monitoring counter enable)
MCE	błędy sprzętowe (machine check enable)
PSE	rozszerzenia wielkości strony (page size extensions)
DE	rozszerzenia uruchomieniowe (debugging extensions)
TSD	licznik czasu (time stamp disable)
PVI	wirtualne przerwania (protected mode virtual interrupt)
VME	rozszerzenia trybu V86 (V86 mode extensions)

Rys. 2. Rejestr sterujący CR4 w procesorach PENTIUM

Lista instrukcji wzbogaciła się o kilka rozkazów użytkowych oraz systemowych. Jest wśród nich rozkaz porównania słów 64 bitowych z zamianą argumentów (CMPXCHG8B) oraz identyfikacja procesora (CPUID), która zwraca nie tylko typ układu ale również opis jego dodatkowych możliwości. Stwierdzenie zaimplementowania tej instrukcji w danym procesorze polega na sprawdzeniu możliwości zmiany wartości znacznika ID (21 bit) w rejestrze EFLAGS.

Rozkazy RDMSR i WRMSR służą do odczytywania i zapisywania rejestrów specyficznych MSR (model specific registers). Rejestry te są po części rozwinięciem koncepcji rejestrów testowych, których występowanie oraz funkcje zależne były od modelu procesora (brak kompatybilności). W związku z tym, że funkcji tego typu pojawiało się coraz więcej zdecydowano wprowadzić mechanizm, który umożliwi w przyszłości w prosty sposób rozwiązanie problemu nowych specyficznych rejestrów sterujących. Odpowiedzialność za ich użycie ponosi oprogramowanie (systemowe). Ze względu na uproszczenie kodowania dostęp do tych rejestrów nie jest swobodny lecz indeksowany co jednocześnie pozwala na wprowadzenie dużej ich liczby. Indeks rejestru przekazywany jest w ECX a wartość w EDX:EAX (64 bity). Dostęp swobodny (MOV) do rejestrów testowych (TR3 – TR7) został zablokowany.

Kolejnym nowym rozkazem jest RDTSC. Odczytuje on wartość wewnętrznego licznika zegarowego (time stamp counter) i zapisuje w rejestrach EDX:EAX. Stan tego 64 bitowego licznika (rejestr MSR) zerowany jest po podaniu sygnału RESET i inkrementowany w każdym cyklu zegara taktującego procesor (wewnętrznie). Możliwe jest zablokowanie wykonania tego rozkazu dla poziomu użytkowego (znacznik TSD w rejestrze CR4).

Większe możliwości do wykorzystania w diagnostyce i optymalizacji daje mechanizm liczników zdarzeń (performance monitoring counter). Można za ich pomocą nie tylko mierzyć czas w cyklach zegara ale także zliczać dziesiątki różnych zdarzeń takich jak np. zapis danych, trafienia w pamięci podręcznej a nawet mierzyć skuteczność przewidywania skoków.

Ponieważ obsługiwane zdarzenia ściśle związane są z mikroarchitekturą, ich zbiór zależy od rodzaju procesora. Dwa niezależne rejestry zliczają zaprogramowane wcześniej zdarzenia. Zarówno do liczników jak i rejestrów konfiguracyjnych dostęp odbywa się za pośrednictwem mechanizmu rejestrów specyficznych (MSR).

Ciekawego rozszerzenia doczekało się stronicowanie (page size extensions). Mechanizm dużych stron pozwala na definiowanie stron o wielkości 4 MB. Jest to spójny obszar zastępujący przestrzeń wszystkich normalnych stron (4 KB) z jednej tablicy (1024 pozycje) i może być zdefiniowany tylko na poziomie katalogu tablic. Wielkość strony określa znacznik PS (bit 7) w rekordzie katalogu tablic. W dużych stronach translacji podlega jedynie 10 najstarszych bitów a 22 młodsze stanowią przemieszczenie.

Rozszerzenia trybu V86 (V86 mode extensions) dotyczą obsługi przerwania w tym trybie. Przerwania sprzętowe obsługiwane są zawsze poza trybem V86 na najwyższym poziomie ochrony ale możliwe jest wirtualne ich blokowanie (jeżeli IOPL<3 co uniemożliwia ich rzeczywistego maskowania – normalnie generując wyjątek). Jeżeli mechanizm ten jest aktywny (bit VME rejestru CR4) to wszelkie operacje (CLI, STI, PUSHF, POPF) na fladze IF (zezwolenia przyjmowania przerwania) przekierowane są na znacznik VIF (bit 19 rejestru EFLAGS). Wykonanie rozkazu STI przy ustawionym znaczniku VIP (bit 20 rejestru EFLAGS) powoduje wygenerowanie wyjątku. Dzięki temu wykrycie wirtualnego zamaskowania przerwania możliwe jest przez procedurę obsługi (zgłoszonego przerwania) i jeżeli jest to dopuszczalne (ze względu na charakter przerwania) odłożenie obsługi przerwania w czasie. W takiej sytuacji procedura obsługi powinna ustawić znacznik VIP aby wykryć wirtualne odblokowanie przerwania.

Analogiczny mechanizm obowiązuje w trybie chronionym odnośnie procesów wykonywanych na 3 poziomie ochrony jeżeli ustawiony jest znacznik wirtualnych przerwania PVI w rejestrze CR4.

Przerwania programowe w trybie V86 normalnie obsługiwane są przez procedury trybu chronionego, jeżeli IOPL jest na poziomie 3. W przeciwnym wypadku wykonanie rozkazu INT na 3 poziomie ochrony (tryb V86) spowoduje wygenerowanie wyjątku. Przy włączonym rozszerzeniu trybu V86 wykonanie rozkazu INT powoduje najpierw odwołanie do specjalnej tablicy przekierowań (32 bajty), która znajduje się bezpośrednio przed tablicą zezwoleń wejścia wyjścia w segmencie TSS. Jeżeli odpowiadający przerwaniu bit z tej tablicy jest wyzerowany to obsługa przerwania odbywa się w ramach aktualnego zadania w trybie V86 tak jak w trybie rzeczywistym.

Rozszerzenie mechanizmów uruchomieniowych (debugging extensions) polega na umożliwieniu ustawiania pułapek na adresach przestrzeni wejścia/wyjścia. Zrealizowano to za pomocą zabronionego do tej pory ustawienia (wartość 2) pól R/W, które definiują rodzaj przechwytywanego odwołania dla każdej z czterech pułapek. Mechanizm ten dostępny jest po ustawieniu znacznika DE rejestru CR4.

Mechanizm zgłaszania błędów sprzętowych (machine check) pozwala na zainstalowanie procedury obsługi na okoliczność wystąpienia błędu (przekłamań) zarówno wewnątrz procesora (błędy parzystości) jak i na magistrali zewnętrznej (zgłaszane przez inne urządzenia dedykowaną linią). Jeżeli błąd taki wystąpi i bit MCE w rejestrze CR4 jest ustawiony zostanie wygenerowane specjalne przerwanie. Jeżeli mechanizm ten jest wyłączony to w takiej sytuacji nastąpi wstrzymanie procesora (shutdown) – przejście w stan, z którego wyjść można jedynie podając sygnał RESET.

Do obsługi specyficznych cech systemu takich jak zarządzanie poborem mocy wprowadzono oddzielny tryb pracy procesora tak zwany SMM (system management mode). Co prawda tryb ten pojawił się już w procesorach 386 oraz 486 choć tylko w wersjach o obniżonym poborze mocy (do komputerów przenośnych) ale na dobre zagościł dopiero w architekturze procesorów PENTIUM. Jedynym sposobem wejścia w tryb SMM jest zgłoszenie specjalnego przerwania SMI (system management interrupt). Sposób działania procesora w tym trybie podobny jest do trybu rzeczywistego ale przestrzeń adresowa jest liniowa o wielkości 4 GB. Po wejściu w tryb SMM procesor zapamiętuje w specjalnie wydzielonej pamięci swój stan i zaczyna wykonywać rozkazy od wyznaczonego adresu. Adres ten można zmienić ale tylko w trybie SMM. Dzięki temu cały mechanizm jest zupełnie przezroczysty nie tylko dla programów użytkowych ale także dla systemu operacyjnego. Powrót z trybu SMM realizuje instrukcja RSM.

Cechą wyróżniającą PENTIUM MMX jest nowa stałopozycyjna jednostka wektorowa typu SIMD (single instruction multiple data), która realizuje 57 nowych operacji. Są to instrukcje zoptymalizowane pod kątem przetwarzania multimediiów. Charakterystyczna jest dla nich arytmetyka z nasyceniem. Rozkazy te pracują na upakowanych formatach danych (8 bajtów, 4 słowa, 2 dwusłowa lub poczwórne słowo). Osiem roboczych 64 bitowych rejestrów MM0–MM7 jest mapowanych w rejestry koprocessora. Dzięki temu nie potrzeba żadnych dodatkowych zabiegów ze strony systemu operacyjnego do przełączenia kontekstu tej jednostki, wystarczy standardowe wsparcie dla jednostki zmiennoprzecinkowej. Powoduje to jednak, że nie można bezpośrednio przeplatać operacji MMX i zmiennoprzecinkowych, a program który chce korzystać z obu jednostek musi przeładowywać wspólne rejestry. Zmiana ich stanu tak aby po operacjach MMX ponownie mogły być wykorzystane przez jednostkę zmiennoprzecinkową odbywa się za pomocą rozkazu EMMS. Dostęp do rejestrów MMX jest swobodny i są one adresowane bezwzględnie w przeciwieństwie do rejestrów zmiennoprzecinkowych (model stosowy).

## Procesory VI generacji

Linie procesorów VI generacji rodziny x86 firmy INTEL, oznaczoną symbolem **P6** tworzą układy PENTIUM PRO, CELERON, PENTIUM II oraz PENTIUM III.

Procesory te różnią się między sobą w nieznaczny sposób. Pierwszy z układów tej grupy (PENTIUM PRO) charakteryzuje się mniejszymi pamięciami podręcznymi pierwszego poziomu (po 8 KB) oraz brakiem jednostki MMX. Z kolei ostatni jej przedstawiciel (PENTIUM III) został dodatkowo wyposażony w rozszerzenie SSE (Streaming SIMD Extension) czyli blok realizujący zestaw nowych rozkazów będących rozwinięciem koncepcji MMX.

Liczne rozszerzenia systemowe i nowe mechanizmy są cechą specyficzną różnych wersji i modeli procesorów P6. W celu ich wykorzystania należy najpierw sprawdzić czy zostały zaimplementowane. Do tego celu służy instrukcja CPUID, która wywołana z wartością 1 w rejestrze EAX zwraca w ECX status zaimplementowanych rozszerzeń.

	7	6	5	4	3	2	1	0	
	R						XMM	FXSR	+24
MMX	R					PN	PSE 36	PAT	+16
CMOV	MCA	PGE	MTRR	SEP	R	APIC	CX8	+8	
MCE	PAE	MSR	TSC	PSE	DE	VME	FPU	+0	

  

R	zarezerwowane (reserved)
FPU	jednostka zmiennoprzecinkowa (floating point unit)
VME	rozszerzenia trybu V86 (virtual mode enhancements)
DE	rozszerzenia uruchomieniowe (debugging extensions)
PSE	rozszerzenie wielkości strony (page size extensions)
TSC	licznik czasu (time stamp counter)
MSR	rejstry specyficzne (model specific registers)
PAE	rozszerzenie adresu fizycznego (physical address extension)
MCE	wyjątek błędów sprzętowych (machine check exception)
CX8	instrukcja CMPXCHG8B
APIC	wbudowany APIC (advanced programmable interrupt controller)
SEP	szybkie wywołanie systemu (fast system call)
MTRR	rejstry typu obszarów pamięci (memory type range registers)
PGE	globalne strony (page global flag)
MCA	architektura kontroli błędów (machine check architecture)
CMOV	instrukcje CMOV, FCMOV oraz FCOMI
PAT	tablica atrybutów stron (page attribute table)
PSE 36	36 bitowy adres strony (36 bit page size extension)
PN	wbudowany numer identyfikacyjny procesora (processor number)
MMX	jednostka MMX
FXSR	instrukcje FXSAVE i FXRSTOR
XMM	rozszerzenie Streaming SIMD

Rys. 3. Informacja o rozszerzeniach architektury zwracana przez CPUID

W modelu programowym procesorów P6 pojawiło się kilka nowych instrukcji. Są to warunkowe przesłania CMOV i FCMOV (warunki takie jak dla instrukcji skoków), zmiennoprzecinkowe porównanie (FCOMI) modyfikujące znaczniki (jednostki stałopozycyjnej) EFLAGS, odczyt liczników zdarzeń (RDPMC) oraz instrukcja UD2 powodująca wygenerowanie wyjątku niezdefiniowanego rozkazu. Ta ostatnia jest po prostu zarezerwowanym niezdefiniowanym kodem operacji (kod ten nigdy nie będzie wykorzystany).

Rozkazy SYSENTER i SYSEXIT służą do szybkiego przekazania sterowania do systemu operacyjnego (wywołania funkcji systemowej) oraz szybkiego powrotu. Przeznaczone są do pracy w środowisku płaskiego modelu pamięci na dwóch poziomach ochrony (system / user). Instrukcje nie zapisują stanu żadnych rejestrów, przeładowując tylko wartości rejestrów CS, SS, EIP i ESP z odpowiednich rejestrów MSR (model specific registers) oraz wpisując stałe wartości do rejestrów deskryptorów segmentów kodu i stosu.

Nowy mechanizm stron globalnych pozwala za pomocą znacznika G (global – bit 8) w deskryptorach stron zdefiniować strony nie podlegające odrzuceniu z buforów TLB na skutek przeładowania rejestru CR3 (przełączenia zadań). Odpowiedzialność za prawidłowe wykorzystanie mechanizmu ponosi system operacyjny. Jako globalne powinny być oznaczane tylko te strony, które odwzorowane są tak samo (w przestrzeń fizyczną) w każdym kontekście. Mechanizm włączany jest znacznikiem PGE (bit 7) rejestru CR4.

Kolejnym rozszerzeniem stronicowania jest mechanizm 36 bitowego adresu fizycznego PAE. Pozwala on na dostęp do 64 GB przestrzeni adresowej. Włączenie tego mechanizmu następuje po ustawieniu znacznika PAE (bit 5) w rejestrze CR4 i zmienia sposób działania stronicowania. W nowym trybie rejestr CR3 wskazuje na specjalną tablicę (indeksowaną 2 najstarszymi bitami adresu liniowego) zawierającą cztery rekordy opisujące niezależne katalogi tablic stron. Opisy stron są 64 bitowe dlatego w katalogach i tablicach stron (4 KB) mieści się 512 rekordów (indeksowanych 9 bitami adresu liniowego). Przy włączonym rozszerzeniu adresu fizycznego duże strony mają wielkość 2 MB ( $32 - 2 - 9 = 21$  bitowe przemieszczenie na stronie).

W niektórych procesorach P6 zaimplementowano mechanizm PSE 36, który jest wzbogaceniem rozszerzenia wielkości strony PSE i umożliwia dla dużych stron (4 MB) podanie 36 bitowego adresu fizycznego. Najstarsze bity umieszczone są wtedy na pozycjach 16 – 13 deskryptora strony. Nie jest potrzebna żadna dodatkowa aktywacja tego mechanizmu (poza włączeniem rozszerzenia wielkości strony PSE w CR4).

Procesory P6 pozwalają na efektywne wykorzystanie pamięci podręcznych poprzez zdefiniowanie fizycznych obszarów pamięci oznaczonych jako „uncacheable”, „write through”, „write back”, „write protected” oraz „write combining”. Nowa strategia „write protected” wykorzystuje pamięć podręczną tylko dla odczytów. Każdy zapis do takiego obszaru unieważnia zaalokowaną linię pamięci podręcznej. Dla obszarów „write combining” funkcje pamięci podręcznej są wyłączone (przesłania trafiają bezpośrednio do pamięci zewnętrznej) ale możliwe jest odkładanie w czasie zapisów i składanie ich w ramach jednego przesłania na magistrali.

Rejestry MTRRs (memory type range registers) definiują określone obszary pamięci według powyższych schematów. W skład rejestrów MTRRs wchodzi rejestr obszarów stałych (8 x 64 KB, 16 x 16 KB, 64 x 4 KB) oraz zmiennych dla których definiuje się adres bazowy i maskę (po 24 bity – najstarsze bity 36 bitowego adresu). Dokładne informacje o zaimplementowanych funkcjach MTRRs zwraca rejestr MTRRcap. Dostęp do tego mechanizmu odbywa się poprzez rejestry MSR.

Rozszerzenie PAT daje możliwość precyzyjnego definiowania typu obszarów pamięci w ramach stronicowania. Specjalna tablica PAT (rejestr MSR) zawiera definicje 8 typów obszarów pamięci. Każdy typ może być zdefiniowany jako „uncacheable”, „write through”, „write back”, „write protected”, „write combining” lub „uncached”. Ten ostatni jest najbardziej dominujący (w przeciwieństwie do pierwszego, który może być przysłonięty obszarem „write combining” zadeklarowanym w rejestrach MTRRs). Indeksami do tablicy PAT są (mniej znaczące) bity PCD i PWT deskryptora strony oraz (najbardziej znaczące) znacznik PATi (bit 7 w deskryptorach stron 4 KB, bit 12 w deskryptorach stron 2 MB i 4 MB). Początkowa wartość tablicy PAT ustawiona jest w taki sposób, że bity PCD i PWT dają taki efekt jak w procesorach bez rozszerzenia PAT. Ostatecznie strategia wykorzystania pamięci podręcznych zależy od mechanizmu PAT oraz ustawień rejestrów MTRRs (wybierana jest bardziej restrykcyjna).

Rozbudowany mechanizm wykrywania błędów sprzętowych (machine check architecture) pozwala na precyzyjne określenie przyczyny zgłoszenia błędu. Wszystkie błędy wykryte podczas pracy układu rejestrowane są w odpowiednich rejestrach MSR. Niektóre z tych błędów zostają skorygowane (korekcja ECC), nie powodując zaburzeń pracy. Te błędy, które nie mogą zostać skorygowane powodują wygenerowanie specjalnego wyjątku (Machine Check Exception). Daje to możliwość wykrycia i rejestrowania przyczyny. Przewidziano również możliwość (w pewnych szczególnych przypadkach) kontynuowania pracy (na stosie znajduje się poprawny adres powrotu). Na mechanizm ten składa się szereg rejestrów MSR.

Dodatkowy zestaw instrukcji rozszerzenia SSE (PENTIUM III) dotyczy operacji na upakowanych formatach danych zmiennoprzecinkowych (4 x 32 bity) i jest specjalizowany pod kątem graficznych operacji wektorowych. Instrukcje te pracują na ośmiu nowych 128 bitowych rejestrach. W celu wykorzystania tego rozszerzenia wymagane jest wsparcie systemu operacyjnego (przy zmianie kontekstu). Wsparcie to sygnalizowane jest ustawieniem znacznika OSFXSR (bit 9) rejestru CR4. Dodatkowo przez system operacyjny ustawiany powinien być znacznik OSXMMEXCPT (bit 10) jeżeli obsługiwane są niezamaskowane wyjątki SSE.

Do szybkiego zapisania i odtworzenia pełnego stanu koprocatora służą instrukcje FXSAVE i FXRSTOR. Osiem rejestrów wspólnych dla jednostki zmiennoprzecinkowej oraz MMX zapisywane jest z wyrównaniem do 128 bitów. Zapamiętany zostaje też stan rejestrów rozszerzenia SSE. Cała struktura ma wielkość 512 bajtów. Użycie tych rozkazów przez system operacyjny do zmiany kontekstu koprocatora zapewnia pełną kompatybilność z przyszlymi układami i ich nowymi cechami.

Numer identyfikacyjny procesora jest unikalnym 96 bitowym identyfikatorem. Odczytać go można za pomocą rozkazu CPUID wywołanego z wartością EAX = 1 (bardziej znaczące 32 bity w EAX) oraz EAX = 3 (mniej znaczące 64 bity w EDX:ECX) ale tylko jeżeli funkcja ta jest zaimplementowana i włączona. Włączenie mechanizmu następuje po podaniu sygnału RESET, a wyłączenie po ustawieniu 21 bitu rejestru BBL\_CR\_CTL (MSR).

Procesory grupy P6 posiadają ciekawy mechanizm uaktualniania mikro kodu. Kilka specjalnych rejestrów MSR przeznaczonych jest do przeprowadzenia takiej aktualizacji. Jej celem jest eliminacja pewnych błędów wykrytych już po wprowadzeniu układu na rynek i zarejestrowanych w tak zwanej erracie. Aktualizacja musi być wykonana po każdym wyzerowaniu procesora, dlatego najczęściej odpowiedzialny za tą operację jest BIOS. Specjalnie przygotowana sekwencja mikro kodu ma długość 2048 bajtów (48 bajtów nagłówka) i jest przeznaczona dla konkretnego modelu (tylko pod warunkiem pełnej zgodności zostanie załadowana). Format samej sekwencji mikro kodu (nie licząc nagłówka) nie jest ujawniany.

Zainteresowanych szczegółami opisanych mechanizmów odsyłam do źródeł:

[1] „The Intel Architecture Software Developer’s Manual Vol. 1 Basic Architecture” Order Number 243190\*, INTEL corp. 1999

[2] „The Intel Architecture Software Developer’s Manual Vol. 2 Instruction Set Reference” Order Number 243191\*, INTEL corp. 1999

[3] „The Intel Architecture Software Developer’s Manual Vol. 3 System Programming Guide” Order Number 243192\*, INTEL corp. 1999

[4] „Intel Architecture Optimization Manual” Order Number 242816-003\*, INTEL corp. 1997

[5] „Intel Architecture Optimization Manual” Order Number 245127-001\*, INTEL corp. 1999

\* dokumenty dostępne w sieci INTERNET na stronach firmy INTEL ([developer.intel.com](http://developer.intel.com))