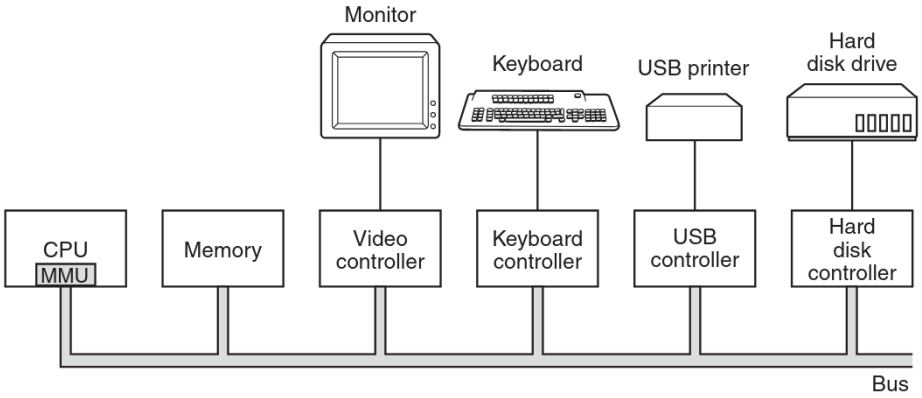
Architektura komputerów



- procesor
- pamięć
- sterowniki urządzań (kontrolery) wejścia-wyjścia, do których podłączone są urządzenia peryferyjne
- szyna (magistrala) systemowa łączące te elementy

Procesor

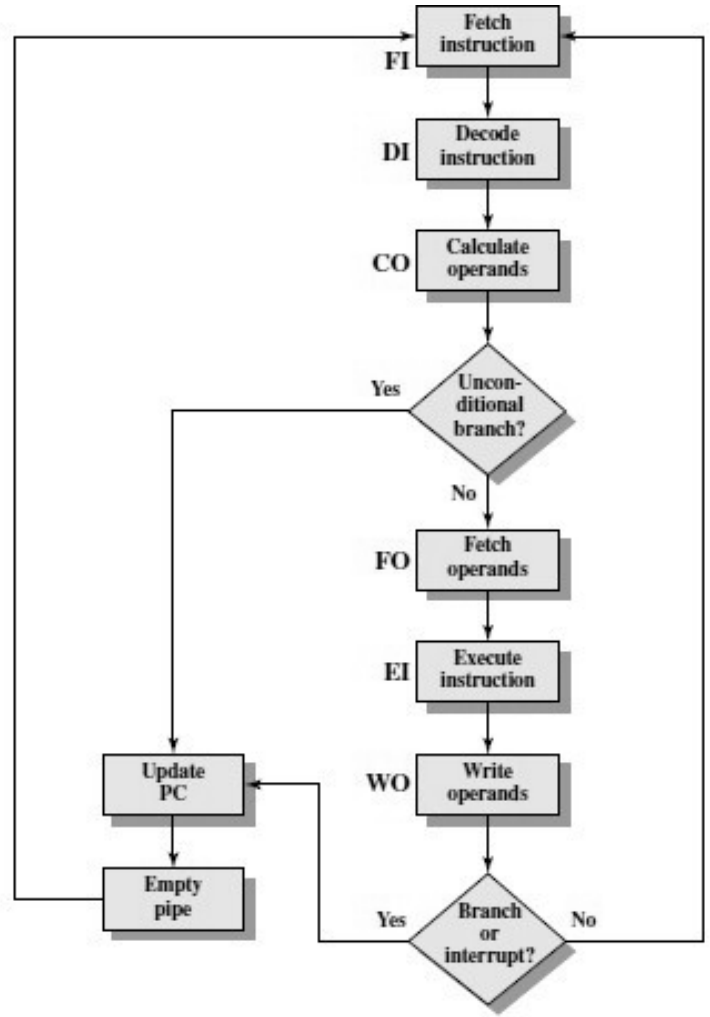
- rejestry
  - rejestry ogólnego zastosowania (x86: EAX, EBX, ECX, EDX)
  - licznik programu (*program counter*) - zawiera adres następnej instrukcji (x86: EIP)
  - wskaźnik stosu (*stack pointer*) wskazuje najwyższy element stosu wywołań w pamięci (x86: ESP)
- słowo statusu programu (PSW *program status word*)
  - wyniki instrukcji warunkowych, flagi, bity kontrolne, stan systemu
  - tryb ochrony (tryb jądra, użytkownika)
- potok instrukcji - pobranie, zdekodowanie, wykonanie instrukcji

System operacyjny musi znać stan wszystkich rejestrów. Podczas przełączania zadań zapisuje stan rejestrów, żeby móc je później przywrócić przy wznowieniu programu.

Architektura współczesnego procesora

- **przetwarzanie potokowe** - podział rozkazu na wyspecjalizowane etapy
- **superskalarność** - zrównoleglenie wykonania rozkazów w obrębie jednego procesora poprzez zwielokrotnienie skalarnych jednostek wykonawczych
- analiza przepływu danych, przewidywanie rozgałęzienia, spekulatywne wykonywanie - badanie zależności między rozkazami i wykonywanie ich poza kolejnością, aby zmniejszyć opóźnienia
- **hiperwątkowość** (*hyper-threading*) - wiele wątków w jednym procesorze
- **instrukcje SIMD** (*Single Instruction Multiple Data*) - jedna instrukcja operuje na wielu danych jednocześnie (np. multimedia, obliczenia naukowe), MMX (*MultiMedia Extensions*), SSE (*Streaming SIMD Extensions*), AMD 3DNow (*3D NO Waiting*)
- **wielordzeniowość** - wiele jednostek wykonawczych (rdzeni) w jednym procesorze
- wsparcie sprzętowe **wirtualizacji**: Intel VT (vmx), AMD V (svm)
- **CISC** i **RICS** - złożone i zredukowane zestawy rozkazów

Przetwarzanie rozkazów



FI: pobierz następną instrukcję do bufora

DI: dekodowanie instrukcji, określ kod operacji i specyfikację argumentów

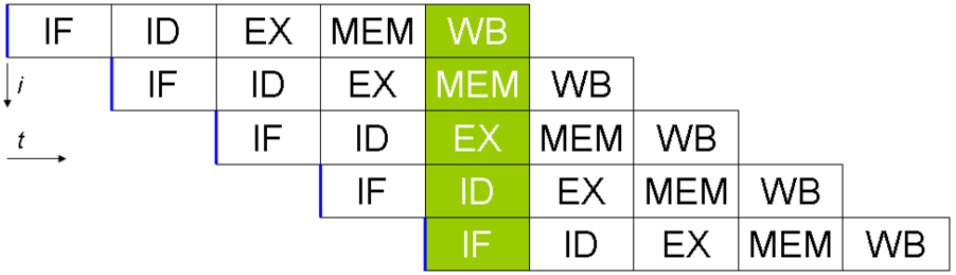
CO: oblicz efektywny adres danych źródłowych

FO: pobierz dane z pamięci jeżeli nie ma ich w rejestrach

EI: wykonaj instrukcję

WO: zapisz wynik w pamięci

Przetwarzanie potokowe



Klasyczny potok RISC:

IF=Instruction Fetch

ID=Instruction Decode

EX=Execute

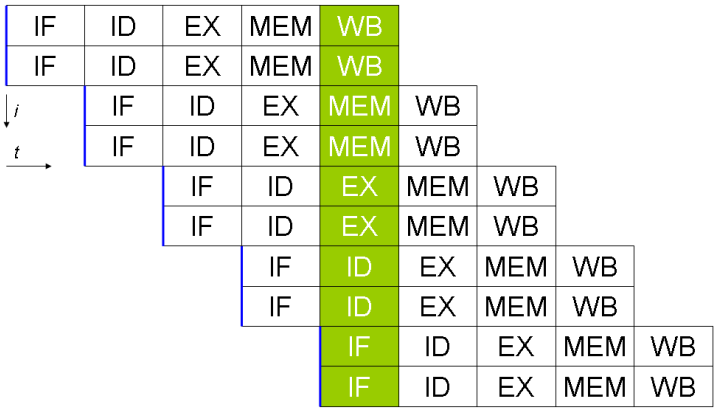
MEM=Memory access

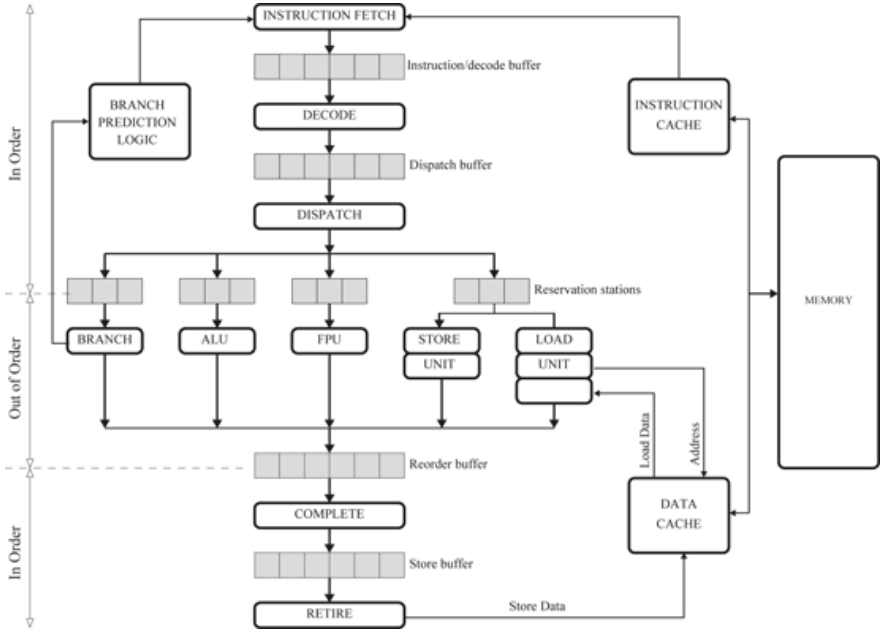
WB=Register write back

- podział rozkazu na wyspecjalizowane etapy
- dzięki podziałowi, różne instrukcje mogą być wykonywane równocześnie
- lepsza wydajność: zwiększenie liczby instrukcji wykonywanych w jednostce czasu
- problem z rozgałęzieniami (instrukcja skoku) i konflikty w dostepnie do zasobów

https://en.wikipedia.org/wiki/Instruction_pipelining

Superskalarność





- zrównoleglenie wykonania rozkazów w obrębie jednego procesora poprzez zwielokrotnienie skalarnych jednostek wykonawczych
- w jednym cyklu procesora wykonywane jest wiele instrukcji
- wykonanie poza kolejnością (*out-of-order*) instrukcji z bufora w celu zmaksymalizowania użycia CPU

http://en.wikipedia.org/wiki/Superscalar,
https://anubhavbhatla.github.io/projects/superscalar/

Ryzyka przetwarzania potokowego

Zatory w potoku poleceń pojawiają się, gdy instrukcje warunkowe nie pozwalają na sekwencyjne wykonanie instrukcji.

Możliwe ryzyka wykonania kodu poza kolejnością:

- **strukturalne** - gdy instrukcje w potoku nie moga być wykonane równocześnie
- **danych** - gdy instrukcje korzystają z tych samych danych i wynik zależy od kolejności operacji
- **sterowania** - wykonanie instrukcji po rozwidleniu ale przed wykonaniem instrukcji warunkowej. Instrukcje z błednej ścieżki muszą zostać odrzucone z potoku.

Ryzyka przetwarzania potokowego

Jak rodzić sobie z konfliktami:

- wykonywanie instrukcji obu ścieżek jednocześnie
- przewidywanie rozgałęzień (np. na podstawie statystyki poprzednich wykonań). Kod jest spekulatywnie wykonywany. W przypadku błednej predykcji efekt tego wykonania jest odrzucany
- *branch-free-code* technika programowania z minimalizowaniem rozgałęzień kodu
- bufor pętli - mała, bardzo szybka pamięć podręczna dla etapu pobierania (FI), jeśli wystąpi rozgałęzienie, sprzęt najpierw sprawdza, czy cel rozgałęzienia znajduje się w buforze pętli
- opóźnianie rozgałęzień - zmiana kolejności instrukcji tak aby instrukcje warunkowe można było wykonać jak najpóźniej

CISC (*Complex Instruction Set Computer*)

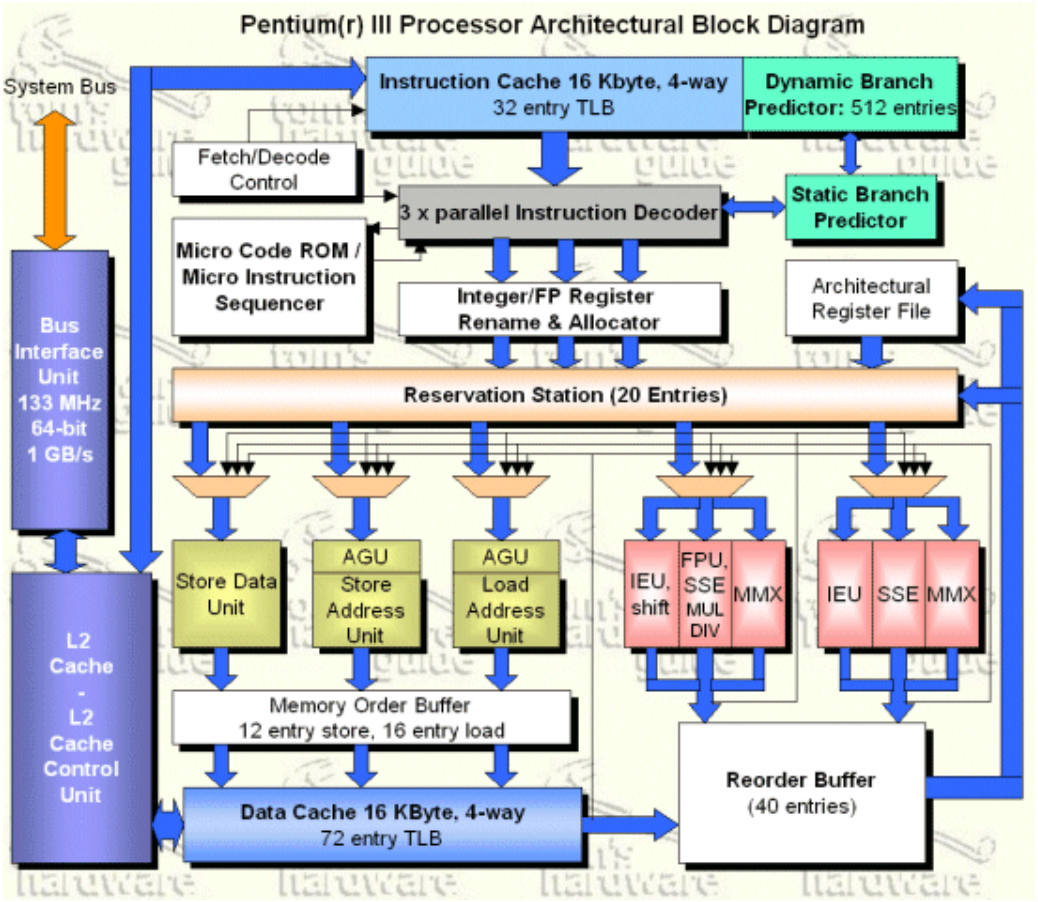
komputer o pełnej liście rozkazów

RISC (*Reduced Instruction Set Computer*)

komputer o zredukowanej liście rozkazów

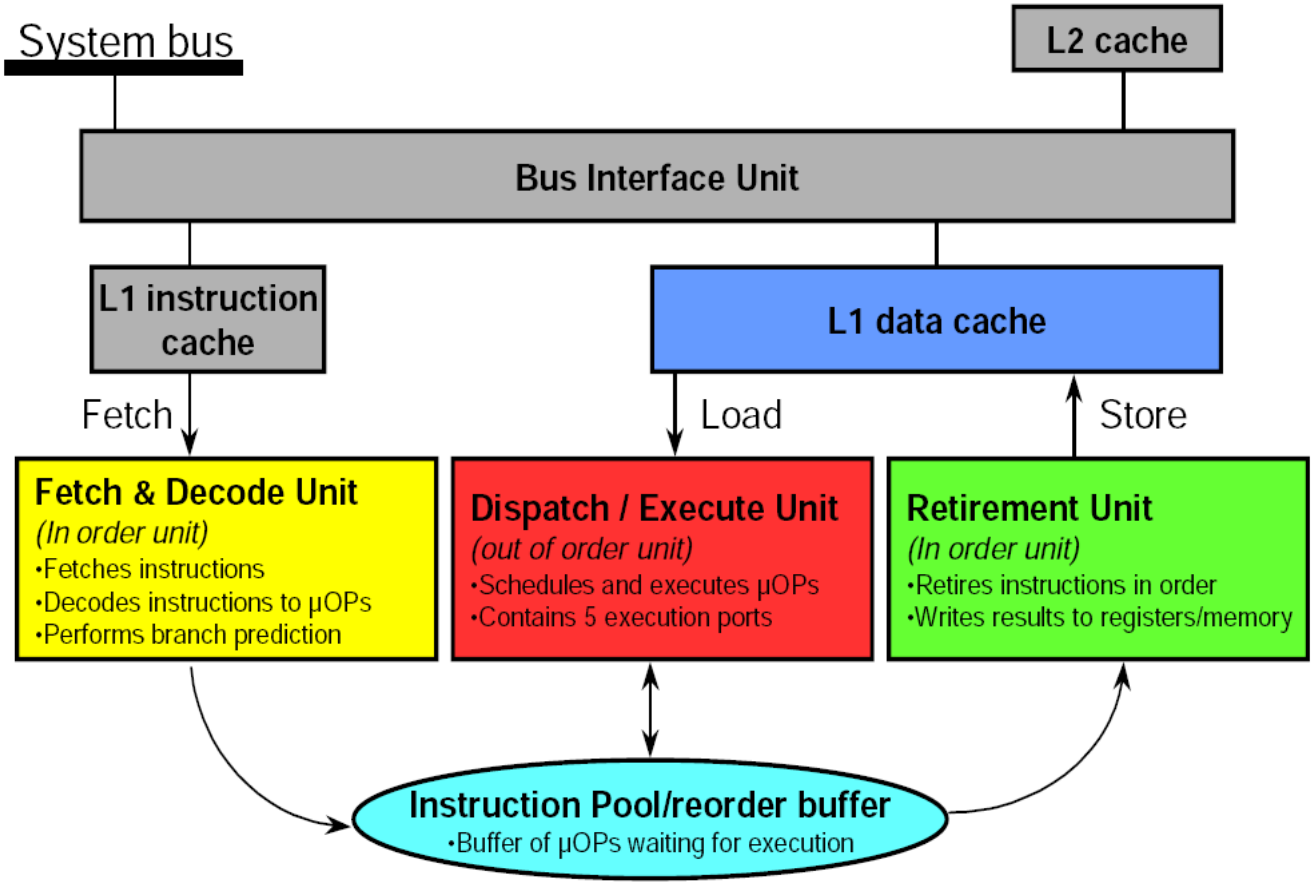
Cechy	RISC	CISC
Liczba instrukcji	Zredukowany zestaw (kilkadziesiąt)	Duży zestaw (100–200)
Złożoność instrukcji	Proste, jednolite	Złożone, wyspecjalizowane
Czas wykonania instrukcji	Zazwyczaj 1 cykl zegara	Wiele cykli zegara
Tryby adresowania	Ograniczone (2–4)	Duża liczba (5–20)
Długość instrukcji	Stała (np. 32 bity)	Zmienna
Odwołania do pamięci	Ograniczone (operacje rejestr-rejestr)	Częste (operacje pamięć-pamięć)
Liczba rejestrów	Duża liczba rejestrów ogólnego przeznaczenia	Mniejsza liczba rejestrów
Jednostka sterująca	Zaimplementowana sprzętowo	Mikroprogramowana (ROM)
Projektowanie potoku	Uproszczone, wydajne	Złożone, trudniejsze do optymalizacji
Przetwarzanie	Optymalizowane pod kątem potoku	Mikroprogramowane, mniej przewidywalne
Zastosowanie	Urządzenia mobilne, systemy oszczędne energetycznie, nowoczesne procesory	Starsze systemy, kompatybilność wsteczna
Przykłady	ARM, MIPS, RISC-V, Apple M1	x86 (Intel, AMD)

Występują też architektury mieszane - złożone instrukcje rozkładane są na prostsze (μOPS)



Zmodyfikowana architektura harwardzka architektura mieszana, łączy w cechy architektury harwardzkiej i architektury von Neumanna. Oddzielone obszary pamięci na dane i rozkazy.

Pentium II and Pentium III Processors Architecture



dynopt.dtc.umn.edu/documents/IA-OPTIMIZATION-Ref-Manual.pdf

Pamięć: rodzaje, własności

- szybki rozwój pojemności pamięci i szybkości procesorów
- wolniejszy przyrost szybkości przesyłania danych pomiędzy procesorem i pamięcią

Interfejs pomiędzy pamięcią główną a procesorem jest najbardziej krytycznym elementem całego komputera, ponieważ jest on odpowiedzialny za przepływ rozkazów i danych pomiędzy tymi układami.

Jeśli dostęp do pamięci jest niewystarczający, to cykle procesora są marnowane (**głodzenie procesora**).

Wymagania dotyczące pamięci: niska cena, duża pojemność, szybkość działania (porównywalna z szybkością CPU)

Hierarchia pamięci:

- rejestry (SRAM)
- pamięć podręczna, cache (SRAM)
- pamięć główna (MCDRAM, DRAM, NVRAM, NVDIMM)
- pamięć dyskowa (HDD, SDD)
- pamięć taśmowa, dyski optyczne

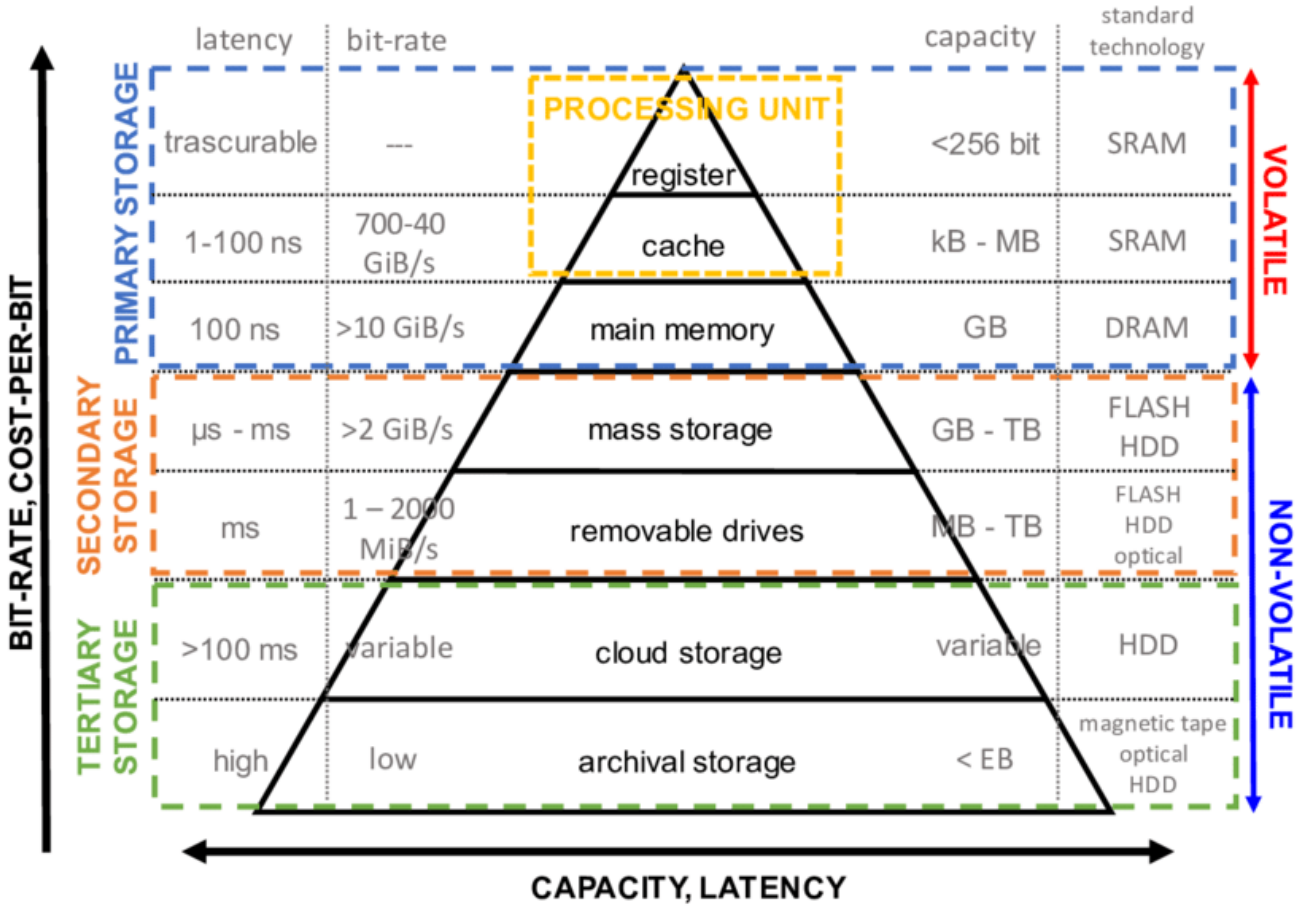
Koszt trafienia/chybienia (w cyklach) dla procesora Pentium M:

rejestr	$\leqslant 1$
L1d	≈ 3
L2	≈ 14
pamięć główna	≈ 240

Zob.: Interactive latency

```
$ curl cheat.sh/latencies
```

Hierarchia pamięci[1]



[1]E. Gemo, *The design and analysis of novel integrated phase-change photonic memory and computing devices*, 2021

Hierarchia pamięci

Im niżej w hierarchi od CPU

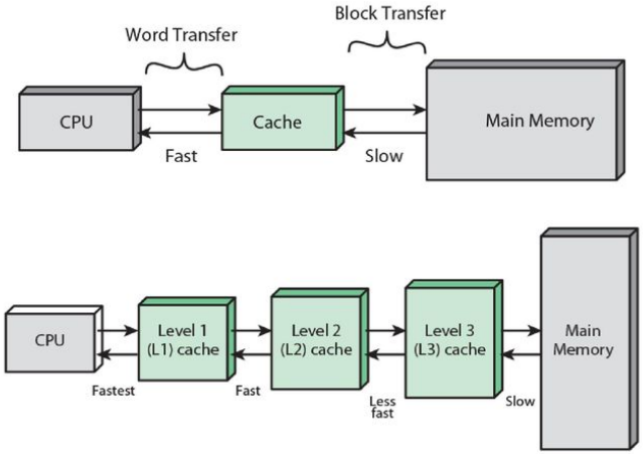
- malejąca cena/bit
- rosnąca pojemność
- rosnący czas dostępu
- malejąca częstość dostępu przez preceosor

Rodzaj dostępu do pamięci:

- dostęp sekwencyjny
  - odczyt/zapis wyłącznie w określonej sekwencji liniowej (np. pamięć taśmowa)
  - czas dostepu zależy od położenia danych
- dostęp swobodny
  - pozycja w pamięci dostępna za pomocą unikatowego adresu (pamięć RAM)
  - czas dostepu stały, nie zalezy od lokalizacji danych
- dostęp bezpośredni
  - pamięć podzielona na bloki (lub rekordy) o unikatowych adresach (np. pamięć dyskowa)
  - najpierw dostęp (swobodny) do najbliższego otoczenia (wybór bloku) a potem poszukiwanie loakcji koncowej (sekwencyjne)
- dostęp skojarzeniowy
  - rodzaj dostępu swobodnego, który umożliwia porównywanie i specyficzne badanie zgodności wybranych bitów wewnątrz słowa (zachodzi to dla wszystkich słów jednocześnie)
  - słowo jest wyprowadzane na podstawie części swojej zawartości, a nie na podstawie adresu (zastosowanie: pamięć podręczna procesora)
  - stały czas dostępu

Pamięć podręczna (cache)

działa jako pośrednik między ultra-szybkim procesorem a wolną pamięcią główną



- przechowuje kopie fragmentu pamięci głównej
- proceseor najpierw sprawdzana obecność danych w pamięci podręcznej
- jeśli danych brakuje (chybienie), to do pamięci podręcznej wczytywany jest właściwy blok pamięci głownej

Lokalność przestrzenna

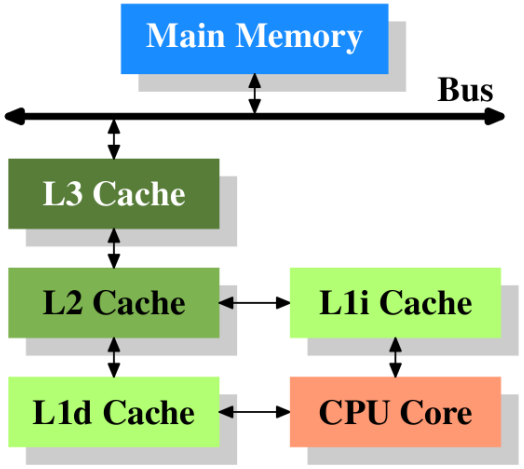
- tendencja do częstych odwołań do danych położonych blisko siebie w pamięci
- takie dane mają szansę trafić do tego samego bloku w pamięci podręcznej

Lokalność czasowa

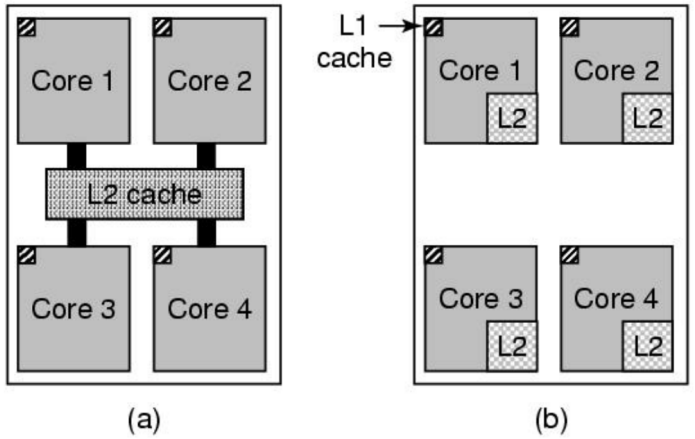
- tendencja do częstych odwołań do tych samych danych w krótkich odstępach czasu
- dane często wykorzystywane mają szansę pozostać w pamięci podręcznej pomiędzy rządaniami

Procesor i pamięć

Architektura jednoprocesorowa



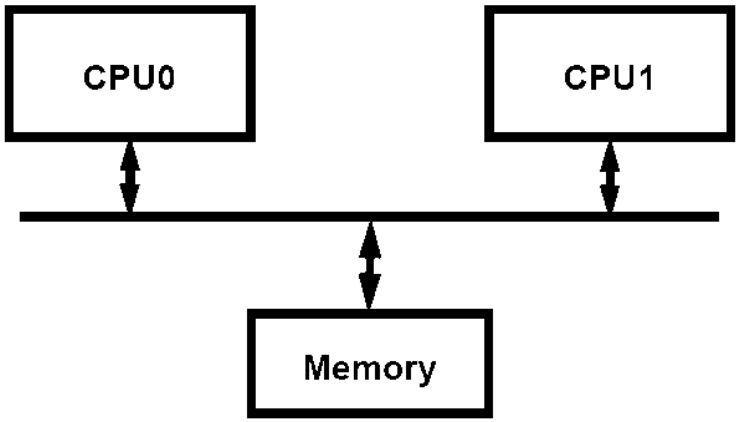
Architektura wieloprocesorowa



a) współdzielony L2 przez 4 procesory
b) niezależne L1 i L2 w układzie 4 procesorów

Wieloprocesorowość symetryczna (SMP)

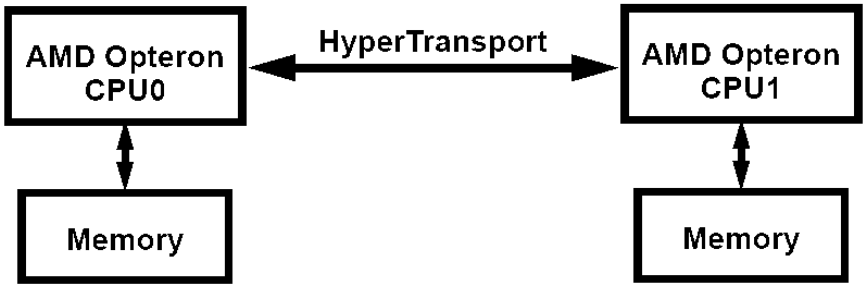
Symmetric Multiprocessing



- procesory współdzielą zasoby pamięci oraz urządzenia wejścia/wyjścia przy pomocy magistrali systemowej
- każdy z procesorów może zostać przypisany do wykonywania konkretnego zadania, tak aby w systemie następowało równoważenie obciążenia (*load balancing*)
- przepustowość szyny i pamięci ogranicza szybkość działania procesorów

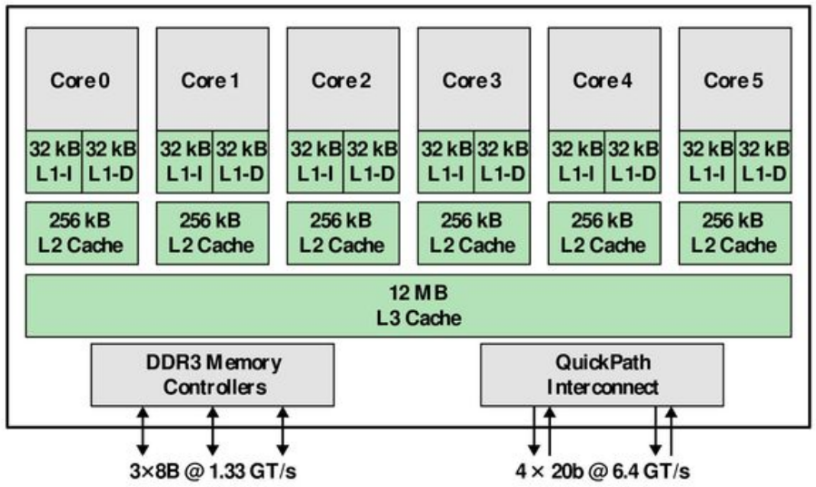
Niejednolity dostęp do pamięci (NUMA)

Non-Uniform Memory Access



- minimalizacja opóźnień dostępu do pamięci poprzez przydzielenie pamięci lokalnej dla każdego procesora
- każdy procesor posiada własny kontroler pamięci lokalnej
- procesory łączone między sobą za pomocą szyny o dużej przepustowości i niskich opóźnieniach (HyperTransport), która nie ma bezpośredniego połącznia z układem pamięci
- wydłużony czas dostępu do pamięci zdalnej (połączonej z innym procesorem)
- wymaga właściwej organizacji danych w pamięci aby zapewnić efektywność

Architekruty wieloprocesorowe



Rysunek 1: Intel Core-i7 990X

- wiele procesorów (rdzeni) na jednej kości
- każdy rdzeń posiada jednostkę wykonawczą, rejestry, lokalną pamięć podręczną, rdzeńie mogą być wielwątkowe
- rdzenie współdzielą pamięć L3
- pamięć połączona z procesorem za pomocą szybkiej szyny (DDR3), urządzenia I/O za pomocą osobnej szyny (PCIe)

Rodzaje pamięci półprzewodnikowych:

RAM (*Random Access Memory*) pamięć o dostępie swobodnym – odczyt-zapis, wymazywanie/zapisywanie elektryczne na poziomie bajta

Static RAM (SRAM) - statyczna pamięć o dostępie swobodnym

- rejestry i pamięć podręczna
- ulotna, przechowuje dane tak długo, jak długo włączone jest zasilanie
- każdy bit przechowywany w układzie zbudowanym z 6 transystorów (mniejsza gęstość danych niż DRAM)

Dynamic RAM (DRAM) - pamięć dynamiczna

- pamięć głowna komputera
- ulotna, wymaga okresowego odświeżania zawartości

Pamięci dynamiczne

Synchronous DRAM (SDRAM) - pamięc dynamiczna pracująca synchronicznie z magistralą systemową

	napięcie	pojemność	przepustowość	rok
single data rate				
SDR SDRAM	3.3 V	512 MB	533-1066 MB/s	1996
double data rate				
DDR SDRAM:	2.5 V	1 GB	1.6-3.2 GB/s	2000
DDR2 SDRAM	1.8 V	4 GB	3.2-6.4 GB/s	2003
DDR3 SDRAM	1.5 V	8 GB	6.4-19.2 GB/s	2007
DDR4 SDRAM	1.2 V	16 GB	12.8-25.6 GB/s	2012
DDR5 SDRAM	1.1 V	64 GB	25.6-64 GB/s	2020

$$\text{moc} = \text{pojemność} \times \text{napięcie}^2 \times \text{częstotliwość}$$

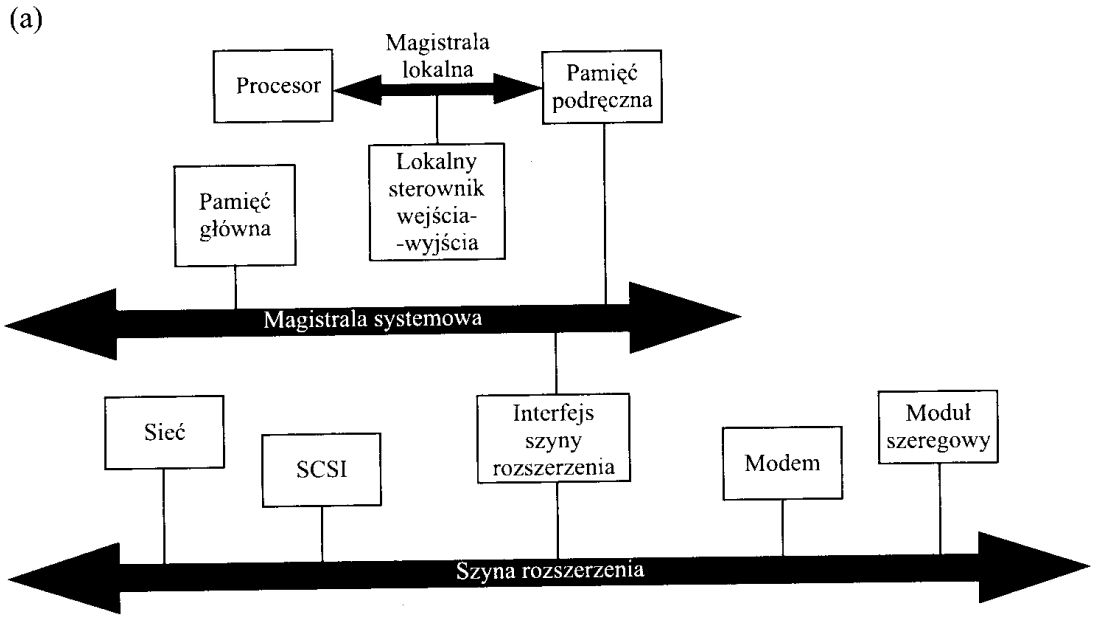
DDR Generations: Memory Density and Speed

Rodzaje pamięci półprzewodnikowych nieulotnych

- **ROM** (*Read-Only Memory*) pamięć stała – tylko odczyt, zapisywanie w trakcie produkcji, tania i szybka
- **PROM** (*Programmable ROM*) programowalna pamięć jednokrotnego zapisu
- **EPROM** (*Erasable and Programmable ROM*) wymazywalna i programowalna pamięć stała – głównie odczyt, wymazywanie światłem UV, zapisywanie elektryczne
- **pamięć błyskawiczna** (*flash memory*) – wymazywanie elektryczne na poziomie bloku (256 B-16 KB), zapisywanie elektryczne; szybki odczyt, wolniejszy zapis (SSD, pamięci USB, karty pamięci MC, MMC, SM)
- **NVRAM** (*Non-Volatile RAM*) – pamięć typu SRAM/DRAM z baterią podtrzymującą zawartość po odłączeniu zasilania (zastosoanie BIOS)[2]
- **NVDIMM** (*Non-Volatile Dual In-line Memory Module*) – pamięć typu DRAM powiązana z układami pamięci błyskawicznej, co pozwala zachować zawartość pamięci ulotnej po awarii zasilania

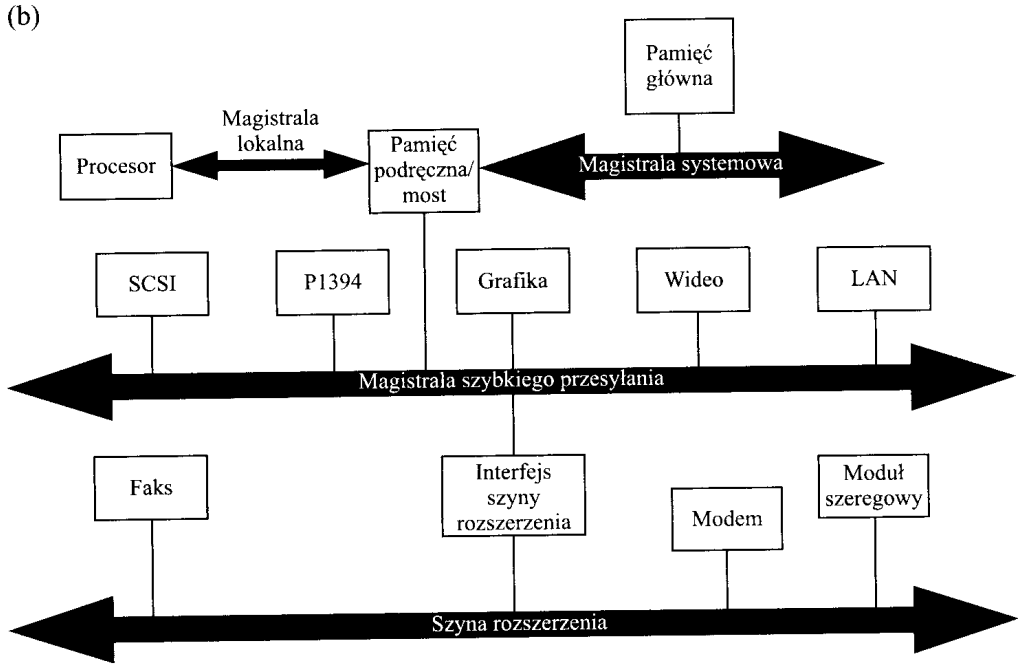
[2] Także EEPROM (*Electrically Erasable and Programmable ROM*) wymazywalna i programowalna pamięć stała (na poziomie bajtu) – głównie odczyt, wymazywanie/zapisywanie elektryczne; szybki odczyt, wolny zapis.

Magistrale (szyny) systemowe



- komunikacja między szyną systemową i szyną rozszerzenia może nastepować bez angażowania CPU

Magistrale (szyny) systemowe



- hierarchiczna magistrala o wysokiej wydajności
- urządzenia o większych wymaganiach są blizej CPU

Magistrale urządzeń

Nazwa	Rok powstania	Aktualna wersja	Przepustowość	Typ / Szerokość linii	Częstotliwość	Zastosowania
ISA	1981	brak	8–16 MB/s	równoległa 8–16 bitów	8 MHz	karty rozszerzeń, modemy, karty dźwiękowe
EISA	1988	brak	33 MB/s	równoległa 32 bity	8.33 MHz	karty rozszerzeń, karty graficzne
PCI	1992	PCI 2.3	533 MB/s	równoległa 32–64 bity	33–66 MHz	karty rozszerzeń, karty graficzne, karty sieciowe
PCIe	2004	PCIe 6.0	256 GB/s (x16)	szeregowa 1, 2, 4, 8, 16 linii	64 GHz	karty graficzne, dyski SSD, karty rozszerzeń
USB	1996	USB4 2.0	10 GB/s	szeregowa 1 para różnicowa	20 GHz	urządzenia peryferyjne, pamięci masowe, urządzenia mobilne
IDE/ATA	1986	ATA/133	133 MB/s	równoległa 16 bitów	133 MHz	dyski twarde, napędy optyczne
AGP	1997	AGP 3.0	2.1 GB/s	równoległa 32 bity	66 MHz	karty graficzne
SATA	2003	SATA III	600 MB/s	szeregowa 1 para różnicowa	6 GHz	dyski twarde, dyski SSD, napędy optyczne
SCSI	1986	SCSI Ultra-640	640 MB/s	równoległa 8-16 bitów	160 MHz	dyski twarde, skanery, serwery
SAS	2004	SAS 4	2.3 GB/s	szeregowa 1 para różnicowa	22.5 GHz	dyski twarde, serwery, pamięci masowe

ISA (*Industry Standard Architecture*, IBM 1980)

- wymaga ręcznej konfiguracja IRQ, adresów I/O oraz kanału DMA

EISA (*Extended ISA*, Gang of Nine 1989)

- rozszerzenie ISA umożliwiające 32-bitowy transfer danych
- adresowanie do 4 GB RAM
- *Plug and Play*, prez problemy z konfliktami IRQ nazywany *plug and pray*

Ograniczenia:

- brak wsparcia w nowoczesnych systemach operacyjnych (np. Windows 10, Linux nie obsługuje ISA natywnie)
- przestarzała, zastąpiona przez PCI.

PCI (*Peripheral Component Interconnect*, Intel 1992)

- obsługuje standard podłącz i używaj (PnP, *Plug and Play*), autokonfiguracja urządzań
- system odpytuje PCI przy starcie o dostępne urządzenia
- każde urządzenie na osobnej szynie z osobnym adresem
- szerokie wsparcie w systemach operacyjnych (Windows, Linux, macOS)
- możliwość użycia przerwań współdzielonych (*IRQ sharing*), co poprawia skalowalność

Ograniczenia:

- szyna współdzielona, ograniczona przepustowość
- ograniczona liczba urządzeń (maksymalnie 5 slotów na mostku PCI, 256 urządzeń w systemie)
- konflikty przerwań (IRQ) w starszych systemach (np. Windows 98)
- popularna w latach 90., zastąpiona przez PCIe.

Magistrala PCI Express

- wysoka przepustowość (do 64 GB/s w wersji 6.0), idealna dla kart graficznych, dysków NVMe i sieciowych kart wysokiej wydajności.
- niski opóźnienia i skalowalność dzięki architekturze *point-to-point*
- każde urządzenie jest połączone bezpośrednio z kontrolerem
- wsparcie dla *hot-plugging* (podłączania urządzeń „na gorąco")
- pełna kompatybilność z nowoczesnymi systemami operacyjnymi
- obsługa wielu linii (x1, x4, x8, x16), zależnie do potrzeb urządzenia
- zastępuje PCI i AGP (Advanced Graphics Port, PCI dla kart graficznych)
- brak linii przerwań IRQ, używa sygnałów MSI (Message Signaled Interrupts)

Wady i problemy:

- wyższy koszt implementacji w porównaniu do PCI
- wymaga nowoczesnych sterowników, co może powodować problemy z kompatybilnością w starszych systemach

Uniwersalna szyna szeregowa (*Universal Serial Bus*, USB, 1995)

- standard szyny zewnętrznej do podłączania do komputera do 127 urządzeń peryferyjnych (jeden IRQ)
- *Plug and Play* — automatyczna detekcja i konfiguracja urządzeń
- *hot plugging* - podłączenie nie wymaga wyłaczenia zasilania
- łatwość rozmnażania portów i wydłużania połączenia poprzez zastosowanie maksymalnie pięciu koncentratorów (*USB hubs*),
- załącze uniwersalne, wsparcei szerokiej gamy urządzań (klawiatura, mysz, drukarki, skanery, kamery wideo, dyski)
- szeroka kompatybilność z systemami operacyjnymi (Windows, Linux, macOS, Android)

Ograniczenia:

- wymaga obecności dokładnie jednego kontolera po stronie hosta (niemożliwe podłączenie dwóch komputerów)

IDE (*Integrated Drive Electronics*, 1986) właściwie **ATA** (*Advanced Technology Attachement*), od 2003 – **PATA** (*Parallel ATA*)

- szyna do łączenia dysków HDD i napędow CDROM (40 pinów)
- MTBF $\approx 1.2 \times 10^6$ h [3] (prawd. awarii dysku w czasie roku $\frac{24h \cdot 356}{MRFB} \approx 7\%$)
- zastąpiony przez SATA

Ograniczenia:

- niska przepustowość (do 133 MB/s w ATA/133), co ogranicza wydajność nowoczesnych dysków.
- bak wsparcia dla *hot-plugging*
- ograniczona liczba urządzeń, każdy sterownik IDE potrzebuje IRQ i może obsłużyć 2 urządzenia wewnętrzne (*master* i *slave*)
- brak wsparcia w nowoczesnych systemach operacyjnych (wymagany tryb kompatybilności lub emulacja)

[3] MTBF (*Mean Time Between Failures*) – czas po jakim z pewnej puli urządzeń zostaje połowa sprawnych. Z 1000 dysków o MTBF 1.2×10^6 h będzie się psuł jeden co (średnio) $\frac{MTFB}{24h \cdot 1000} = 50$ dni.

Szeregowy ATA (*Serial ATA*, SATA)

- kolejkowanie zadań w celu minimalizacji liczby skosków głowicy
- powielacze portów - możliwość podłoczęnia SATA do wielu urządzeń
- wyznacznik portu - mozliwość podłączenia dwóch portów do tego samego SATA (nadmiarowa ścieżka)
- połączenia punkt-punkt
- możliwość podłączania wewnętrzych i zewnętrznych urządzeń
- CRC (*Cyclic Redundancy Check*) dla pakietów danych, rozkazów i statusu
- łatwość przyłączenia (wsparcie dla *hot swapping* - wymiana urządzenia bez rerestaru systemu)
- Szerokie wsparcie w systemach operacyjnych (Windows, Linux, macOS).
- MTBF $\approx 2.5 \times 10^6$ h

SCSI (*Small Computer Systems Interface*)

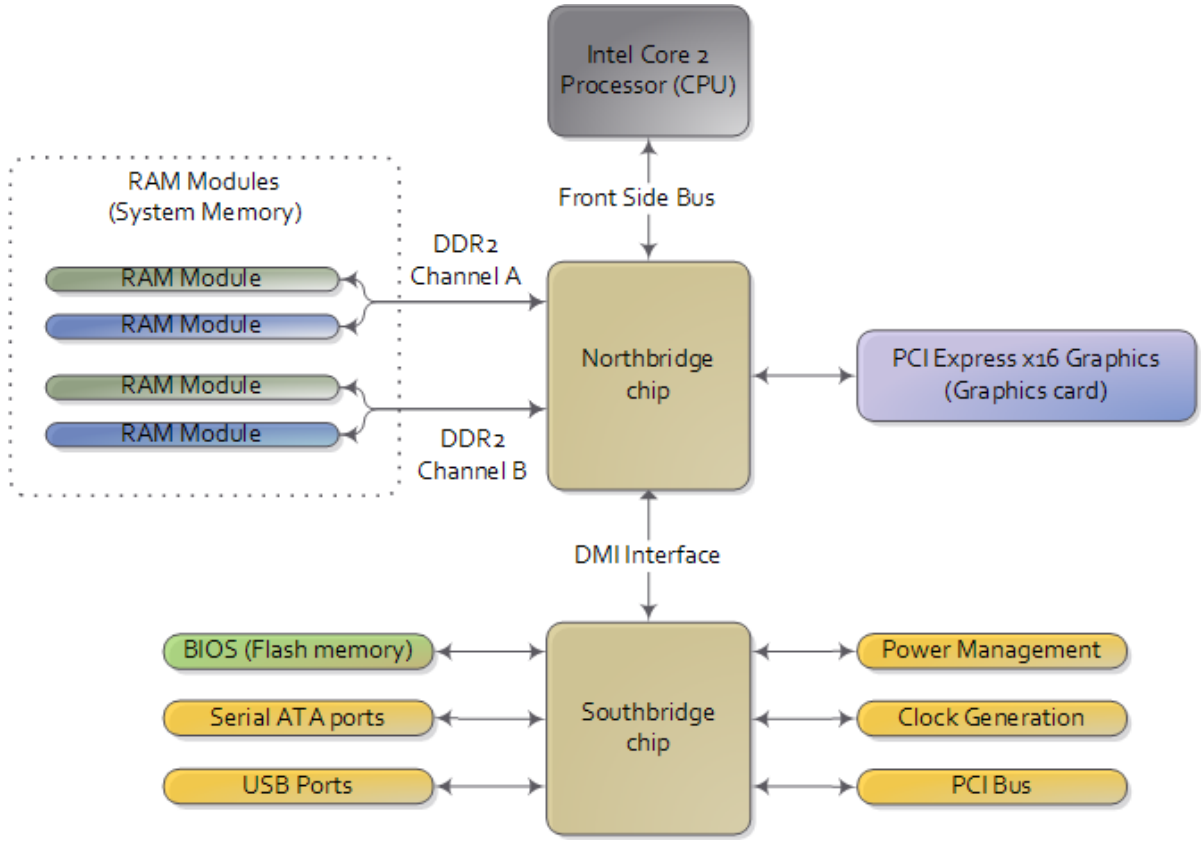
- wysoka wydajność i niezawodność, szczególnie dla stacji roboczych i serwerów (odpowiednik ATA w PC ale mniej obciążający CPU)
- jeden IRQ, obsługa do 16 urządzeń (w tym sterownik), łącze wielopunktowe (*multidrop*) dyski, napędy CD-ROM, napędy taśmowe (*streamer*), skanery
- maksymalna długość do 25 m
- możliwość podłączania urządzeń o różnej prędkości na tym samym łańcuchu.
- MTBF $\approx 1.6 \times 10^6$ h

https://en.wikipedia.org/wiki/Parallel_SCSI

SAS (*Serial Attached SCSI*)

- szeregowa szyna, zastąpiła SCSI
- jeden IRQ, połączenie punkt-punkt (*initiator-target*), tryb pełnego dupleksu
- zastosowanie ekspanderów (*expander*) daje możliwość podłączenia do 65535 urządzeń
- MTBF $\approx 1.6 \times 10^6$ h

Architektura płyty głównej



G. Duarte http://duartes.org/gustavo/blog/post/motherboard-chipsets-memory-map

Chipset

- **Front Side Bus** - magistrala wyjściowa procesora
  Komunikacja procesora z resztą świata:
  - adresy pamięci RAM
  - adresy I/O mapowane na adresy pamięci (Memory Mapped I/O)
  - przerwania i sygnały
- **mostek północny** - łączy CPU z urządzeniami dużej szybkości: RAM, GPU, PCIe, Gigabit Ethenet
- **mostek południowy** - współpraca z pozostałymi urządzeniami ICH (I/O Controller Hub) Intel, FCH (Fusion CH) AMD
- elementy chipsetu: sterownik CPU, sterownik DRAM, sterownik cache, sterownik przerwań, sterownik DMA, sterownik magistrali,
- mostek północny obecnie często zintegrowany z południowym lub nawet z CPU