25. Start počítače, operační systém a jeho zaveden

Inicializace procesoru signálem Reset nebo jeho restart

Po stistku tlačítka napájení u osobního počítače:
Stisknutím tlačítka napájení odešle PSU signál základní desce skládající se z jedniček. Ta mu ho zase odešle zpět a po jeho obdržení PSU, začne okamžitě procházet elektrický proud celým systémem.
Čítač/časovač začne posílat procesoru resetovací příkaz (tím je zajištěno resetování nebo i vypnutí počítače v případě přetížení, kolísavého napětí nebo přehřátí zdroje).
Po skončení všech interních testů, kdy je proud dodáván všemi součástmi a je stabilizováno vstupní napětí, začne odesílat zdroj přes port P8 pin 1 čítači na základní desce +5V signál nazývaný POWER GOOD (někde POWER_OK či POK) s přípustnou tolerancí od +2,4V do +6,0V (patrně logika TTL). Doba mezi vlastním zapnutím počítače a prvním odesláním POWER_GOOD je většinou v rozmezí od 0,1 do 0,5 sekundy.

Na začátku rutiny BIOS zkontroluje sám sebe pomocí kontrolního součtu. Následně se spustí kontrola dat uložených na CMOS paměti (později EEPROM, u nejnovějších FLASH), přičemž na ní proběhne zároveň test zápisu/čtení. Jedná se o malou oblast paměti (64-256 bajtů), napájenou z malé baterky umístěné na základní desce.

Nyní proběhne kontrola technických prostředků počítače, informace o jejich konfiguraci jsou zjišťovány z propojek na základní desce počítače nebo z paměti CMOS. Nastavení jsou postupně konfrontována se skutečností. Tomuto procesoru se obecně říká POST.

Nastane vnitřní příprava procesoru a inicializace základních zařízení. Prvních 16 záznamů v tabulce vektorů přerušení se naplní ukazateli na přerušovací rutiny služeb (ISRs) se sídlem v BIOS ROM. Proběhne test přechodu do chráněného režimu a zpět. Maskovatelná přerušení jsou od teď zapnuta, aby bylo možné zachytávat a zpracovat přerušení dalších zařízení, neboť se budou zpracovávat BIOSy jiných zařízení.

Provede se tedy test systémového řadiče, řadiče paměti a řadiče I/O obvodů, obvodu přímého přístupu do paměti (DMA), časovači systému a programovatelného periferního rozhraní a nakonec ověření prvních 64 kB paměti (tu pak BIOS používá jako pracovní oblast). Případné chyby jsou interpretovány pomocí zvukových signálů ze speakru počítače, známé jako beep kódy.

počáteční nastavení registrů

Při zapnutí napájení RC člen, způsobí, že napájení naběhne plynule (to je pro procesor důležité, protože když napětí se dostane přes nějakou hodnotu tak proběhne jeho vnitřní reset). Takže RESET je připnutí RC článku na chvíli, co způsobí, že jeho registry se nastaví do počátečního stavu (u resetu se nevypne zdroj)
Registr DX obsahuje typ procesoru zakódovaní do čísla
Registr AX obsahuje 0, když test proběhl v pořádku a pokud ne, tak obsahuje kód chyby

POST (Power On Self Test)

Jedná se o diagnostický program, který kontroluje hardware v zařízení a zároveň i jejich činnost. Spouští se automaticky po startu přístroje.

Jeho průběh začíná obvykle inicializací a konfigurací procesoru a následným spuštěním série testů ke zjištění, zda počítačový hardware pracuje správně. Případné chyby zjištěné v průběhu testu jsou uloženy nebo oznámeny prostřednictvím vizuálních (blikání LED nebo zobrazením textu na displeji) nebo zvukových prostředků (série pípnutí – tzv. beep kód). Po dokončení je řízení předáno bootovací sekvenci volající ovládací software, nebo zavaděč operačního systému.

POST se vyvinul z přímočarého jednoduchého procesu na poměrně složitý a spletitý. Je to dáno obrovským množstvím hardware a dalších standardů, který musí podporovat. Průměrný uživatel má tak povědomí o průběhu POSTu na osobních počítačích buď pouze prostřednictvím jednoduchých zpráv zobrazených v textovém režimu ihned po startu počítače, nebo je skryt za grafickým logem výrobce základní desky (je tu však možnost v Setupu BIOSu přepnout do textového režimu).

POST se skládá z první a druhé fáze u osobních počítačů (U platformy MAC je to dosti neznámé kvůli uzavřenosti systému)
V první fázi proběhne kontrola technických prostředků počítače a informace o jejich konfiguraci.
V druhé fázi se zobrazují informace o výrobci, znak BIOS,číslo verze.
Poté se zkontroluje, zda zařízení uvedená v paměti existují a fungují správně a blíže se idenfitikují.Kontruleje se procesor po nastavení v první části, paměti, jenž mohou uvádět větší hodnotu než jaká je skutečně nainstalovaná.Kontrolují se také buňky v ram paměti.

BIOS(Basic Input Output System)

Implementuje základní vstupně–výstupní funkce pro počítače IBM PC kompatibilní a představuje vlastně firmware pro osobní počítače.

Programový kód BIOSu je uložen na základní desce v nevolatilní (stálé) paměti typu ROM, EEPROM nebo modernější flash paměti s možností jednoduché aktualizace (anglicky update).

Původní IBM PC BIOS byl uložen v paměti ROM (pouze pro čtení), která byla zasunuta do soketu v základní desce a oprava BIOSu byla možná pouze výměnou ROM čipu. Protože to bylo nepraktické, začala se používat pro BIOS paměť EEPROM, kterou bylo možné přeprogramovat (změnit její obsah) tak, že byla vyjmuta z patice a přeprogramována ve speciálním zařízení. Kolem roku 1995 se začaly používat flash paměti, které lze přeprogramovat bez vyjmutí ze základní desky. Důvodem změn BIOSu byly zejména změny v hardwaru (nové procesory).

Flashování BIOSu

V moderních počítačích je BIOS uložen v přepisovatelné paměti, což umožňuje obsah přepsat nebo nahradit. To lze provést pomocí speciálního programu, který bývá obvykle poskytovaný výrobcem systému, nebo v POSTU, s uložením na pevný disk nebo USB flash disk. Soubor obsahuje takzvaný "image BIOS„ při kterém může být BIOS přepsán, aby mohlo být provedené vylepšení, které zajistí nové verzi opravit chyby a poskytnout větší výkon, nebo na podporu novějšího hardwaru a také může sloužit k opravě poškozeného BIOSu.

UEFI(Unified Extensible Firmware Interface)

Jedná se o náhradu zastaralého firmwarového rozhraní BIOS.
UEFI je nový standard, který je oficiálně zaváděn z několika důvodů. Prvním a nejdůležitějším důvodem je podpora Secure boot (viz dále). Druhým důvodem je využití schopností nových procesorů a ukončení zpětné kompatibility s 16bitovými procesory 8086, které byly v prvních IBM PC kompatibilních počítačích. Třetím důvodem pak je podpora GPT, která umožňuje zavést operační systém z diskových oddílů (resp. pevných disků) větších než 2 TiB (což je limit původního MBR).

Přesto má UEFI kritické bezpečnostní problémy, obsahuje zadní vrátka.

Počítače, které jsou chráněny secure bootem, mohou zavést jen „certifikovaný“ operační systém, což působí problémy zejména alternativním systémům, jako je Linux. Proto Linux Foundation vytvořila vlastní UEFI Secure Boot system, který secure boot obchází.

Secure Boot

Secure boot je metoda, která umožňuje zajistit start počítače tak, že jsou použity jen „certifikované softwarové komponenty“. Fakticky jde o to, že při startu počítače jsou při zavádění do paměti kontrolovány elektronické podpisy (veřejný klíč musí být uložen v čipu UEFI nebo TPM), kterými musí být podepsán zavaděč, jádro systému, jaderné softwarové moduly a podobně (v Linuxu musí být například podobně chráněna i funkce kexec).

Rozdíl mezi BIOS a UEFI

UEFI jo kompletne přepracovaný BIOS, je 64bitový a mimo jiné se používá úplně nový zavaděč operačního systému.
Pokud spustíme počítač vybavený UEFI či pouze BIOSem, v obou případech probíhá spuštění stejně. BIOS nebo UEFI se načte z paměti (ROM, EEPROM nebo modernější flash). Proběhne kontrola hardware a následně zavedení firmware základních ovladačů.

Bootování už ale probíhá odlišně. Zatím co u klasického BIOSu je vyhledán a spuštěn ve spouštěcím sektoru systémového disku zavaděč operačního systému (často tedy boot manager Windows), tak UEFI má již vlastní zavaděč operačního systému, do kterého jsou uloženy boot managery operačních systémů. Tomuto zavaděči je na disku vyhrazena vlastní partition. Tedy oddíl, který je naformátovaný souborovým systémem FAT 32.

SetUp

Při bootování počítače se nám ukáže logo výrobce a máme na výběr uvedeným stiskem klávesy vybrat možnost nastavení.Např. Testování paměti/systému,vybrání bootovacího média,Nastavení v BIOSU.Toto nastavení nám umožňuje např. pozměnit:
- Taktování procesoru
- Povolení virtualizace
- Nastavení napěti na operačních pamětech
- Povolení/zablokování portů na základní desce

Jsme schopni dosti pozměnit konfiguraci systému a díky UEFI vytvářet profily přetaktování a chladících postupů.

MBR(Master Boot Record)

Je hlavní spouštěcí záznam, který je umístěn v prvním sektoru pevného disku (nebo obdobného média), tedy na jeho úplném začátku. Jeho velikost je 512 bajtů a je v něm umístěn:
- zavaděč operačního systému, kterému BIOS předává při startu počítače řízení
- partition table na logické části (oddíly)
- číselný identifikátor disku

MBR dokáže adresovat maximálně 2 TB disky. Jeho nástupcem je GPT, což je součást UEFI standardu.

Boot sektor

```
je vyhrazený oddíl nebo oblast v pevném disku, diskety nebo jiného podobného zařízení, obsahující krátký a pro běžné uživatele nepřístupný program pro zavedení operačního systému. Zpřístupní se pouze po zavedení do počítače jako bootovací mechanismus a provede se reboot.

Na počítačích kompatibilních s IBM vybere BIOS spouštěcí zařízení, poté z něj zkopíruje první sektor (což může být MBR, VBR nebo jakýkoli spustitelný kód) na adresu 0x7C00.

Termín Bootblock je také používaný pro označení zvláštního druhu malých programů, obvykle spouštěných po zapnutí nebo restartu počítače z energeticky nezávislých pamětí jako je Flash ROM. Po skončení restartu se CPU a hardware dostane do přednastaveného stavu a kód se spustí. Zaváděcí program je obvykle úplně první program, který CPU provádí. Vzhledem k této skutečnosti, Flash ROM (zejména NOR Flash) má často zvláštní sektory speciálně určené pro uchování tohoto typu programů. Tyto sektory se často nazývají Boot sektory, ale tento pojem spíše označuje určitý druh sektorů, které mají lepší hardwarovou ochranu proti náhodnému smazání a přepsání, aby se zamezilo situacím kdy selže zavádění operačního systému na samém začátku zaváděcí sekvence.
```

Windows

```
Jedná se o několik operačních systémů od firmy Microsoft. Všechy mají grafické uživatelské rozhraní, avšak liší se použitým jádrem systému, úrovni podpory multitaskingu (současného běhu více úloh najednou) i používanými knihovnami a účelem použití.
```

Windows 7

```
Jedná se operační systém uveden na trh v roce 2009.
Tento systém byl snad nejvíce populární ze všech windows v této době.Napravil reputaci Windows Vista.
Systém při vydání poskytoval zpětnou kompatibilitu s existujícími ovladači, hardwarem a aplikacemi.
```

Windows 10

```
Jedná se současně o nejnovější operační systém od Microsoftu, který byl vydán v roce 2015. Zavádí jednotné uživatelské prostředí pro různé platformy(stolní počítače, notebooky, tablety, chyté telefony, Xbox)
Jako vždy microsoft nabízí několik edic kde každá dává jinou funkčnost např. Pro má funkce vzdálené plochy a přidává AD a Azure Active Directory.
```

macOS

Systém Mac OS byl uveden s prvním počítačem Macintosh v roce 1984. Aktuální verze macOSu je 11.0 s kódovým označením Big Sur představená 12. listopadu 2020.

MacOS je operační systém vydávaný společností Apple na jejich počítače. Jedná se o uzavřený systém kde se dbá na uzavřenost a bezpečnost systému. Systém je založen BSD a ne na linuxu jak bývá obvykle řečeno.

Systém kombinuje jednoduchost a možnost pracovat efektivně díky zaměřenosti na přirozenost UI.Je těžké se dostat do HW nebo nastavovat něco kam systém uživatelským rozhraním přímo nepustí.
Nedostaneme se k ovladačům nebo nastavením komponent jako v Linuxu nebo Windows.Proto většina vývojářům tato platforma nesedí.Na druhou stranu měl MacOS vždy ty nejlepší video editující software a audio-vizuální tvorba na něm byla bezchybná.

Linux

Jedná se o svobodný a otevřený počítačový operační systém, který je založen na linuxovém jádru. Linuxové systémy jsou šířeny v podobě distribucí, které je možné nainstalovat nebo používat bez instalace.Používané licence umožňují systém zdarma a velmi volně používat, distribuovat i upravovat. Tím se odlišuje od proprietárních systémů.

Operační systém Linux používá Linux kernel, který vychází z myšlenek Unixu a respektuje příslušné standardy POSIX a Single UNIX Specification.

Jádro Linuxu umožňuje spouštět více programů (úloh) najednou. Každý program se může skládat z jednoho nebo více procesů, tedy se jedná o víceúlohový systém. Každý proces potom může mít jeden nebo více podprocesů. Operační systémy, které umožňují běh více procesů, nebo dokonce podprocesů současně, jsou schopny využít i vícejádrové a víceprocesorové počítače a výrazně zefektivnit práci uživatele. Jádro Linuxu je víceuživatelské, takže umožňuje spouštět programy různých uživatelů, například jeden uživatel může obsluhovat počítač přímo, zatímco další mohou obsluhovat stejný počítač například přes síť nebo dokonce Internet. Příslušné uživatelské účty jsou před neoprávněným přístupem chráněny autentizací, například jménem a heslem. Uživatelé mají přidělena různá práva, od naprosté kontroly nad systémem, kterou má obvykle správce (root), až do různé míry omezené účty uživatelů.

V současné době je označením Linux míněno nejen jádro operačního systému, ale zahrnuje do něj též veškeré programové vybavení (software), které uživatelé používají (tj. aplikace, utility, grafické uživatelské rozhraní apod.) i přesto, že je vyvíjeno nezávisle na samotném jádře Linuxu. Linux je šířen v podobě linuxových distribucí, které obsahují jak zmíněné jádro, tak zmíněný doplňující software v takové formě, která usnadňuje jeho instalaci a používání (instalace někdy není nutná, viz Live CD).