Hardver minőségbiztosítás

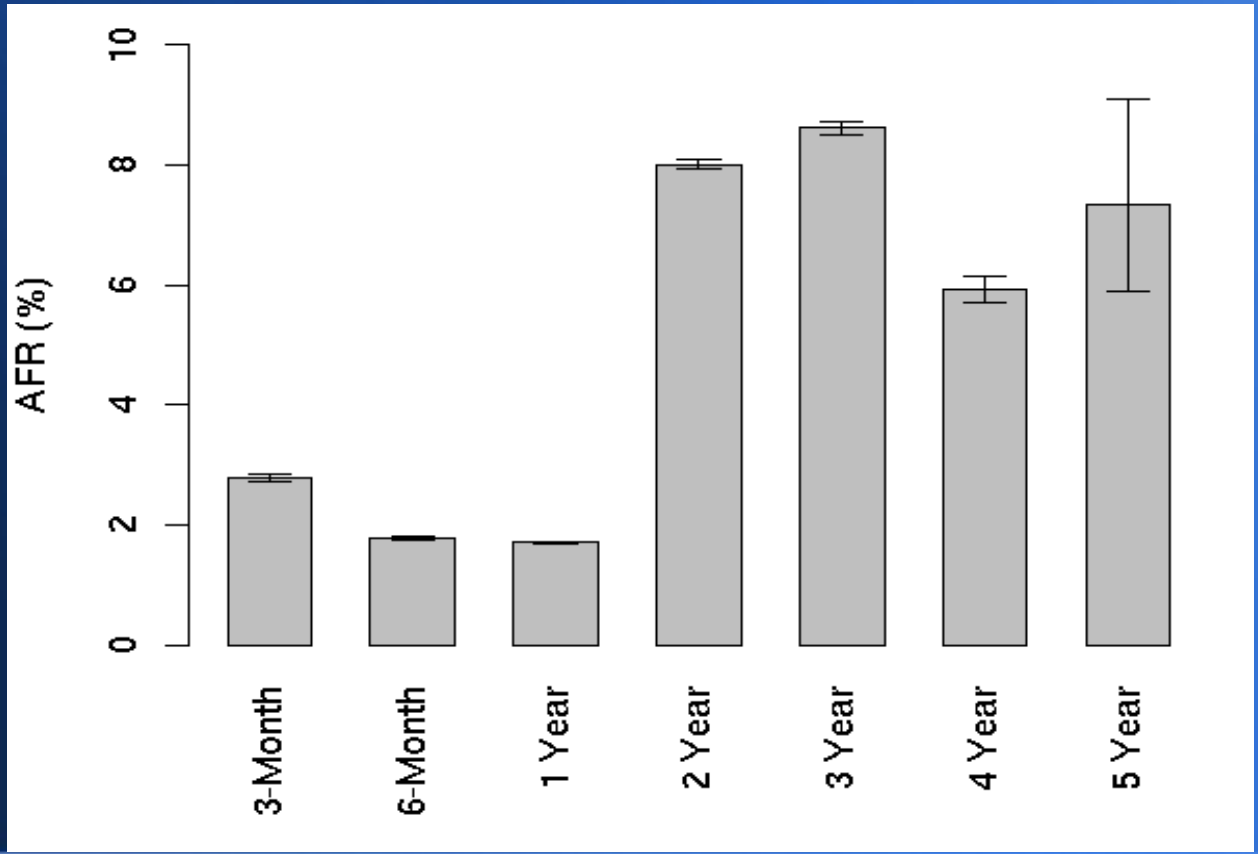
Benkocs Norbert Attila
2012 február 29.

Miről lesz szó?

- Hardvereszközökben előforduló gyakoribb problémák
  - Hardveres megoldások és védelmek
  - Szoftveres megoldások

Storage: HDD

- Legfontosabb elem (ez tárolja minden adatunkat)
- Nagy hibaarány



HDD Hibák

- Szektorszinten (olvasási hibák esetére): ECC (Error Correcting Code)
- Ha ECC-vel nem javítható → hibás szektor → tartalék szektorok (spare sectors)
- HDD és vezérlő közt: CRC
- Monitoring: SMART (Self-Monitoring, Analysis and Reporting Technology)
    - Nem minden esetben megbízható :(

SSD

- Solid-state drive – flash alapú
- Nincsenek mozgó alkatrészek (HDD esetén a hibák 70%-a mechanikai hiba)
- Gyors (random) read

SSD Hibák

- HDD-hez képest sokkal könnyebben megjósolhatóak a hibák
- Wearout: NAND celláknak korlátozott írási ciklusa van (kb. 100,000 – 1,000,000)
- Bitszintű hibák → FEC
- Szektorszintű hibák → spare sectors
- Write cache problémák

Storage megoldások

- Több HDD/SSD → RAID (redundant array of independent disks)
  - Összefűzés (RAID 0), Tükrözés (RAID 1), Paritással (RAID 5)
  - Ezek kombinációi (RAID 10, 50, …)
  - HW vezérlő / SW
  - Battery backup (write cache miatt)

Storage megoldások

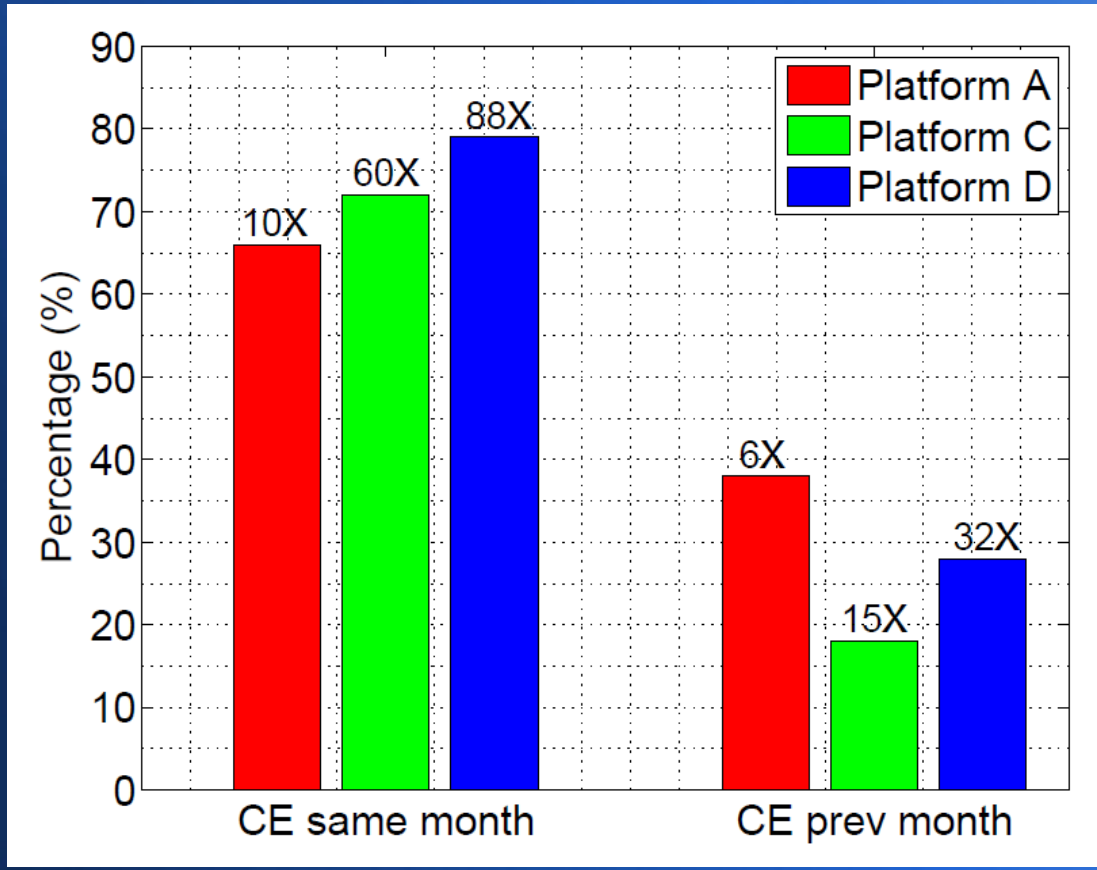
- NAS/SAN (Network Attached Storage / Storage Area Network)
  - NAS: fájlrendszer szintű (NFS, SMB)
  - SAN: blokkszintű (ATA over Ethernet, iSCSI)
  - Az adatok más gépen / eszköz(ök)ön helyezkednek el

RAM

- Hibák javítása/detektálása: ECC
- Correctable errors: ECC-vel javítható
- Uncorrectable errors: ECC-vel detektálható, de nem javítható → app crash!
- CE után ajánlott a RAM csere

RAM

- Google: a DRAM modulok 8%-ában keletkezik hiba 1 év alatt



RAM érdekességek

- RAM mirroring: Két RAM modul tartalmazza ugyanazt az adatot; uncorrectable error esetén is megvan az adat („RAID 1 for RAM”)
  - Tükrözött RAM pár akármelyike eltávolítható (hot-swapping)

CPU feature-ök

- Virtualizáció
- Szoftverhibák esetére:
  - MMU/MPU (Memory Protection Unit)
  - Privilégiumszintek

Virtualizáció

- Több guest OS futtatása egy rendszeren
  - Az OS-ek teljesen függetlenek, egymásról nem tudnak / egymás működését nem tudják zavarni
- Szoftverhibák elleni védelem: kernel/OS összeomlás
- Biztonság: szolgáltatások izolációja

MMU/Privilégiumok

- Egyik legalapvetőbb védelmi mechanizmus
- Programok (processzek) egymástól való izolációja
    - Egymás memóriáját ne tudják piszkálni
- Bizonyos műveleteket (pl. hardver elérése) csak az OS végezhet

CPU hibák

- A hardver nem hibátlan, tervezési hibák becsúsznak
- Főleg a processzort érinti (de nem csak azt), az a legbonyolultabb
- Intel i7 sorozat: ~153 dokumentált bug
- TI OMAP: ~212 dokumentált bug

Pár jelentősebb hiba

- Pentium FDIV bug: lebegőpontos osztás hibás eredményt adhatott :)
- Pentium „F00F” bug: CPU deadlock
- AMD L3 cache TLB bug: Memory corruption

Köszönöm a figyelmet!