

INFORMATIKAI RENDSZEREK MŰKÖDÉSI BIZTONSÁGA

Kürti Sándor

vezérgazgató, KÜRT Computer Rt. – sandor.kurti@kurt.hu

Neumann János az emberi agy működésének modellezésével kapcsolatban, a Yale egyetemi előadásaihoz 1956-ban írt jegyzetében¹ az idegsejtek és az agy együttműködéséről a következőket írja: „Az élő szervezet komplexitásának egyik fontos következménye, hogy a legkülönbözőbb környezeti feltételek között is rendkívül megbízható módon működik annak ellenére, hogy a szerkezeti elemek önmagukban rendkívül megbízhatatlanok.”

E felismerés után közel ötven évvel elértük, hogy az informatikai ipar már tömegméretekben képes előállítani rendkívül megbízhatatlan működésű szerkezeti elemeket, ám az élő szervezet által biztosított megbízható hálózati működést ezekkel az elemekkel még nem sikerült modelleznünk.

E meghökkenítő bevezetéssel mindössze az a célom, hogy az Olvasót a továbbiakban együttgondolkodásra készítsem arról a tudomány- és gazdaságtörténeti kérdésről, hogy hogyan sáfárkodtunk Neumann hagyatékával az informatikai rendszerek biztonsága szempontjából. Induljunk ki Neumann

János és Hermann Heine Goldstine, a számítógépek konstrukciós elvére vonatkozó, 1947-ben tett esszenciális megállapításaiból:

- Szükség van egy párhuzamos működésű memóriaegységre. A memóriaegységnek mind számokat, mind pedig utasításokat tárolni kell tudnia.

- Szükség van egy vezérlőegységre, amely különbséget tud tenni számok és utasítások között; az utasításokat interpretálni tudja, és emberi beavatkozás nélkül különböző utasítások végrehajtását tudja vezérelni.

- Szükség van egy párhuzamos működésű aritmetikai egységre, amely bináris rendszerű összeadásra, kivonásra, szorzásra és osztásra alkalmas.

- Szükség van egy olyan kimenő-beemenő egységre, amely át tudja hidalni a gép gyors memóriaegysége és a lassú emberi memória közötti sebességkülönbséget.²

Figyelembe véve azt a tényt, hogy ezek a megállapítások akkor születtek, amikor még csak egyetlen elektronikus elv alapján műkö-

¹ Az egyetemi jegyzet *A számítógép és az agy* címet kapta (*The Computer and the Brain*. Yale University Press, 1959, magyar kiadás: *A számítógép és az agy*. Gondolat, Budapest, 1964). A *számítógép* megnevezést itt, és a továbbiakban kizárólag az elektronikus, digitális jelfeldolgozással működő számítógépek meghatározására használom, tudva, hogy léteznek analóg számítógépek, és figyelembe véve azt a tényt is, hogy Szalay Sándor, aki először fordította magyarrá a *computer* szót, ezekre az eszközökre még a *számológép* megnevezést alkalmazta.

² Az első, valóban elektronikus kivitelű számológép az ENIAC (Electronic Numerical Integrator and Calculator) volt. Építése 1943-tól 1946-ig tartott. 1956-ban – noha kifogástalanul működött – lebontották. Az ENIAC sikere arra indította a vezető katonai köröket (az ENIAC elsősorban lőtáblák kiszámítására szolgált), hogy megbízást adjanak azoknak az elvi problémáknak a tanulmányozására, amelyek a numerikus számítások elektronikus eszközökkel való elvégzésénél felmerülnek. A vizsgálatokat Neumann János és Hermann Heine Goldstine végezték el: eredményeik 1947-ben, illetve 1948-ban bizalmas jelentés formájában kerültek zártkörű publikációra.

dő számítógép létezett (amely viszont nem az itt leírt architektúrával rendelkezett), és tudva, hogy ezek a mondatok ma is helytállóak, amikor több tízmillió számítógép van használatban, a legkevesebb, amit megállapíthatunk, hogy a két tudós meghatározása telitalálat volt.

Ugyanakkor az elmúlt időszakban, elsősorban a vírusok, a hackerek és az évezredváltás, az Y2K világméretű problémája kapcsán mind gyakrabban vetődött fel az a kérdés, hogy nem lett volna-e időszzerű ezeken az alapelveken változtatni?

A probléma lényegére rávilágítva: ha kizárólag a vezérlőegységben dől el egy hieroglifasorozatról, hogy utasítást rejt-e magában, amelyet végre kell hajtani, vagy adatok vannak benne, amelyek az utasításnak a tartalmát határozzák meg, akkor egyszerűen nincs esély a nemkívánatos utasítás vagy nemkívánatos adat kiszűrésére a rendszerből. Mintha egy bankban a nyitott trezor előtt dőlne el, hogy aki éppen odakerült, az mit tegyen és mennyi pénzzel.

A 80-as évek elejéig az informatika a Neumann-Goldstine-elvekkel teljes összhangban fejlődött. Az informatikai kutatás-fejlesztés, a kísérleti gyártás, a gyártás és minőségbiztosítás, valamint az értékesítés – a klasszikus iparágakban kialakult normák, szabványok szerint – az elektronikai ipar égése alatt történt, a fent felsorolt architektúraelemek magas minőségi színvonalú fejlesztésével, előállításával.

A „forradalmi” változást a személyi számítógép (personal computer – PC) megjelenése és a számítógépek hálózatba kötésének lehetősége jelentette. Neumann fogalmai között a „hálózat” mint az agyi idegsejtek hálózata, s ennek a *számítógépen belüli* modellezése jelenik meg. A 80-as évekre realitása lett annak, hogy a „hálózat” kikerüljön a számítógépből, és számítógépek közötti összeköttetést valósítsa meg, mely összekötéssel teljesen új tudományos és műszaki lehetőségek nyíltak meg az informatika területén.

Igazán forradalminak az új helyzet gazdasági kezelését nevezhetjük. Az a tőke, amelyik megértette a személyi számítógép lényegét – azt, hogy ez az eszköz nemre és korra való tekintet nélkül mindenkit érinteni fog –, az igen gyorsan, földrajzilag igen koncentráltan, óriási, eddig soha nem látott hatalomra tett szert. Ez a tőke elég erősnek bizonyult ahhoz, hogy elvesse a termékek előállításának klasszikus rendszerét (kutatás-fejlesztés, kísérleti gyártás, gyártás és minőségbiztosítás...), és elfogadtasson a világgal egy új termékelőállítási rendszert, melyben a vezérlő elv az „olcsó termék” nimbusza. E termék értékesítése lett az igazán forradalmi, hiszen a marketing kommunikációjában az eddigi leghatásosabb, vásárlásra készítő jelmondat jelent meg: „vásárolj, mert ha nem, a világ elmegy melletted”. Persze a termék olcsó is volt, tehát mindenki számára úgy tűnt, hogy nagyon megéri az árát.

Mitől lehetett olcsó? Éppen attól, hogy a kutatás-fejlesztés költségeit lefaragták, a minőségbiztosításra lényegében nem költöttek. Mindenki számára elfogadhatóvá vált az a képtelenség, hogy a termék bármikor elromolhat, és mivel a vásárlót jogi védelem sem illette meg, hiszen szinte minden termék hibás volt, a felhasználók beletörődtek a „kikapcsolom, majd bekapcsolom és működni fog” üzemeltetési mód használatába.

Mindez az érzés a 90-es évek végére alapvetően megváltozott. E rossz minőségű eszközök hálózatba kötésével a hibák egy része kritikussá tette a hálózat működését. A világméretű Y2K probléma például a minőségbiztosítás leegyelembb szabályainak be nem tartására hívta fel a figyelmet. Az informatikai rendszeren belüli dátummeghatározó algoritmusok megtalálása, működési módjának felismerése és esetenkénti kicserélése dollármilliárdokba került. És a számla még nincs teljesen kiegyenlítve, mert ez a probléma a jövőben is bármikor előkerülhet.

Az ebben az időben a már őskövületnek tekintett Neumann-Goldstine-architektúra is a támadások keresztútjába került. A kutatók nagy része kizárólag a szükséges kutatás-fejlesztési befektetések elmaradásának, és nem az architektúra nagyszerűségének tekintette e rendszer fennmaradását.³ A számítógépes vírusok elterjedését is éppen ezen architektúra és a rossz minőségű operációs rendszerek együttes hatásának tulajdonították.

Az informatikai eszközök és az internet világméretű elterjedésével az itt felsorolt minőségi problémák lényegében nem csökkentek, sőt! Mígnem 2000-ben a tőzsde megelégedte az informatikai ipar által festett délibábot, és nagyon komoly figyelmeztetést adott: az informatikai cégek részvényeinek árzuhanása következett be. Mivel a kulcskérdés az informatikai rendszerek működési biztonsága volt, azaz a tőzsde nem hagyott kétséget afelől, hogy a működési biztonságot jelentős mértékben növelni kell, az igazi kérdés az maradt, hogy „mindezt hogyan kéne elfogadtatni a vevővel?”. Mert ez egyet jelentett azzal, hogy vége az olcsó világnak.

Miért? Eddig éppen azért volt olcsó a termék, mert a kutatást, a fejlesztést, a minőséget nem fizették meg, így annak költsége nem is került bele a termék árába. Sőt! Az adott helyzetben a minőség már igen sokba került, mert az ipar elárasztotta a világot gyatra termékekkel, ezeket vagy le kell cserélni, vagy a meglévő termékek köré kell megépíteni a biztonságot. Az informatikai iparág az utóbbi utat választotta.

Ma attól életképesek a Neumann-Goldstine-architektúrájú hardverrel és a „szo-

kásosan” hibás operációs rendszerrel működő együttesek, mert védelmi rendszert építenek köréjük. Ez a védelmi rendszer, mivel eredendően nem része a számítógépnek (ahogy az autónak szerves része a fék, a biztonsági öv, újabban a légszák), újabb minőségi problémát jelent: az egyedi tervezés és a védendő rendszerhez való egyedi illesztés problémáját. E védelmi rendszerek éppen a hardver-szoftver hiányosságok elfedésére hivatottak, mint például az információ-hozzáférést szabályozó rendszerek (tűzfal, behatolásvédelem, vírusvédelem, tartalomszűrés, forgalommenedzselés, titkosító eszközök), vagy az információtárolást biztosító rendszerek (mentő és archiváló rendszerek). E védelmi rendszerek között jelentek meg a közelmúltban az eddig kizárólag önállóan használt kockázatkezelő és a katasztrófa-kezelő rendszerek is.

Összefoglalva, az elmúlt közel ötven évben az informatika ez ezen belül a számítógép fejlődése igen látványos volt, a méretcsökkenés, a kapacitásnövekedés, a számítási sebesség növekedése, az energiafelhasználás csökkenése mind-mind legalább három nagyságrendnyit változott. Ugyanebben az ötven évben viszont a számítógépek architektúrája lényegében változatlan maradt. Ez Neumann János zsenialitásának és az informatikai forradalom hiányosságának együttes következménye. Mivel az informatikai forradalmat a tengerentúlról kezdeményezték és ma is onnan irányítják, nekünk nincs emiatt szégyellnivalónk. Viszont nagyon büszkék lehetünk az informatikai idősámításban örök életűnek tűnő, Neumann János által kidolgozott architektúrára.

³Fóti Marcell *Az iparág hazugsága, avagy Buffer Overrun* című írásában (Byte, 2000, július) veszi górcső alá a Neumann-architektúra őskövület jellegét.

Kulcsszavak: *konstrukciós elv, architektúra, minőségbiztosítás, egyedi tervezés, információ-hozzáférés, védelmi rendszer*