INFORMATIKAI RENDSZEREK MÛKÖDÉSI BIZTONSÁGA

Kürti Sándor
vezérigazgató, KÜRT Computer Rt. – sandor.kurti@kurt.hu

Neumann János az emberi agy mûködésének modellezésével kapcsolatban, a Yale egyetemi elõadásaihoz 1956-ban írt jegyzetében[1] az idegsejtek és az agy együttmûködésérõl a következõket írja: *„Az élõ szervezet komplexitásának egyik fontos következménye, hogy a legkülönbözõbb környezeti feltételek között is rendkívül megbízható módon mûködik annak ellenére, hogy a szerkezeti elemek önmagukban rendkívül megbízhatatlanok.*"

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

E meghökkentõ bevezetéssel mindössze az a célom, hogy az Olvasót a továbbiakban együttgondolkodásra késztessem arról a tudomány- és gazdaságtörténeti kérdésrõl, 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 mûködésû memóriaegységre. A memóriaegységnek mind számokat, mind pedig utasításokat tárolni kell tudnia.*
- *Szükség van egy vezérlõegységre, amely különbséget tud tenni számok és utasítások között; az utasításokat interpretálni tudja, és emberi beavatkozás nélkül különbözõ utasítások végrehajtását tudja vezérelni.*
- *Szükség van egy párhuzamos mûködésû aritmetikai egységre, amely bináris rendszerû összeadásra, kivonásra, szorzásra és osztásra alkalmas.*
- *Szükség van egy olyan kimenõ-bemenõ 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 mûkö-

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

[2] Az elsõ, valóban elektronikus kivitelû számológép az ENIAC (Electronic Numerical Integrator and Calculator) volt. Építése 1943-tól 1946-ig tartott. 1956-ban – noha kifogástalanul mûködött – lebontották. Az ENIAC sikere arra indította a vezetõ katonai köröket (az ENIAC elsõsorban lõtáblák 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 zártkörû publikációra.

dõ 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 idõszakban, elsõsorban a vírusok, a hackerek és az évezredváltás, az Y2K világméretû problémája kapcsán mind gyakrabban vetõdött fel az a kérdés, hogy nem lett volna-e idõszerû ezeken az alapelveken változtatni?

A probléma lényegére rávilágítva: ha kizárólag a vezérlõegységben dõl el egy hieroglifasorozatról, hogy utasítást rejt-e magában, amelyet végre kell hajtani, vagy adatok vannak benne, amelyek az utasításnak a tartalmát határozzák meg, akkor egyszerûen nincs esély a nemkívánatos utasítás vagy nemkívánatos adat kiszûrésére a rendszerbõl. Mintha egy bankban a nyitott trezor elõtt dõlne el, hogy aki éppen odakerült, az mit tegyen és mennyi pénzzel.

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

A „forradalmi" változást a személyi számítógép (personal computer – PC) megjelenése és a számítógépek hálózatba kötésének lehetõsége 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 számítógépbõl, és számítógépek közötti összeköttetést valósítsa meg, mely összekötéssel teljesen új tudományos és mûszaki lehetõségek nyíltak meg az informatika területén.

Igazán forradalminak az új helyzet gazdasági kezelését nevezhetjük. Az a tõke, 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 tõke elég erõsnek bizonyult ahhoz, hogy elvesse a termékek elõállításának klasszikus rendszerét (kutatás-fejlesztés, kísérleti gyártás, gyártás és minõségbiztosítás…), és elfogadtasson a világgal egy új termékelõállítási rendszert, melyben a vezérlõ elv az „olcsó termék" nimbusza. E termék értékesítése lett az igazán forradalmi, hiszen a marketing kommunikációjában az eddigi leghatásosabb, vásárlásra késztetõ jelmondat jelent meg: „vásárolj, mert ha nem, a világ elmegy melletted". Persze a termék olcsó is volt, tehát mindenki számára úgy tûnt, hogy nagyon megéri az árát.

Mitõl lehetett olcsó? Éppen attól, hogy a kutatás-fejlesztés költségeit lefaragták, a minõségbiztosításra 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 beletörõdtek a „kikapcsolom, majd bekapcsolom és mûködni fog" üzemeltetési mód használatába.

Mindez az érzés a 90-es évek végére alapvetõen megváltozott. E rossz minõségû eszközök hálózatba kötésével a hibák egy része kritikussá tette a hálózat mûködését. A világméretû Y2K probléma például a minõségbiztosítás legelemibb szabályainak be nem tartására hívta fel a figyelmet. Az informatikai rendszeren belüli dátummeghatározó algoritmusok megtalálása, mûködési módjának felismerése és esetenkénti kicserélése dollármilliárdokba került. És a számla még nincs teljesen kiegyenlítve, mert ez a probléma a jövõben is bármikor elõkerülhet.

Az ebben az idõben a már õskövületnek tekintett Neumann-Goldstine-architektúra is a támadások kereszttüzébe került. A kutatók nagy része kizárólag a szükséges kutatásfejlesztési befektetések elmaradásának, és nem az architektúra nagyszerûségének tekintette e rendszer fennmaradását.[3] A számítógépes vírusok elterjedését is éppen ezen architektúra és a rossz minõségû operációs rendszerek együttes hatásának tulajdonították.

Az informatikai eszközök és az internet világméretû elterjedésével az itt felsorolt minõségi problémák lényegében nem csökkentek, sõt! Mígnem 2000-ben a tõzsde megelégelte az informatikai ipar által festett délibábot, és nagyon komoly figyelmeztetést adott: az informatikai cégek részvényeinek árzuhanása következett be. Mivel a kulcskérdés az informatikai rendszerek mûködési biztonsága volt, azaz a tõzsde nem hagyott kétséget afelõl, hogy a mûködési biztonságot jelentõs mértékben növelni kell, az igazi kérdés az maradt, hogy „mindezt hogyan kéne elfogadtatni a vevõvel?". Mert ez egyet jelentett azzal, hogy vége az olcsó világnak.

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

Ma attól életképesek a Neumann-Goldstine-architektúrájú hardverrel és a „szokásosan" hibás operációs rendszerrel mûködõ együttesek, mert védelmi rendszert építenek köréjük. Ez a védelmi rendszer, mivel eredendõen nem része a számítógépnek (ahogy az autónak szerves része a fék, a biztonsági öv, újabban a légzsák), újabb minõségi problémát jelent: az egyedi tervezés és a védendõ rendszerhez való egyedi illesztés problémáját. E védelmi rendszerek éppen a hardver-szoftver hiányosságok elfedésére hivatottak, mint például az információ-hozzáférést szabályozó rendszerek (tûzfal, behatolásvédelem, vírusvédelem, tartalomszûrés, forgalommenedzselés, titkosító eszközök), vagy az információtárolást biztosító rendszerek (mentõ és archiváló rendszerek). E védelmi rendszerek között jelentek meg a közelmúltban az eddig kizárólag önállóan használt kockázatkezelõ és a katasztrófakezelõ rendszerek is.

Összefoglalva, az elmúlt közel ötven évben az informatika és ezen belül a számítógép fejlõdése 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 idõszámításban örök életûnek tûnõ, Neumann János által kidolgozott architektúrára.

[3]Fóti Marcell *Az iparág hazugsága, avagy Buffer Overrun* címû írásában (Byte, 2000, július) veszi górcsõ alá a Neumann-architektúra õskövület jellegét.

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