NANCY G. LEVESON

Narratívák hálójában – Rendszerező széljegyzetek egy ígéretesen induló párbeszédhez

Mivel a számítógépek alkalmazása igen gyorsan terjed mindenütt, biztosítani kell, hogy beépítésük a lehető legfelelősségteljesebb módon és olyan ütemben történjék, ami az embereket nem teszi ki szükségtelen kockázatoknak. A technológiai újítások folytán fellépő kockázatok ismertek voltak már jóval a számítógépek megjelenése előtt is: nem most történik meg először, hogy az ember valami olyan különösen hasznos új technológiára tett szert, ami potenciálisan veszélyes lehet. A tanulmány szerzője sokféle olyan érdekes párhuzamot von a nagynyomású gőzgépek korai fejlődési szakasza és a szoftverfejlesztés mai helyzete között, ami alkalmazható a számítógépek komplex rendszerekben való használatára.

Kulcsszavak: *nagynyomású gőzgép, biztonsági szempontból kritikus rendszerek, szoftverbiztonság, szoftverfejlesztés, komplex rendszerek, kockázat-megelőzés*

Szerzői információ:

Nancy G. Leveson
A Washingtoni Egyetem számítógép-tudományi és alkalmazott informatikai tanszékének professzora Seattle-ben. Egy általa megnyitott és úttörőként művelt új kutatási terület, a szoftverbiztonság elismert nemzetközi szaktekintélye, számos nemzetközi és amerikai tudományos társaság tagja. A közelmúltban az űrrepülőgépekben alkalmazott szoftverek biztonságos működésének értékelését vezette. Szakmai munkásságának fő célja – saját megfogalmazása szerint – „a szoftverbiztonság szakterületének fejlesztése, megbízható szoftverek és rendszermérnöki gyakorlat kialakítása mindenütt, ahol az élet- és vagyonbiztonság veszélybe kerülhet”.
E-mail: leveson@cs.washington.edu

Így hivatkozzon erre a cikkre:
Leveson, Nancy G.. „Nagynyomású gőzgépek és számítógép-szoftver”. *Információs Társadalom* VI, 1. szám (2006): 69–90.
https://dx.doi.org/10.22503/inftars.VI.2006.1.9

Nancy G. Leveson*

Nagynyomású gőzgépek és számítógépszoftver

„Egy jelenség tudományos magyarázata a racionális rend mintaszerű kifejeződésének tűnhet, ám ebből nem szabad arra következtetnünk, hogy a magyarázat megtalálása is ennek a rendnek megfelelően történt. A tudomány csak a tények megállapítása után fejezi ki a rendet, előrehaladása közben azonban – különösen az egyes kutatási területek élvonalában – zűrzavaros képet mutat és szenvedélyes viták kereszttüzében áll."

William Ruckelshaus [33, 108]

A számítógépek alkalmazása a potenciálisan veszélyes gépi berendezések ellenőrzésére fokozódó figyelmet váltott ki a szoftverek lehetséges hibái iránt, amelyek esetleg hozzájárulhatnak súlyos balesetek bekövetkezéséhez. A számítógéppel összefüggő balesetek száma – azoknak a korlátozásoknak köszönhetően, amelyeket a biztonsági szempontból kritikus fontosságú vezérlési és ellenőrzési áramkörökben való alkalmazásukkal szemben életbe léptettek – mindeddig csekély volt. Ahogyan azonban egyre szélesebb körben felismerik a számítógépek felhasználásának gazdasági és technológiai előnyeit, alkalmazásuk igen gyorsan terjed mindenütt. Biztosítanunk kell tehát, hogy a számítógépek beépítése a biztonsági szempontból kritikus rendszerekbe a lehető legfelelősségteljesebb módon és olyan ütemben történjék, amely az embereket nem teszi ki szükségtelen kockázatoknak.

A technológiai újítások folytán fellépő kockázatok ismertek voltak már jóval a számítógépek megjelenése előtt is: nem most történik meg először, hogy az ember valami olyan különösen hasznos új technológiára tett szert, amely potenciálisan veszélyes lehet. Mielőtt megismételnénk ugyanazokat a hibákat, amelyeket elődeink elkövettek, tanulhatunk a múltból. Sokféle olyan, számunkra különösen érdekes párhuzam vonható a nagynyomású gőzgépek korai fejlődési szakasza és a szoftverfejlesztés mai helyzete között, amelyek alkalmazhatók a számítógépek komplex rendszerekben való használatára.

A felrobbanó kazánok problémái

„A nagy találmányok sohasem, a nagy felfedezések pedig csak ritkán egyetlen értelem művei. Minden nagy találmány valójában vagy a kisebb találmányok egyfajta aggregátuma, vagy pedig valamilyen előrehaladási folyamat során megtett végső lépés. Nem teremtés, hanem növekedés – éppúgy, mint a fák növekedése az erdőben. Ebből

* Computer Science and Eng. Dept., FR-35. Seattle: University of Washington, WA 98195.

E tanulmány rövidített változata megjelent az *IEEE Computer* 1994. októberi számában. Teljes szövege megnyitó előadásként hangzott el az 1992 májusában Ausztráliában, Melbourne-ben tartott nemzetközi szoftverfejlesztési konferencián *(International Conference on Software Engineering)*, és megjelent a konferencia kiadványában is.

következik, hogy ugyanaz a találmány gyakran különböző országokban egyidejűleg születik meg, több ember munkájának gyümölcseként. Egy-egy fontos találmány gyakran még az előtt bukkan fel, hogy a világ készen állna a befogadására, és a boldogtalan feltaláló – saját kudarca révén – megtanulja, hogy ha valaki megelőzi korát, ez éppolyan szerencsétlenség lehet számára, mint ha lemarad a kortól. A találmányok csak akkor válnak sikeressé, amikor nemcsak szükség van rájuk, hanem az emberiség értelmileg már elég fejlett ahhoz is, hogy szükségességüket felismerve és elismerve azonnal használatba vegye őket.

Robert H. Thurston: *A gőzgép fejlődéstörténete* (*A History of the Growth of the Steam Engine*, 1883)

A gőz erejének felhasználása terén az első ismert kutatások közül több kísérlet az i. e. 60 körül élt alexandriai Hérón* nevéhez fűződik. Csak a 16. és a 17. században került azonban sor arra, hogy a gőzenergia kutatását a bányákba beszivárgó víz kiszivattyúzásának problémája egyfajta érdekességből szükségszerűséggé tette. Számos feltaláló próbálta meg igába fogni ezt az erőforrást, de az első gőzzel meghajtott működő gépezet megépítésének és értékesítésének érdemét rendszerint Saverynek tulajdonítják. Azután Newcomen tervezte meg 1700 körül azt a gyakorlatban is felhasználható, hengerben ide-oda mozgó dugattyúval működő gépet, ami valamennyi rá következő gőzgép előfutára lett.

1786-ban James Watt műszerkészítőként dolgozott a glasgow-i egyetemen, és azt a feladatot kapta, hogy javítsa meg a Newcomen-gép egyik modelljét, amelyet a természetfilozófiai órákon használtak. A történelemben előforduló szerencsés egybeesések egyike folytán Watt már korábban baráti viszonyba került több professzorral, köztük dr. Joseph Blackkel, a kémia professzorával, aki megbeszélte vele új felfedezését: a latens hő jelenségét. Watt volt az egyetlen a gőzgép korai fejlesztői között, akinek közvetlen és közvetett kapcsolatai voltak olyan tudósokkal, akik a hőjelenségeket tanulmányozták [17].

Watt arra az elhatározásra jutott, hogy továbbfejleszti Newcomen készülékét, és számos fontos elgondolást szabadalmaztatott, köztük a gőz sűrítésére szolgáló különálló kondenzátor alkalmazását, továbbá egy olyan gép terveit, amely rotációs mozgást hoz létre. Mindez éppen abban az időszakban történt, amikor az ipari forradalom addig soha nem látott szükségletet és igényt teremtett a gépi meghajtóerő iránt. Watt egy Matthew Boulton nevű sikeres gyárossal közösen előállt egy olyan gőzgép tervével, amely a 18. század utolsó évtizedében lezajlott technológiai fejlődés élvonalát képviselte. A gőzenergia alkalmazása mind a termelékenység, mind a termelt árumennyiségek tekintetében átalakította az egész ipart, és még ennél is forradalmibb változásokat hozott a közlekedésben és a szállításban, amikor mozdonyok és hajók meghajtására alkalmazták. Boulton és Watt gépei alacsony (5–15 psi)** nyomású gőzt használtak, ami behatárolta hatékonyságukat és gazdaságosságukat. A nagyobb (1 at-

* Hérón munkásságának idejét egyes kutatók jóval korábbra, az i. e. 220–150 közötti időszakra teszik. – *A ford.*

** psi *(pound per square inch):* font/négyzethüvelyk, a nyomás angolszász mértékegysége. A normál légnyomás körülbelül 14,7 psi. – *A ford.*

moszféra fölötti) nyomás nagyobb teljesítményű és gazdaságosabb gépeket tett volna lehetővé, de Watt ezt ellenezte, azon az alapon, hogy a nagy nyomás fokozza a robbanás veszélyét, és így elfogadhatatlan kockázatot jelent. Noha Watt és Boulton ellenállt a nagynyomású gőzgépek bevezetésének, szabadalmuk 1800-ban lejárt, és hamarosan megjelentek az ilyen gépek is. Oliver Evans az USA-ban és Richard Trevithick Angliában szinte egyidejűleg tervezett olyan hajtóműveket, amelyek kondenzátorral voltak ellátva, és a gőzt közvetlenül egy dugattyú mozgatására használták. Ezeknek az úgynevezett nagynyomású gőzgépeknek a működéséhez az atmoszferikusnál nagyobb gőznyomásra volt szükség.

A nagynyomású gőzgép első széles körben elterjedt alkalmazása – a gőzhajókon – gyakori és végzetes következményekkel járó robbanásokhoz vezetett: az utasok és a legénység tagjai egyaránt a levegőbe repültek, leforrázódtak, megsérültek a szétrepülő fémrepeszektől, a robbanások sokakat levetettek a gőzhajók fedélzetéről, és ezek a szerencsétlenek a tengerbe fulladtak. A balesetek gyakoriak voltak a nagynyomású gőz ipari alkalmazásainál is. A korai gőzgépeknél rossz minőségű, gyenge anyagokat használtak, alacsony szintű szakmai követelményeket támasztottak velük szemben, a gépészek nem rendelkeztek megfelelő szakértelemmel, mert hiányos volt a kiképzésük, és súlyos problémák voltak a minőség-ellenőrzéssel [10].

Mivel a gépészek jellemzően csak informális és rendszertelen képzésben részesültek, az USA-ban nagy volt az igény a képzés intézményesítése és a standard követelmények felállítása iránt. Még az a javaslat is napirendre került, hogy a szövetségi kormány létesítsen külön akadémiát a gőztechnológia tanulmányozására és oktatására. Mindebből azonban semmi sem lett, és a gépészek még sok éven át szinte csak tetszőlegesen választott képzést kaptak [30]. Watt előrejelzései az új hajtómű veszélyességét illetően helyesnek bizonyultak. Cameron és Millard így írt:

> „Ahogy a gőzenergia technológiája fejlődött, Watt egyre nehezebb dilemmával találta szemben magát: a nagyobb teljesítmény és nagyobb hatékonyság irányában érvényesülő trend egyúttal megnövelte a robbanások kockázatát. Az általa létrehozott technológia kicsúszott az ellenőrzése alól, és egyre nagyobb veszélyt jelentett az életre és a tulajdonra nézve egyaránt. Watt arra számított, hogy a nagynyomású gőz alkalmazásából még több baleset és haláleset fog származni. A közbiztonságot érintő fenyegetés most már beárnyékolta a gőzenergia közhasznú felhasználását..."
>
> Ám mit tehetett Boulton és Watt? Nem voltak abban a helyzetben, hogy szembeszálljanak azokkal a gazdasági erőkkel, amelyek egyre nagyobb teljesítményt követeltek a gőzgépektől, ugyanis ha megtagadták volna, hogy továbbfejlesszék a technológiát, számos más – kevésbé jól képzett vagy akár képzetlen gépész – kész lett volna vállalni a nagynyomású gőz alkalmazásával járó kockázatokat. Mindössze annyit tehettek, hogy ráirányították a közvélemény figyelmét az új technológiában rejlő veszélyekre, és emlékeztették mérnöktársaikat a közbiztonság garantálása terén fennálló speciális kötelezettségeikre. Watt vitát kezdeményezett az új technológia kockázatairól, és befolyását arra használta fel, hogy nyomást gyakoroljon a biztonságosabb és műszakilag jobban kivitelezett alternatív megoldások bevezetése érdekében [10, 6–7. oldal].

Watt kampánya a nagynyomású gépek alkalmazása ellen – néhány nagy nyilvánosságot kapott balesettel együtt – lelassította ezek elterjedését Angliában. Trevithick arról panaszkodott, hogy versenytársai erősen eltúlozták a kockázatok és a balesetek jelentőségét:

> „Azt hiszem, hogy B. és Watt urak készek minden tőlük telhetőt megtenni annak érdekében, hogy a robbanásveszélyt az újságokban és magánleveleikben is egészen másként tüntessék fel, mint amilyen az a valóságban" [17].

A nagynyomású gőz alkalmazásának egyik német támogatója 1842-ben azt írta, hogy a gőzgép fogyatékosságairól és biztonsági kockázatairól folyó intenzív viták elfedték az új gépek előnyeit, és „elégedetlenséget váltottak ki az ipari közösségben" [10].

A közvélemény háborgása ténylegesen arra kényszerítette a nagynyomású gőzgépek tervezőit, hogy biztonsági berendezéseket építsenek be a gépekbe [12]. Az ilyen típusú gépek kockázatai nem magából a hajtóműből, hanem a kazánból származtak: a kazán volt az, ami felrobbanhatott, és ez okozta a legtöbb baleseti sérülést. A kazángyártás technológiai színvonala azonban elmaradt a gépek gyors tökéletesítésétől. A mérnökök munkája nyomán gyorsan felhalmozódtak a termodinamikára, a gőznek a hengerben mutatott viselkedésére, a berendezések gyártásához használt anyagok erősségére és a gőzgép működésének sok más aspektusára vonatkozó tudományos ismeretek. Kevés tudományos eredmény állt azonban rendelkezésre a gőznyomásnak a kazánban való kialakulására, a korrózió és az anyagromlás hatásaira, valamint a kazánrobbanások okaira vonatkozóan [17]. A nagynyomású gőz alkalmazása ugyanakkor kiemelkedő igénybevételt jelentett a kazánokkal szemben, felszínre hozva a kazánok gyártásához használt anyagok gyengeségeit, és elavulttá tette a kazánok megtervezésénél addig használt módszereket.

A veszélyek ellensúlyozására a gépészmérnökök kétféle típusú biztonsági berendezés használatát vezették be. A veszélyes szintet elérő gőznyomás csökkentésére egyrészt biztonsági szelepeket, másrészt könnyen olvadó ólomdugókat alkalmaztak, amelyeknek ki kellett olvadniuk, amikor a hőmérséklet a gőz túlhevítése miatt túlságosan magasra emelkedett a kazánban. Ezek a széles körben reklámozott technológiai eszközök azonban nem oldották meg a problémákat, és a robbanások száma továbbra is növekedett. A biztonsági berendezések azért voltak sikertelenek, mert a mérnökök nem értették meg teljes mértékben a gőzkazánokban lezajló fizikai jelenségeket: a gőzfejlesztés folyamatainak dinamikáját csak a 19. század második felében sikerült tisztázni.

A nagyszámú baleset bekövetkezésének másik oka az volt, hogy a mérnökök súlyos tévedéseket követtek el a gőzgépek működési környezetére vonatkozó kalkulációikban, ideértve a gépészek, illetve a karbantartók képzésének minőségét is. A hajtóművek és a biztonsági berendezések tervei legtöbbször azon a feltételezésen alapultak, hogy a tulajdonosok és a gépkezelők racionálisan, lelkiismeretesen és hozzáértő módon viselkednek. A gépészeket és a karbantartókat azonban gyengén képezték ki, és olyan gazdasági ösztönzők érvényesültek, amelyek háttérbe szorították a biztonsági megfontolásokat annak érdekében, hogy nagyobb teljesítményt érjenek el, illetve több munkát végezhessenek. A tulajdonosok és a gépészek kevéssé értették meg a gőzgép működését és felhasználásának korlátait.

A gépkezelők hibái minden bizonnyal hozzájárultak a problémákhoz, ám nem csupán ők voltak felelősek a balesetekért. Mindazonáltal legtöbbször a tulajdonosokra és a gépészekre hárult a robbanásokért viselt felelősség legnagyobb része; a bírálatok ritkán érintették a mérnököt, aki a gépet megtervezte. Mint fentebb megjegyeztük, sok rosszul képzett és kellő szakértelemmel nem rendelkező mérnök vállalta a nagynyomású gőztechnológia fejlesztésével járó kockázatot. Szakmájuk tudományos alapjai abban az időben még kevéssé voltak kidolgozva, és a meglévő ismeretek is csak nehezen voltak elérhetők. A feltaláló-mérnökök személyes tudásszintje jelentette a gépek biztonságos működésének legfőbb elemét, és Watt arra az álláspontra helyezkedett, hogy a mérnökök személyes felelősséggel tartoznak a társadalomnak a biztonságos és hatékony gőzgépek kifejlesztéséért, és vállalniuk kell a balesetek büntetőjogi következményeit.

A nagynyomású gőz alkalmazásának korai ellenzői a veszélyek csökkentésére az új technológia használatának korlátozásával járó szabályozást javasoltak. Ez az elgondolás azonban kevés sikert aratott. A 19. század első felében a kormányok nem érezték feladatuknak, hogy beavatkozzanak a magánvállalatok működésébe. A gőzgép a siker eszméjét testesítette meg, és „a szinte akadálytalan nemzeti haladás, a minden korábbit felülmúló prosperitás és boldogság" szimbólumává vált [10]. Számos mérnök azt állította, hogy a gőzenergia alkalmazásából származó társadalmi és gazdasági nyereség elfogadhatóan kompenzálja a vele járó kockázatokat. Az USA-ban tipikus volt Thomas Hart Benton szenátor fellépése, aki nagyban hozzájárult a gőzhajókon történő kazánrobbanások csökkentésére irányuló törvények meghozatalának megakadályozásához. Benton kijelentette, hogy a gőzhajók kaptányai és tulajdonosai – kevés kivétellel – a legkiválóbb emberek, és ő sohasem látott semmiféle balesetet egyetlen gőzhajón sem, annak ellenére, hogy igen sokat utazott, hozzátéve, hogy hajóra szálláskor mindig nagy gondot fordított annak megtudakolására, hogy a hajógépek jó állapotban vannak-e [9].

A gőzgépek széles körű bevezetését követően azonban a balesetek számának drámai növekedését aligha lehetett elhanyagolni. Egy gőzhajó felrobbanása Angliában, amit ipari berendezésekben bekövetkezett robbanások sorozata követett, 1817-ben egy speciális bizottság felállításához vezetett, amelynek jelentést kellett készítenie a nagynyomású gőz veszélyeiről. A bizottság jelentése annak elismerésével kezdődött, hogy a gőzenergia nagymértékben hozzájárul a nemzeti prosperitáshoz, és hangsúlyozta a magángazdaságba való állami beavatkozás hátrányait. Kitért azonban arra is, hogy „amikor a tudatlanság, kapzsiság vagy hanyagság a közbiztonságot veszélyezteti, akkor a parlament kötelessége a beavatkozás" [9]. A bizottság gyakori kazánellenőrzéseket javasolt, ám javaslatai ténylegesen nem léptek hatályba. Körülbelül ugyanebben az időben az USA-ban Philadelphia városi tanácsa volt az első törvényhozó testület, amely tudomást vett a balesetekről, és megkísérelte azok kivizsgálását. A városi tanács jelentését továbbították az állami törvényhozáshoz, ám ott az elhalt.

Az 1830-as és 40-es években a balesetek riasztó mértékben tovább szaporodtak, s ez a kormányok részéről a kockázat csökkentésére irányuló újabb kísérleteket eredményezett. Az 1816-tól 1848-ig terjedő időszakban az USA-ban a szabadalmi biztos becslése szerint összesen 230 gőzhajórobbanás történt, amelyekben 2562 személy vesztette életét és 2097 személy sérült meg, a vagyoni kár pedig meghaladta a hárommillió dollárt. A Franklin Intézet, amelyet 1824-ben alapítottak Philadelphiában „a mechanikai

művészetek és az alkalmazott tudomány" művelésére és fejlesztésére, hatéves kutatási programot indított a kazánrobbanások kivizsgálására. Ez az intézet kapta meg az USA kormánya által juttatott első tudományos kutatási pénzalapot, a vizsgálatok alkalmából végzett kísérletekhez szükséges apparátus költségeinek fedezetéül. Ebben az esetben egy találmány és az alkalmazásához társuló balesetek segítették elő a tudomány fejlődését. A kutatások eredményeként jelentések sorozata született, amelyek feltárták a hibákat, és cáfolták a gőz természetére vonatkozó népszerű elméletekben megjelenő mítoszokat. A biztonság növelése érdekében rámutattak a robbanások okaira, és irányelveket fektettek le a kazánok tervezéséhez és építéséhez. Javaslat készült továbbá a kongresszus számára a szabályozást szolgáló törvények meghozatalára vonatkozóan, ideértve azokat a követelményeket is, amelyeket a mérnököknek – tapasztalataikat, tudásukat és jellemüket tekintve egyaránt – teljesíteniük kellett ahhoz, hogy megfeleljenek az elvárásoknak. A gőzhajórobbanások hatására gyengülni kezdett az addig uralkodó ellenállás az állami szabályozással szemben. Mind Angliában, mind az Egyesült Államokban törvényeket fogadtak el, amelyek kártérítést írtak elő a hanyagságból vagy üzemzavarból adódó balesetek következtében elhalálozott utasok családjai számára. Ezek azonban nem tartalmaztak semmiféle felügyeleti kritériumot, és a mérnökök képzettségére nézve sem írtak elő meghatározott követelményeket. Az volt az uralkodó meggyőződés, hogy a mérnökök, illetve a gépészek számára felállított szakképzettségi követelményeket a gyakorlatban túlságosan nehéz érvényesíteni, és a vállalkozók érdekeinek a nyilvánosság elé tárása garantálhatja a közbiztonságot. Végeredményben ezek a törvények sem csökkentették a robbanások számát.

Az újságokban a témával foglalkozó vezércikkek százai juttatták kifejezésre a közvélemény csalódottságát. A nagynyomású gőzgépek gazdasági hasznával, illetve az ezért a társadalom által fizetett árral irodalmi művek is foglalkoztak. *„Household Words"* című művében Dickens is írt erről [11], továbbá Thomas Law Peacock *„Gryll Grange"* című regényében az egyik szereplő megjegyzi, hogy „a nagynyomású gőzgépek nem hintenének halált és rombolást maguk körül, ha alkalmazásukat nem kísérné becstelenség és hanyagság mindenütt, ahol a költségesebb, alacsony nyomású gépek garantálnák az abszolút biztonságot".

1852-ben a közvélemény nyomása és az ismételten több száz ember halálát okozó tengeri katasztrófák sorozata együttesen végül rákényszerítették az USA kongresszusát, hogy elfogadjon egy törvényt, amely szabályozta a gőzhajókazánok építését és üzemeltetését, és ténylegesen csökkentette a gőzhajóbalesetek számát. Ez a törvény volt a jogi szabályozás első sikeres példája az Egyesült Államokban, és ez teremtette meg az első amerikai kormányügynökséget, amely a magánvállalkozások szabályozására létesült [9]. A mozdonyokra és az álló helyzetben használt kazánokra vonatkozóan sajnos nem hoztak hasonló törvényeket, és a gőzhajók kivételével folytatódtak a kazánok használatából eredő balesetek.

Wattnak és másoknak igazuk volt abban a véleményükben, hogy a precizitás és a biztonság új szabványai alapvető fontosságúak a gépi hajtóművek tervezése, gyártása és működtetése terén. Ezeket a magas követelményeket Nagy-Britanniában végül a 19. század utolsó harmadában vezették be kötelező erővel, és ettől kezdve a kazánrobbanások száma Nagy-Britanniában is nagymértékben csökkent. 1905-ben itt már csak 14 haláleset történt kazánrobbanás miatt, míg az Egyesült Államokban az áldozatok száma

ugyanakkor 383 főre rúgott. Később az amerikaiak többsége is felismerte a standard követelmények szükségességét: társaságok alakultak a gőzkazánrobbanások megelőzésére, a biztonság szempontjából legnagyobb körültekintéssel gyártott és működtett gőzmeghajtású gépi berendezések biztosítására speciális biztosítótársaságok szerveződtek, s végül – a Gépészmérnökök Amerikai Társasága *(American Society of Mechanical Engineers)* erőfeszítéseinek köszönhetően – a kazánok biztonságos üzemeltetésére vonatkozóan egységes előírásokat vezettek be [9].

Robbanó szoftver?

Ma a számítógépek korában élünk, és ismét egy olyan technológiával nézünk szembe, melynek alkalmazása terén nagy erejű gazdasági ösztönzők hatnak a szakterület fejlesztése és a technológia veszélyes rendszerek vezérlésére való felhasználása irányában. A számítógépek – csakúgy, mint a gőzgépek és az elektromos rendszerek – képessé tesznek bennünket arra, hogy olyan dolgokat vigyünk véghez, amelyekre azelőtt nem voltunk képesek, és ismét úgy tűnik, hogy a kockázatok az idő előrehaladásával, ahogy a számítógépek egyre több és több funkciót vesznek át az embertől, csak növekedhetnek. A balesetek potenciális következményeit illetően egyetlen különbség mutatkozik: ma olyan rendszereket építünk ki, számítógépeket használva ellenőrzésükre és vezérlésükre, amelyek potenciálisan képesek igen nagy arányú rombolást okozni, az emberi életet és a környezetet egyaránt fenyegetve. Ezekben a rendszerekben csupán néhány baleset is katasztrofális következményekkel járhat.

Ennélfogva nagy fontosságú, hogy a számítógépeket felelősségteljes módon használjuk fel. A múlttal vonható párhuzamok közelebbi vizsgálata kezünkbe adhat néhány kulcsot arra nézve, hogy ez hogyan valósítható meg.

• *A kazántechnológia fejlődése elmaradt maguknak a gőzgépeknek a tökéletesítése mögött.*

Noha a számítógépi hardvertechnológia megdöbbentő ütemben fejlődött, a szoftverfejlesztés üteme jóval lassúbb. Lassúbb a szükségesnél, elsősorban az olyan, általunk megépíteni kívánt komplex rendszerek esetében, mint például az űrállomások vagy az automatikusan vezérelt nukleáris erőművek. Úgy tűnik, hogy ezt a lemaradást kétféle módon lehet behozni. Az első módszer a visszatérés lehet egy olyan mérnöki alapelvhez, amit az idő igazolt: a dolgokat tartsuk egyszerű szinten, és azoknak az eljárásoknak a bonyolultságát, amelyeket megkísérlünk megvalósítani, csak lassan, a tapasztalatokból okulva növeljük. Például az *Ontario Hydro* vállalat lett újabban az első olyan közműszolgáltató Kanadában, amely hatósági engedélyt kapott egy nukleáris erőműnél teljes mértékben számítógépesített biztonsági rendszer alkalmazására. Az ehhez felhasznált szoftver körülbelül hatezer sornyi kódból áll, és csupán a legegyszerűbb, legegyenesebb vonalú kódolási technikákat használja. Bizonyos típusú szoftverhibák kiküszöbölésére a hardverbe beépített üzembiztonsági berendezések (*watch-dog* típusú időzített „őrszemek"), valamint önellenőrző szoftverek vannak beiktatva a rendszerbe. A szoftver olyan jól bevált biztonsági tervezési elvekre épül, amelyek standardként szolgáltak a korábbi hardveralapú üzembiztonsági rendszerekben. Mivel a szoftver ilyen egyszerű, a vele kapcsolatos bizalom megalapozását szolgáló standard tesztelési

technikák mellett formális és informális verifikációs és biztonsági technikákat is tudtak alkalmazni [2, 4].

Ezzel szemben Angliában az első számítógépesített üzembiztonsági rendszer, amely a *Sizewell B* reaktor üzemeltetéséhez készült, az engedélyezéséhez elvégzett értékelés szerint százezer soros kódot, 300-400 mikroprocesszort, továbbá különféle ellenőrzési és üzemlezárási funkciókat foglal magába [35]. Ez a rendszer nem csupán fölötte áll annak, hogysem az ellenőrzésére képesek lennénk kifinomult szoftververifikációs technikát alkalmazni, hanem megsérti azt az alapvető reaktorbiztonsági tervezési elvet is, amely az ellenőrzési és biztonsági berendezések teljes függetlenségét írja elő [1]. Az ilyen típusú biztonsági tervezési követelmények az idők során alakultak ki, és feltétlenül szükségesnek bizonyultak – a számítógéptudósoknak tisztában kell lenniük ezekkel, és a mérnököknek alaposan át kell gondolniuk, hogy figyelmen kívül hagyhatják-e őket: a tervezési kritériumokban, a műszaki fejlesztés több száz éve során bekövetkezett sikerek és kudarcok nyomán felhalmozódott tudás jelenik meg.

A szoftver- és a hardvertechnológia fejlődése közötti szakadék áthidalására alkalmazható második módszer szintén megkívánja tőlünk, hogy valamelyest visszafogjuk a számítógépek iránti lelkesedésünket, és mérsékeljük a beléjük vetett bizalmat. Noha a számítógépekkel szemben korábban mutatkozott bizalmatlanság elvezetett ahhoz, hogy a legkritikusabb rendszerekbe hardveralapú hibaelhárító berendezéseket építsenek be, ez a bizalmatlanság ma elenyészőben van. A meglévő hardveralapú biztonsági mechanizmusokat és blokkolószerkezeteket egyre inkább kiiktatják, s a monitoring és az ellenőrzés funkcióit hovatovább kizárólag a számítógépekre bízzák. A mérnökök gyakran úgy döntenek, hogy a hardverbe beépített biztonsági és blokkoló háttérberendezések nem érik meg a rájuk fordított költségeket (a repülőgépek esetében a súlytöbbletet), és jobban bíznak a szoftver, mint a hardver megbízhatóságában. Ezzel ismét megsértik a biztonságnak azt a standard tervezési alapelvét, amely megköveteli az egypontos hibalehetőségek kiküszöbölését: a rendszert úgy kell felépíteni, hogy egyetlen esemény (például egy szoftverhiba) ne okozhasson balesetet. Jó példa erre a *Therac-25* esete. Ennek a sugárterápiás készüléknek a tervezői – abban a hitben, hogy a hardverberendezésekre többé nincs szükség – kiküszöbölték a rendszerből az ilyen típusú lineáris gyorsítóknál korábban szabványként alkalmazott biztonsági blokkolást, amikor a számítógépes irányításra tértek át. Helyette a blokkolási funkciókat és a biztonsági ellenőrzést a szoftverbe építették be. Miután 1985 és 1987 között hét baleset következett be egymás után, amelyek jelentős mértékű sugárzástúladagolással és négy halálesettel jártak együtt, a vállalat végül engedményeket tett, és hardveralapú biztonsági berendezéseket épített be a készülékekbe [24].

A veszélyes rendszerek irányítása terén a számítógépek alkalmazásakor lehetünk körültekintőek, anélkül hogy szükségtelenül fékezni kívánnánk a technológia fejlődését. James Watt kampányolt a nagynyomású gőzgépek használata ellen, ám csupán annyi sikert ért el, hogy Nagy-Britanniában bizonyos mértékig késleltette azok használatbavételét. Az 1880-as években, ugyanakkor, amikor az ipari világ a gőztechnológia gyors bevezetésével való lépéstartásért küszködött, hasonló kérdések merültek fel a nagyfeszültségű elektromosság bevezetésével kapcsolatban is. Egy másik feltaláló, Thomas Edison bírálta a nagyfeszültség alkalmazását annak bonyolultsága, gyenge megbízhatósága és a közbiztonságra jelentett fenyegetései miatt, és kampányt kezdett,

hogy a közvéleményt ráébressze a veszélyekre. Át akarta adni az embereknek azt a meggyőződését, hogy a kockázatok és kihatásaik idővel még növekedni fognak. A biztonságos, alacsony feszültségű elektromos rendszerek mellett foglalt állást, amelyek véleménye szerint gyors elfogadásra találhattak a közönség körében, azonban – Watthoz hasonlóan – ő is csak részsikereket ért el.

Egy másik feltaláló-mérnök, Elihu Thomson szintén ellenezte a nagyfeszültségű áram használatát, mivel azt túlságosan veszélyesnek tartotta. Ahelyett azonban, hogy az ilyen rendszereket elutasította volna és a mellőzésükért indult volna harcba, Thomson megkísérelt technológiai megoldásokat találni. Úgy vélte, hogy különféle biztonsági berendezésekkel nagymértékben csökkenthető a balesetek kockázata, és azért lobbizott, hogy elismertesse a biztonságos nagyfeszültségű rendszerek kifejlesztésének szükségességét. Thomson fő érve az volt, hogy a biztonságra törekvő műszaki fejlesztési program az erősen versengő piacon üzleti előnyöket biztosít azoknak a vállalatoknak, amelyek vezető szerepre tesznek szert a biztonsági berendezések technológiai megoldásainak kifejlesztésében.

Watt és Edison oly módon kísérelték meg a kockázatok korlátozását, hogy az óriási potenciális hasznokkal kecsegtető technológiák bevezetése ellen foglaltak állást. Ezzel szemben Elihu Thomson úgy érvelt, hogy a kockázat jobban csökkenthető egyszerű, biztonságos berendezések tervezésével, mint a már rendelkezésre álló technológia használatának korlátozásával vagy a technológiai fejlődés drasztikus gátolásával. Thomson megközelítése gyakorlatiasabb, és valószínűleg több sikerrel alkalmazható a biztonsági szempontból kritikus berendezések működését ellenőrző számítógépes rendszerek esetében is.

• *A kazánrobbanások okait illetően kevés tudományos ismeret állt rendelkezésre.*

A kazánokhoz hasonlóan a mi szakterületünk tudományos alapjai is még mindig a kifejlődés stádiumában vannak. Ahhoz, hogy egy bizonyos szakterület a „művészet" állapotából a tudomány szintjére kerüljön, tudás felhalmozására és rendszerezésére van szükség. Noha ez is folyamatban van, ma is több erőfeszítést fordítanak új találmányok kidolgozására és bizonyos eszközök kifejlesztésére még kipróbálatlan, szigorúan tudományos értelemben nem megalapozott technológiai eljárások megvalósításához. Hipotéziseinket azonban a tudomány elvei alapján gondosan értékelnünk és igazolnunk kell.

A próba-tévedés módszere az idők során jól bevált a műszaki tudás felhalmozására. A mérnökök elemzik a hibák és a balesetek okait, majd azok megismétlődésének megakadályozása vagy minimálisra csökkentése érdekében helyesbítő intézkedéseket tesznek. Ezek a javítások és tökéletesítések előbb-utóbb megtalálják az utat ahhoz, hogy beépüljenek a különféle specifikációk, szabványok, kódok és szabályozások szövetébe, abba, amit általában „jó műszaki gyakorlatnak" szokás tekinteni. Ez azonban igen lassú módja a tudás felhalmozásának. A próba-tévedés módszere mellett a mérnökök már korán elkezdtek tudományos elemzésen alapuló megoldásokat is keresni. A technológiai fejlődés mai élénk üteme annak köszönhető, hogy felhalmozódott az alapvető tudás, amit olyan dolgokra vonatkozóan gyűjtöttünk össze, mint a mechanika, az anyagok és a szerkezetek, s így a mérnököknek már nem csak úgy áll módjukban értékelni terveiket, hogy megépítenek valamit, és azután kipróbálják, hogy az vajon meg-

felelően működik-e. Egy-egy új technológia fejlődésének korai éveiben két szakasz különböztethető meg: 1. a problémák lehetséges megközelítéseinek és megoldásainak feltárása (invenció), és 2. mindannak az értékelése, amit ebből a próba-tévedés folyamatból meg lehet tanulni, olyan hipotézisek felállításához, amelyek tudományosan és empirikusan tesztelhetők, a technológia tudományos alapjainak kidolgozása céljából. A legnagyobb hangsúly mindeddig az első szakaszon, vagyis magukon a találmányokon voltak; most azonban eljött az ideje annak, hogy több figyelmet fordítsunk a második szakaszra.

A találmányok létrehozására való törekvés értékes és szükséges erőfeszítés, a leghasznosabb találmányok azonban tudományos ismereteken alapulnak vagy azok révén tökéletesíthetők. Az invenció termékeket, technikákat és eszközöket hoz létre. A tudomány teremti meg a tudást és a termékek, technikák és eszközök értékelésére és tökéletesítésére való képességet. A feltalálók a tudományt használják fel jobb találmányok kidolgozásához és ahhoz is, hogy a már rendelkezésükre álló találmányoknak az újakkal való összehasonlítása révén megbizonyosodhassanak arról, hogy az utóbbiak jobbak a régieknél. A tudományos tudás fokozatos fejlődése vezetett el Watt fontos szabadalmaihoz, amelyek létrehozták a gyakorlatban felhasználható gőzgépet. A gőzgépekre és a kazánokra vonatkozó alapvető tudás további gyarapodása tette lehetővé a hatékonyabb és biztonságosabb gépek gyártását. Noha az alacsony nyomású gőzgépek elkészítéséhez és használatához kezdetleges tudás is elegendő volt, a biztonságos nagynyomású gépekhez mélyebb tudományos alapokra volt szükség.

A szoftverfejlesztés terén létrejött találmányok emelőhatást biztosítottak jelenlegi szoftverrendszereink kiépítéséhez. Nem akarom lekicsinyelni azt, amit elértünk: rendkívül komplex rendszereket építünk fel, amelyek közül számos figyelemre méltóan jól működik hosszabb időn át is. Lehetséges azonban, hogy már annak a határait feszegetjük, amit az ismert tudományos és műszaki elveken alapuló, még jobb találmányok nélkül még hatékonyan megvalósíthatunk. Korai gyors fejlődésünk pedig lelassulhat, ahogyan elérjük azokat a határokat, amelyek gátat szabnak annak, ami a nyers erő révén elérhető. Az 1950-es évek végén és a 60-as évek elején például tanúi lehettünk igen leleményes módszerek kifejlesztésének a programozási nyelveknél alkalmazott parserek kidolgozása terén. A nyelvtanok formális elméleteinek kifejlesztésével azonban lehetővé vált olyan szintaktikus elemző generátorok létrehozása, amelyek kiküszöbölték annak a szükségességét, hogy minden egyes új gépi kód fordítóprogramjához külön parser készüljön.

Hasonló szükségletek ma is felmerülnek a szoftverfejlesztés terén. Ma a legnagyobb szükség – nem a jelenlegi szoftverfejlesztési programok rövid távú megvalósítására, hanem inkább a jövőbeli haladásra tekintve – nem új nyelvek vagy a találmányaink megvalósításához szükséges eszközök kidolgozása iránt, hanem annak a mélyebb megértése iránt nyilvánul meg, hogy találmányaink valóban hatékonyak-e, és miért (vagy miért nem). Nagyobb szükség van például a specifikációs nyelvek megtervezésénél követendő alapvető elvek és kritériumok kidolgozására és hitelesítésére, mint még több nyelv létrehozására. Az alapvető tervezési elvek kidolgozására és validálására, valamint ezek egymással való ütközéseinek és összeegyeztetési lehetőségeinek a megértésére nagyobb szükség van, mint a tervek specifikációjához felhasználható új eszközökre. És nagyobb szükség van a szoftverfejlesztési folyamatok különféle típusai által kiváltott

hatások valós szervezetekben, különféle körülmények között történő tanulmányozására, mint új nyelvek kidolgozására a specifikációs folyamatokhoz.

A kutatók a szoftverfejlesztés egyes alterületein lelkiismeretesebben törekedtek az elméleti alapok kiépítésére, mint másutt. Ilyen terület például a tesztelés, bár még itt is igen sok feladat áll előttünk. A teszteléskutatók elméleti módszereket definiáltak különféle tesztelési stratégiák összehasonlítására mind a költséghatékonyság (például [38]), mind a stratégiák értékelésére szolgáló formális kritériumok (például [16]) szempontjából, továbbá az olyan axiómák vagy tulajdonságok meghatározására is, amelyeket bármely megfelelési kritériumnak (a tesztelés befejezési pontját meghatározó szabálynak) ki kell elégítenie (például [37]). Az elméleti alapok általában megadhatják 1. az értékelés kritériumait, 2. az összehasonlítás eszközeit, 3. a lehetőségek elméleti korlátait, 4. az előrejelzés eszközeit, és 5. az alapvető szabályokat, elveket és struktúrákat.

Hogyan fogjuk kiépíteni ezeket ez alapokat? Ehhez egyrészt matematikai modellek és elméletek kidolgozására, másrészt gondosan megtervezett kísérletek végrehajtására lesz szükség. Az absztrakt rendszerek elemeit definíciókkal hozzák létre, a köztük lévő kapcsolatokat pedig bizonyos feltételezések (például axiómák és posztulátumok) révén teremtik meg. Az absztrakt rendszerekkel kapcsolatban számos kérdés megválaszolható a matematika felhasználásával. A konkrét rendszerekben (ahol a rendszer egyes elemei fizikai objektumok) az elemek létezésének és tulajdonságainak megteremtéséhez empirikusan megalapozott kutatásra van szükség, mivel az adott rendszerben érvényesülő fizikai törvényekre vonatkozó tudásunk szinte mindig tökéletlen.

A számítógép legnagyobb ereje abban áll, hogy olyan általános célú eszköz, amely utasítások (adatok) halmazának bevitelével olyan speciális célú géppé alakítható át, amely alkalmas az adott cél elérésére. A szoftver nem más, mint egy speciális célú gép absztrakt terve, amely – mihelyt lefuttatják valamely számítógépen – konkrét tervvé válik, tehát mind absztrakt, mind konkrét tervként lehet és kell értékelni. A szoftver továbbá egyrészt matematikai objektum, másrészt emberi termék. A szoftver emberek által történő kidolgozásának segítésére szolgáló hatékony eszközöket vagy tervezési technikákat nem hozhatunk létre anélkül, hogy a szoftverfejlesztés során megnyilvánuló emberi problémamegoldási viselkedést is megértenénk.

Szakterületünk tapasztalati aspektusai szükségessé teszik a kísérletezést. A biztonság megteremtésének problémáit tekintve például részleges megoldásként már rendelkezésre állnak bizonyos formális módszerek, de az ilyen technikák alapját képező hipotézisek validálása mindeddig csak csekély mértékben történt meg. Nem tudjuk, hogy a formális módszerek használata vajon kevesebb hiba, vagy másfajta hibák bekövetkezéséhez fog-e vezetni? Az így készült programok vajon megbízhatóbbak? Biztonságosabbak? Bizonyos technikák hatékonyabbak-e, mint mások? Milyen képzésre van szükség e technikák hatékony alkalmazásához? A formális módszerek használata költségesebb vagy kevésbé költséges a korábbiaknál? Mivel a technikákat embereknek kell alkalmazniuk, ezekre a kérdésekre nem lehet csupán matematikai elemzés útján megadni a választ, szükség lesz emberek részvételével folytatott kísérletekre.

Az intuíció fontos szerepet játszik a hipotézisek megalkotásában. Intuíciónk azonban néha félrevezető; egyre újabb és újabb hipotéziseket állítunk fel (ma túlságosan is gyakran), függetlenül attól, hogy intuíciónk mennyi bizalmat enged helyezni azokba.

Jelenleg különféle technikákat alkalmazunk, sőt számos esetben felhatalmazást is adunk másoknak ezek alkalmazására, anélkül, hogy validálnánk működésüket, vagy ellenőriznénk a mögöttük meghúzódó hipotézisek és feltételezések helytálló voltát (például [3]).

Amikor egy fizikus tévesen jelent be valamely felfedezést, mint ahogyan történt például a hidegfúzió esetében, maga az elgondolás a szakterület peremvidékein még egy darabig fennmaradhat. A tudomány ragaszkodása a megismételhetőség és a gondos kísérleti bizonyítás követelményéhez azonban lehetővé teszi, hogy az ilyen „eredmények" bejelentését a tudomány mérvadó többsége viszonylag rövid időn belül elutasítsa. A szoftverfejlesztés technikái és eszközei terén születő eredményeket illetően nekünk is ragaszkodnunk kell az értékelés és a bizonyítás ugyanilyen szintjéhez. Ez azonban sajnos ritkán valósul meg, és továbbra is makacsul hiszünk a „csodaszerekben". Még Brooks és Parnas gondosan alátámasztott és széles körben elfogadottá vált tanulmányainak [8, 27] a megjelenése után is gyakran találkozunk olyan bejelentésekkel, hogy valaki újabb csodaszert talált.

Nem azt hirdetem, hogy mindenkinek abba kell hagynia a kutatást, amelyet a szoftverfejlesztés területén éppen végez, és kezdje el hipotéziseinek tesztelését, valamint az alapok lerakását. Az invenció a műszaki haladás igen fontos része. Azoknak a komoly problémáknak a megoldásához, amelyekkel ma nézünk szembe, eszközökre és technikákra van szükségünk. A megalapozott elvekre épülő találmányok azonban hatékonyabbak lesznek azoknak a komplex problémáknak a megoldásában, amelyekkel küszködünk. Fel kell ismernünk a jelenlegi szoftverfejlesztési technikáink és eszközeink mögött rejlő bizonyítatlan feltételezéseket és hipotéziseket, és nem aszerint kell azokat értékelnünk, amit hinni szeretnénk, hanem annak alapján, amit már ténylegesen sikerült bebizonyítani róluk.

A szoftvervezérelt rendszerek biztonságos kiépítéséhez szükséges hatékony szoftverfejlesztési eszközök kidolgozására való képességünket – a robbanásveszélyes kazánok tökéletesítéséhez hasonlóan – növelni fogja, ha mélyebben megértjük az érintett szakterületek tudományos alapjait.

- *A kazánokhoz tervezett biztonsági berendezések nem működtek olyan jól, mint ahogyan várták, mivel nem a balesetek okainak tudományos megértésén alapultak.*

Nemcsak a szoftverhibák mélyen rejlő okait nem értjük, hanem kevés azoknak a kutatóknak a száma is, akik az ilyen hibák mögött feltárható kognitív folyamatokat vizsgálják. Ez a hibakezelés olyan módszereinek kifejlesztéséhez és alkalmazásához vezetett, amelyek téves feltevéseken alapulnak.

Csupán egyetlen példát említve erre: a biztonsági szempontból kritikus rendszerek üzembe helyezésének a kormányszervek részéről történő engedélyezése és az ilyen rendszerekben alkalmazott szoftverek ultramagas szintű megbízhatóságára vonatkozó kijelentések mindmáig az úgynevezett N-verziós programozás *(N-Version Programming, NVP)* alkalmazásán alapult. Az *NVP* azt jelenti, hogy több fejlesztőcsapat egymástól függetlenül megírja a szoftver számos változatát, majd ezeket a változatokat lefuttatják, és a többségi választ *(majority answer)* használják fel, ha van ilyen. Magát a technikát közvetlenül az N-modulusos redundancián alapuló hardverhiba-tűrési technikából *(hardware fault tolerance technique of N-modular redundancy)* vették át,

ahol egy-egy komponens számos példánya össze van kötve egy döntőáramkörrel, amely kiválasztja a többségi értéket.*

A hardvertechnikát nem a tervezési hibák, hanem a véletlenszerűen előforduló üzemzavarok leküzdésére fejlesztették ki. Az *NVP* ennek dacára átteszi ugyanezt a megközelítést a szoftver területére, és ezt a technikát ma a szoftver állítólag ultramagas szintű megbízhatóságának elérésére szolgáló módszerként alkalmazzák a kereskedelmi forgalomban használt legtöbb repülőgép számítógépes rendszerében. Az a néhány empirikus vizsgálat azonban, amelyet ezzel kapcsolatban elvégeztek, nem terjedt ki a hibák egymástól való függetlenségére vonatkozó feltételezés helyességének tesztelésére, sem pedig az adatok gondos elemzésére annak eldöntéséhez, hogy az ultramagas szintű megbízhatóságot vajon ténylegesen sikerült-e elérni [23]. Kísérletek sorozata [6, 14, 22, 34] és egy matematikai elemzés [13] kétségessé tette ezeket a feltételezéseket.

E technika híveinek legújabb törekvése arra irányul, hogy módszerüket „szoftverváltozatosság" *(software diversity)* névre átkeresztelve összemérhetővé tegyék a „hardverváltozatosság" megtervezésének *(hardware design diversity)* már jól megalapozott módszerével, bár a szoftvertechnika itt sem elégíti ki az alapfeltevéseket. A változatosság a hardver terén nem magától jön létre, azt meg kell tervezni. Ott abból a célból, hogy elkerüljék a közös üzemmódból eredő *(common mode)* általános hibákat, különféle hibamódokra lehetőséget adó komponenseket, például elektronikus és hidraulikus elemeket használnak. Ennek a döntő fontosságú alapfeltevésnek, miszerint az egyes komponensek különféle hibamódokra adnak lehetőséget, a többszörös szoftververziók sem tesznek eleget.

Nemcsak azt kell igazolnunk, hogy a valamely szoftverfejlesztési technika alapját képező feltételezések valóban eleget tesznek mindannak, amit velük kapcsolatban állítanak, hanem a kívánságlista jellegű címkéket is kerülni kell. Egy technikát például a „szoftverváltozatosság" vagy a „szakértői rendszer" címke segítségével valami olyan tulajdonsággal felruházni, amit reményeink szerint elérhetünk vele (ám ezt még ezután kell bizonyítanunk), félrevezető és tudománytalan. A szakértői rendszerek esetében például a „termelési szabályrendszer" *(production-rule system)* megnevezés, ami ténylegesen használatos volt ezek jelölésére, mielőtt valaki előállt a még inkább piacorientált címkével, tudományosabb lenne. [Ha jobban ragaszkodnánk technikáink tudományos megalapozásához], akkor valószínűbb lenne, hogy azoktól, akik ennek a technikának a használatát javasolják, megkövetelnék annak a bizonyítását, hogy a rendszer valóban szakértőként működik, és nem fogadnák ezt el mintegy axiómaként. Pszichológiai elméletek és vizsgálatok valóban arra utalnak, hogy az emberi szakértők nem ilyen módon hoznak döntéseket (például [31, 28]): az emberi döntéshozatalban sokkal kifinomultabb problémamegoldási típusok játszanak szerepet.

A „címkézéssel" megvalósuló bizonyítással rokon a definíció révén történő bizonyítás, például a hibatűrés redundanciaként való definiálása (egy másik elterjedt gyakorlat), vagy a biztonságnak valamiféle védelem (például monitoring- és üzemmegsza-

* A „többségi érték" *(majority value)* ebben az esetben úgynevezett majoráns kritériumot jelent, ami arra vonatkozik, hogy a matematikai megközelítés alapján legnagyobb biztonságot kielégítő választ alkalmazzák. – *A ford.*

kító rendszerek) használatával történő definiálása. Az ilyen esetekben ahelyett, hogy az adott tulajdonság elérésére szolgáló technika definiálásába ágyaznák be a szóban forgó tulajdonságot, a technika ágyazódik be a tulajdonság definiálásába. Ebből két probléma származik. Az első annak a tendenciózus feltételezése, hogy a kívánt tulajdonságot sikerült elérni, mivel a definícióba beágyazott megközelítést használták, például a hibatűrés megvalósul azáltal, hogy redundanciát használnak. A második pedig az a gyakorlat, hogy az adott tulajdonság eléréséhez vezető különféle utak keresése a beágyazott megközelítésre korlátozódik, például ha a biztonságos működést mint bizonyos védőrendszerek használatát definiálják, amelyeknek a segítségével veszélyes helyzetekben is helyreáll a rendszer, akkor más megbízható és hatékony technikákat, amelyek megszüntetik a veszélyes állapotokat vagy azok bekövetkezésének lehetőségét minimálisra csökkentik, tekintetbe sem vesznek.

Ha nem tudunk megfelelő tudásalapot kifejleszteni a szoftvertervezés terén előforduló emberi hibákra vonatkozóan, akkor kétséges, hogy azok kiküszöbölésére vagy kompenzálására képesek leszünk-e igen hatékony szoftverfejlesztési technikákat megtervezni. El kell kerülnünk továbbá azt a hibát is, hogy az ember és a gép közé egyenlőségjelet tegyünk, és elhanyagoljuk szakterületünk kognitív és emberi aspektusait. Végül, ha a leghatékonyabb biztonság- és megbízhatóságnövelő technikákat kívánjuk megtervezni, értékelni és kiválasztani, akkor nem szabad beleesnünk a „címkézéssel" történő bizonyítás vagy a definícióink által korlátozott megoldások és más hasonló tudománytalan gyakorlatok hibájába.

- *A biztonsági berendezések beépítését a gőzgépekbe nemcsak a kazánokra vonatkozó tudományos tudás hiánya gátolta, hanem egyfajta szűklátókörűség is, amelynek következtében csupán technológiai megoldásokat próbáltak megtervezni, anélkül, hogy tekintetbe vették volna a gépekkel összefüggő társadalmi és szervezeti tényezőket, azt a környezetet, amelyben a gépi berendezéseket használták.*

Egy nagy légitársaság, amely arról híres, hogy a világ legjobb repülőgép-karbantartási programját tudhatja magáénak, néhány évvel ezelőtt bevezetett egy szakértői rendszert a karbantartó személyzet munkájának segítésére. A karbantartás minősége visszaesett. A személyzet függővé kezdett válni a számítógépesített döntéshozataltól, s nem volt többé hajlamos önálló döntéseket hozni és vállalni azokért a felelősséget. Miután a szoftvert megváltoztatták oly módon, hogy csupán információt szolgáltasson, és csak akkor, amikor ezt megkívánják tőle, a minőség ismét javult. Ehhez a jelenséghez hasonló példát találtak a repülőgépek vezetése terén is: amikor a számítógépek bevezetése növelte a pilóták önbizalmát és önelégültségét, egyúttal csökkentette szituatív éberségüket, s ennek folytán veszélyes helyzetek alakultak ki. A biztonság növelése érdekében alkalmazott számítógépek használata ténylegesen az ellenkező hatást is elérheti, ha nem veszik gondosan tekintetbe az emberi tényezőket, azt a komplex környezetet, amelyben a számítógépet használni fogják.

Egyesek felvetették, hogy a megoldás az lehet, ha az embereket teljesen kiküszöbölik a kritikus ciklusokból. Amennyiben azonban így járunk el, akkor valójában megalapozatlan bizalmat helyezünk a programozók képességeibe abban a tekintetben, hogy azok minden eshetőséget előre látnak, és helyesen előre meg tudják határozni a legjobb megoldást minden körülmények között. Ezzel szemben még a magas szinten

automatizált rendszerek felügyeleténél, karbantartásánál és működtetésénél is szükség van az emberekre.

A szűk technológiai szemlélet egy másik aspektusa a technikai megoldásokra helyezett hangsúly, a szervezeti és vezetési megfontolások figyelmen kívül hagyásával. Az elmúlt húsz év majdnem minden nagyobb balesetében (például Three Mile Island, Csernobil, Challenger, Bhopal és Flixborough) komoly szervezeti és vezetési hiányosságok játszottak közre. Az olyan vezetés, amely nem tekinti prioritásnak a biztonsági kérdéseket, a technikai személyzet legjobb erőfeszítéseit is kudarcra kárhoztathatja. Az érintett szervezetek az említett közelmúltbeli balesetek mindegyikében kifinomult, potenciálisan hatékony biztonsági programokkal és biztonsági berendezésekkel rendelkeztek. A biztonsági berendezések potenciális hatékonyságát mindegyik esetben nem technikai tényezők hiúsították meg. A biztonsággal való törődés, a felelősségérzet és az elszámoltathatóság a szervezetekben éppen olyan fontos, vagy még fontosabb, mint a technológia.

- *A gőzgépekkel kapcsolatos balesetekért legtöbbször nem a tervezőket vagy magát a technológiát tartották felelősnek, hanem a gőzgépek kezelőit.*

Sajnos igen gyakran előfordul, hogy a balesetekért a gépi berendezések kezelőit teszik felelőssé, amikor olyan helyzetbe kerülnek, ahol az emberi hiba elkerülhetetlen. Ez ma is éppoly gyakran fordul elő, mint száz évvel ezelőtt, és amikor a szoftverfejlesztők az emberi tényezőkre vonatkozóan elegendő tudás és a tervek évtizedeken át történő fokozatos tökéletesítésének tapasztalatai nélkül kezdenek ember-gép interfészeket tervezni, még komolyabb problémává válik.

Jó példa erre – bár szinte általánosnak tekinthető az a meggyőződés, hogy a repülőgép-balesetek többségét a pilóták hibái okozzák – az amerikai légierőnél repülés közben bekövetkezett 681 vészhelyzetről készített tanulmány, ami azt mutatta ki, hogy a gépek személyzete 659 esetben képes volt kiküszöbölni a berendezések meghibásodásából és különféle karbantartási hiányosságokból adódott problémákat, miközben csupán tíz esetben fordultak elő a pilóták által elkövetett hibák. Más légi közlekedési tanulmányok azt mutatják, hogy a pilótákkal összefüggő repülőgép-balesetek 80%-a nem az érintett személyek ostobaságának vagy pánikba esésének, hanem vagy a kiképzésük fogyatékosságainak, vagy pedig annak volt tulajdonítható, hogy a műszerek és a vezérlőberendezések kialakításánál elhanyagolták a pszichotechnikai szempontokat [18].

Az emberek azért hatékonyak vészhelyzetekben, mert képesek elemezni a helyzetet, és újszerű megoldásokkal tudnak előállni. Az emberek akkor dolgoznak jól, ha a világról olyan helytálló modellel és mélyebb ismeretekkel rendelkeznek, amelyeket felhasználhatnak cselekedeteik eredményeinek előrelátására. Az operátorok – annak érdekében, hogy végrehajthassák feladataikat, illetve hogy megakadályozhassák a balesetek bekövetkezését vagy enyhíthessék azok következményeit – néha szükségesnek találják, hogy megszegjék a szabályokat. A rugalmasság szükségességét azok a hibák is mutatják, amelyek gyakran előfordulnak valamely munkafeladat megoldása során, amikor az alkalmazottak szigorúan „a papírforma szerint" dolgoznak. Ahhoz, hogy vészhelyzetekben döntéseket hozhassanak, az operátoroknak használható formában adott

megfelelő információkkal kell rendelkezniük, és érteniük kell annak a rendszernek a működését, amelyet irányítanak.

A *Three Mile Island* reaktorbaleset klasszikus példája annak, hogy egy balesetért tévesen az operátorokat teszik felelőssé, és utólagos éleslátással az operátorok tevékenységeit tekintik hibásnak. Ezért a balesetért általában az erőmű kezelőit hibáztatják, noha a baleset eseménysorozatát a gépi berendezés olyan üzemzavarai indították el és kísérték mindvégig, amelyek teljesen függetlenek voltak az operátorok cselekvéseitől. Az operátorok főbb hibái csak az események után váltak láthatóvá, az adott időpontban jobb döntések meghozatalához nem állt rendelkezésükre elegendő információ arról, hogy milyen folyamatok mennek végbe az erőműben. A bekövetkezett eseményeket a meglévő műszerezettség mellett valójában elkerülhetetlennek nevezték [7], mivel ezek közvetlenül az elektromechanikai rendszerterv hibáiból adódtak. A számítógép például a riasztások és az információk kinyomtatásával órákkal elmaradásban volt, noha a döntéseket perceken belül kellett meghozni, továbbá a műszerek a vészhelyzet körülményei között leolvashatatlanok voltak és téves információt szolgáltattak. A *Three Mile Island* balesetet megelőzően a nukleáris mérnökök kevéssé érdeklődtek az operátorok számára készülő interfészek tervezése iránt. A Kemeny Bizottság jelentése a balesetről azzal a következtetéssel zárult, hogy az operátor által elkövetett hibát a rendszerterv alapvető hibái váltották ki, amelyek ezt követően is mindvégig közrejátszottak az események alakulásában [20].

Az iráni légibusz Vincennes-nál történt balesete jól ismert, de az ember-számítógép interfész gyenge tervezése miatt sok más baleset is bekövetkezett, amelyek kevés nyilvánosságot kaptak. Nagy Britanniában egy vegyi üzemben egy számítógép riasztójelzések hosszú listáját nyomtatta ki, amikor áramkimaradás történt. A tervezőcsapat feltételezte, hogy hasonló helyzetben az operátor azonnal megszakítja az üzem működését. Ehelyett az operátor azt figyelte, ahogy a számítógép kinyomtatja a riasztások listáját, és azon gondokodott, hogy mit tegyen. Az ember ilyen esetben nem tehető egyedül felelőssé: ha bárki túlságosan sok információval terhelődik, az a legvalószínűbb, hogy nem fog tenni semmit, amíg megpróbálja megérteni a helyzetet [21].

Az emberi pszichológia és viselkedés alapvető megértése a felhasználói interfészek tervezésének olyan előfeltétele, amely igen gyakran hiányzik a szoftverfejlesztők képzéséből. Az olyan tervek például, amelyek egy képernyőn – az *enter* billentyű benyomásával történő ellenőrzés és igazolás céljából – adatokat vagy utasításokat jelenítenek meg egy operátor számára, egy bizonyos idő elteltével, miután csupán kevés hiba fordul elő – oda vezetnek, hogy az operátornak szokásává válik az *enter* billentyű gyors egymásutánban történő többszöri lenyomása. Legtöbben már magunk is beleestünk ebbe a csapdába.

A megoldás nyilvánvaló. A szoftverfejlesztőknek komolyabban kell venni az emberi tényezőket, és a biztonsági szempontból kritikus szoftverekhez készülő interfészek tervezésébe pszichotechnikai szakértőket kell bevonni.

- *A korai gőzgépek üzemeltetéséhez alacsony szaktudásbeli követelményeket állítottak fel, a gépészek nem rendelkeztek megfelelő szakképzettséggel és szaktudással.*

A biztonsági szempontból kritikus szoftver kidolgozásához speciális tudásra és szakértelemre van szükség mind a fejlesztők, mind a menedzsment részéről. A jól kép-

zett személyzet iránti igény – mint bármely más gyorsan fejlődő technológia esetében – itt is megelőzi a kínálatot, és a szükséges képzettség és szaktudás megkövetelése gyakran hiányzik.

A szoftvertervezők képzése túlságosan gyakran elmarad a szakma legújabban elért fejlettségi szintjétől, továbbá csupán a számítógépes ismeretekre koncentrál, anélkül hogy biztosítaná az alapvető mérnöki készségek oktatását is. Túlságosan is gyakran találkozunk olyan emberekkel, mint például az a nukleáris mérnöki diplomával rendelkező férfi, aki azt mondta nekem, hogy szoftvert tervez repülőgépek irányításához, noha nem igazán ismeri az alapvető repüléstani elveket (és – gyanítom – a szoftvertervezési elveket sem). A biztonsági szempontból kritikus szoftverek tervezői között találhatók olyan emberek, akiknek a szoftvertechnikára vagy a felhasználási területre, sőt akár mindkettőre vonatkozó tudása kívánnivalókat hagy maga után.

Az Egyesült Államokban sok államilag jóváhagyott szabvány előírja, hogy a kritikus műszaki programok személyzetében legyen legalább egy megfelelően képzett és működési engedéllyel bíró mérnök. A rendszerbiztonsági mérnökök működésének engedélyezéséhez az egyes államok eltérő követelményeket támasztanak. Az előírások rendszerint nem kívánják meg, hogy az egyes programok végrehajtásán dolgozó valamennyi mérnök a szakképzettségét igazoló működési engedéllyel *(professional engineering licence)* rendelkezzen vagy professzionális biztonsági mérnök legyen, de azoktól, akik a program végrehajtásában például vezető mérnökként vagy rendszerbiztonsági menedzserként felelős pozíciókat töltenek be, megkövetelik az előírt képesítést és a szakmájuk gyakorlásához szükséges engedélyeket, továbbá elvárják azt is, hogy vállaljanak felelősséget a legmagasabb mérnöki és etikai követelmények betartásáért. Ugyanakkor a szoftvermérnökökkel szemben, akik ugyanazokon a programokon dolgoznak, semmiféle hasonló követelményt nem támasztanak.

A nagyfeszültségű elektromosság ellen folytatott kampányában Edison figyelmeztetett az elektromos áramszolgáltatók részéről megnyilvánuló, csekély szakértelemből és tudatlanságból fakadó problémákra, csakúgy, ahogy Watt is hangsúlyozta a mérnökök személyes erkölcsi felelősségét a biztonságos és hatékony gőzgépek létrehozásáért, és szorgalmazta a mérnökök büntethetőségét balesetek esetén [10]. Ha a szoftverfejlesztés terén mi magunk nem ragaszkodunk a kompetencia és a biztonság minimális szintjeinek a meghatározásához, akkor a kormány fog közbelépni, és megteszi ezt helyettünk. A közvélemény jogosan várja el, hogy a veszélyes rendszereket az elérhető legbiztonságosabb technológia felhasználásával építsék meg.

Watt, Edison és a 18. század más feltalálói kampányokat folytattak a szakismeretek szintjének emeléséért, mivel felismerték azokat a potenciális veszélyeket, amelyek találmányaikból származhatnak, ha azok rossz kezekbe kerülnek. Előre jelezték, hogy az új technológiai rendszerek műszaki megvalósításához szükség lesz a biztonság és a pontosság magasabb szintjének elérésére, és szigorú szakmai követelmények felállítását kezdeményezték [10]. Edison és Watt azt vallották, hogy „a mérnökök felelősek a szakszerű munka elvégzéséért, beleértve a legnagyobb biztonságot is" [10]. Fáradozásuk hozzájárult ahhoz, hogy végül szakmai társaságok alakultak, amelyek vállalták a biztonsági és szakképzettségi követelmények meghatározását.

Az ilyen előírásokat és a működési engedélyek megszerzéséhez teljesítendő követelményeket igen gondosan kell megfogalmazni. Nagy-Britanniában a nagyfeszült-

ségű elektromosság lassú bevezetéséért és az elektromosság használatában az USA-hoz viszonyítva bekövetkezett elmaradásért az új technológia elterjedésének erőteljes szabályozását hibáztatták [26]. Azok a szabályok például, amelyek a vezetékek minimális szigetelésére vonatkozó szabványokat meghatározták, szigorúbbak voltak a szükségesnél, és ezeket okolták az installációk magas költségeiért. Ám sok brit mérnök úgy érvelt, hogy bár a kiterjedt szabályozás ugyan növeli a költségeket, de egyben csökkenti a tűz és a sérülések veszélyét. A brit villamosmérnökök az 1890-es években – egységes csoportot alkotva – arra a meggyőződésre jutottak, hogy a szabályozás hiánya az USA-ban elősegítette a villamosipar fejlődését, de ennek az volt az ára, hogy több baleset fordult elő, amelyek „oly gyakoriak voltak, hogy valósággal a rendszer elidegeníthetetlen részének számítottak" [26]. A brit mérnökök ugyanakkor elítélték az amerikaiakat a gőzkazánok nem biztonságos használatáért és karbantartásáért.

A rosszul felállított követelmények ugyanúgy gátolhatják a számítógép-technológia fejlődését, mint ahogyan a 19. században a túlságosan szigorú szabályozás szükségtelenül gátolta a villamos technológia fejlődését Nagy-Britanniában. Még ennél is rosszabb, hogy az ilyen előírások akaratlanul is áthárítják a felelősséget a gyártókról és a fejlesztőkről a kormányszervekre, amelyeknek sokkal kevesebb tényleges közvetlen lehetőségük van a végtermék biztonságosságának ellenőrzésére. A rosszul felállított követelmények nemcsak hatástalanok maradhatnak, hanem növelhetik is a kockázatokat.

Néhány újabb kísérlet a kritikus rendszerekben alkalmazott szoftverekkel szemben támasztandó követelmények meghatározására egyenlőségjelet tesz a *biztonságosság* és a *megbízhatóság* közé (példa erre az „integritási szint" megnevezés használata, amely rendszerint csak a megbízhatósági szint más megjelölése). A biztonságosságot gyakran (elsősorban az atomenergia-iparban) a biztonsági védőberendezések megbízhatóságaként definiálják. A kockázat ilyen felfogása általánosan elterjedt a *megbízhatóságra* törő műszaki tervezésben, ám a *biztonságot* előtérbe helyező tervezők keserves tapasztalatok árán megtanulták, hogy egyrészt az igen megbízható rendszerek nagyon veszélyesek is lehetnek, másrészt viszont lehetséges olyan rendszereket is tervezni, amelyek nagyon biztonságosak, bár megbízhatatlanok. A csupán a megbízhatóság figyelembevételét és fokozását célzó követelmények nem lesznek hatékonyak igen sok olyan baleset kivédésére, amelyek nem üzemzavarok miatt következnek be, és nem nyújtanak hatékony védelmet azokkal a balesetekkel szemben sem, amelyek olyan rendszerekben és alrendszerekben (például a szoftverben) előadódó hibák következtében történnek, ahol az igen magas szintű megbízhatóság nem érhető el vagy nem garantálható.

A biztonságtechnikai mérnökök a biztonságot a kockázatok felől kiindulva definiálják, és a problémát oly módon kívánják megoldani, hogy módszereket keresnek a veszélyforrások kiküszöbölésére vagy ellenőrzésére. Két megközelítés lehetséges: az egyik a veszélyek bekövetkezésének kiküszöbölése vagy minimálisra csökkentése, a másik pedig – a sérülések és a nagyobb károk megelőzése érdekében – a veszélyforrások ellenőrzés alá vonása akkor, amikor azok bekövetkeznek. Ha például a szóban forgó veszélyforrás a tűz, akkor az első megközelítés vagy éghetetlen anyagok alkalmazását írja elő, vagy pedig kiküszöböli, illetve minimálisra csökkenti a szikrák előfordulásának lehetőségét. Ilyenkor valójában maga a rendszerterv válik inherens módon biztonságossá, és az gondoskodik róla, hogy a tűz kockázata rendkívül alacsony legyen vagy egyálta-

lán ne álljon fenn. A második megközelítés (a védekezőrendszer) a már bekövetkezett tűz észlelése és kioltása érdekében füstjelzőkre és permetezőrendszerekre épül; a kockázat tehát ebben az esetben a védőberendezések megbízhatóságától függ. A szembeszálló *(upstream)* megközelítés, a veszélyforrások kiküszöbölése vagy minimalizálása biztonságosabb rendszert eredményezhet, de egyben megkövetelheti a lemondást is bizonyos hasznokról (például az output csökkentésével vagy a fejlesztési költségek növelésével jár együtt), és előfordulhat az is, hogy ilyen megoldás nem lehetséges. Az alkalmazkodó *(downstream)* megközelítés kevesebb kompromisszumot követelhet a tervezés során, de magasabb kockázati szintet eredményezhet.

A rendszerbiztonsági elemzés magában foglalja mindezeknek az alkuknak a meghatározását és értékelését a rendszer korai tervezési szakaszaiban. Ha definícióinkat és szabványelőírásainkat a védőberendezések használatára korlátozzuk, akkor voltaképpen kizárjuk a potenciálisan eredményesebb megközelítések alkalmazását, még mielőtt azokat egyáltalán figyelembe vehettük volna. Továbbá ha a védőberendezésekre támaszkodunk, ez megoldásainkat megint csak az igen magas megbízhatóságú védőberendezések és igen nagy megbízhatóságú szoftver kifejlesztésére szolgáló módszerekre korlátozza.

Lelkesedésünkben emellett nem akarjuk sem megvalósíthatatlanul magas követelményszint felállításával a haladást korlátozni, sem pedig rossz követelmények bevezetésével nemtörődöm módon növelni a kockázatokat. Mint korábban említettük, a legtöbb szoftvertervezési technikánk hatékonysága és várható beválása tudományosan nem megalapozott. Veszélyes, ha a biztonság megteremtésére csupán egy bizonyos szoftvertervezési módszert választunk, feltételezve, hogy az hibátlan vagy igen nagy megbízhatóságú szoftvert fog eredményezni. A technológia fejlődése nyomán azok a követelmények, amelyek konkrétan előírják bizonyos megközelítések használatát, gyakran elavulttá válnak. A gyártók pedig sem erkölcsi, sem jogi értelemben nem fogják kötelességüknek érezni, hogy túlmenjenek azon, ami a szabványban elő van írva számukra.

A gyártók és mindazok, akik személyes anyagi hasznot húznak bizonyos technikák alkalmazásából, amelyek esetleg bekerülnek a szabványokba, néha domináns szerepet játszanak az előkészítési folyamatokban. Ennek eredményeként lazább követelmények vagy inkább kereskedelmi, mintsem műszaki értékű technikák alkalmazására vonatkozó javaslatok születhetnek.

Az alternatív megoldás olyan rugalmas követelmények kidolgozása, amelyek nem valamely specifikus módszert írnak elő, hanem általános kritériumokat határoznak meg valamely technika elfogadhatóságát illetően, és biztosítják, hogy azok, akik biztonsági szempontból kritikus rendszerek szoftvereit tervezik meg, rendelkezzenek a szükséges kompetenciával, és személyes felelősséget viseljenek az adott időpontban elérhető legjobb eljárások használatáért és a szóban forgó programok sajátosságaiért.

Mint az elektromosságra vonatkozóan Edison is állította, a technológia fejlődésének fokozott állami szabályozása esetleg senkinek sem válik hasznára, de elkerülhetetlenné válik, hacsak mi, a technológia fejlesztői és felhasználói nem tesszük meg a szükséges lépéseket az általunk létrehozott rendszerek biztonságos működésének, valamint az ezeket megteremtő szakemberek műszaki kompetenciájának biztosítása érdekében.

Köszönetnyilvánítás

E tanulmány kidolgozásához sokan nyújtottak számomra értékes segítséget a dolgozat korábbi változataihoz fűzött megjegyzéseikkel. Közülük szeretném kiemelni a következőket: Daniel Berry, John Gannon, Susan Gerhart, David Notkin, David Parnas, Jon Reese, John Rushby, Elaine Weyuker. Nem tételezendő fel azonban, hogy ők szükségképpen egyetértenek a tanulmányban foglalt állításokkal.

Irodalom

[1] Aitken, A. (1982): Fault Analysis. In Green, A. E. (ed.): *High Risk Safety Technology.* New York: John Wiley & Sons.

[2] Archinoff, G. H. – Hohendorf, R. J. – Wassyng, A. – Quigley, B. – Borsch, M. R. (1990): Verification of the Shutdown System Software at the Darlington Nuclear Generating Station. *Proc. Int. Conf. on Control and Instrumentation in Nuclear Installations,* Glasgow, UK., May.

[3] Bollinger, T. – McGowan, C. (1991): A Critical Look at Software Capability Evaluations. *IEEE Software,* July 1991, 25–41.

[4] Bowman, W. C. – Archinoff, G. H. – Raina, V. M. – Tremaine, D. R. – Leveson, N. G. (1991): *An Application of Fault Tree Analysis to Safety Critical Software at Ontario Hydro.* Conf. on Probabilistic Safety Assessment and Management (PSAM). Beverly Hills, April 1991.

[5] Briggs, A. (1982): *The Power of Steam.* Chicago: The University of Chicago Press.

[6] Brilliant, S. S. – Knight, J. C. – Leveson, N. G. (1990): Analysis of Faults in an N-Version Software Experiment. *IEEE Trans. on Software Engineering,* vol. SE-16, No. 2, February, 238–247.

[7] Brookes, M. J. (1982): Human Factors in the Design and Operation of Reactor Safety Systems. In Sills, D. L. – Wolf , C. P. – Shelanski, V. (eds.): *Accident at Three Mile Island: The Human Dimensions, Boulder.* Colorado: Westview Press.

[8] Brooks, F. P. (1987): No Silver Bullet: Essence and Accidents of Software Engineering. *IEEE Computer,* April 1987, 10–19.

[9] Burke, J. G. (1966): Bursting Boilers and the Federal Power. *Technology and Culture,* vol. VII, No. 1, Winter 1966, 1–23.

[10] Cameron, R. – Millard, A. J. (1985): *Technology Assessment: A Historical Approach.* Dubuque, Iowa: Kendall/Hunt Publishing Company.

[11] Dickens, Charles (1851): Household Words. In Stone, Harry (ed.) (1968): *Uncollected Writings from Household Words, 1850–1859.* Bloomington: Indiana University Press.

[12] Dickinson, H. W. (1963): *A Short History of the Steam Engine.* London: Frank Cass & Co. Ltd.

[13] Eckhardt, D. E. – Lee, L. D. (1985): A Theoretical Basis for the Analysis of Multiversion Software Subject to Coincident Errors. *IEEE Trans. on Software Engineering,* vol. SE-11, No. 12, December 1985, 1511–1516.

[14] Eckhardt, D. E. – Caglayan, A. K. – Knight, J. C. – Lee, L. D. – McAllister, D. F. – Vouk, M. A. (1991): An Experimental Evaluation of Software Redundancy as a Strategy for Improving Reliability. *IEEE Trans. on Software Engineering,* vol. SE-17, No. 7, July 1991, 692–702.

[15] Farey, J. (1827): *A Treatise on the Steam Engine: Historical, Practical, and Description.* London: Longman, Rees, Orme, Brown, and Green.

[16] Goodenough, J. B. – Gerhart, S. (1975): Toward a Theory of Test Data Selection. *IEEE Transactions on Software Engineering,* vol. SE-1, No. 2, June.

[17] Hills, R. L. (1989): *Power from Steam: A History of the Stationary Steam Engine.* Cambridge: Cambridge University Press.
[18] Johnson, W. G. MORT (1980): *Safety Assurance Systems.* New York: Marcel Dekker, Inc.
[19] Josephson, M. (1961): *Edison.* London: Eyre and Spottiswoode.
[20] Kemeny, John G. (1979): *The Need for Change: The Legacy of Three Mile Island.* Report of the President's Commission on Three Mile Island. New York: Pergamon Press.
[21] Kletz, T. (1988): Wise After the Event. *Control and Instrumentation,* vol. 20, No. 10, October, 57–59.
[22] Knight, J. C. – Leveson, N. G. (1986): An Experimental Evaluation of the Assumption of Independence in Multiversion Programming. *IEEE Trans. on Software Engineering,* vol. SE-12, No. 1, January, 96–109.
[23] Knight, J. C. – Leveson, N. G. (1990): A Reply to the Criticisms of the Knight and Leveson Experiment. *Software Engineering Notes,* January,
[24] Leveson, N. G. – Turner, C. S. *The Story Behind the Therac-25 Accidents: A Computer-Related Accident Investigation,* submitted for publication.
[25] Millard, A. J. (1990): *Edison and the Business of Innovation.* Baltimore: Johns Hopkins University Press.
[26] Millard, A. J. (1987): *A Technological Lag: Diffusion of Electrical Technology in England, 1879–1914.* New York: Garland Publishers.
[27] Parnas, D. L. (1985): Software Aspects of Strategic Defense Systems. *Communications of the ACM,* vol. 28, No. 12, December, 1326–1335.
[28] Parnas, D. L. (1987): Why Engineers Should Not Use Artificial Intelligence. Proceedings of the CIPS Edmonton '87 Conference, Edmonton, Alberta, November 16–19. Published in Schaeffer, J. – Stewart, L. (eds.): *Intelligence Integration.* Dept. of Computing Science, University of Alberta, 39–42.
[29] Passer, H. (1953): *The Electrical Manufacturers.* Cambridge, Mass.: Harvard University Press.
[30] Pursell, C. H. (1969): Early Stationary Steam Engines in America. Washington, DC: Smithsonian Institution Press.
[31] Rasmussen, J. (1987): Cognitive Control and Human Error Mechanisms. In Rasmussen, J. – Duncan, K. – Leplat, J. (eds.): *New Technology and Human Error.* New York: John Wiley & Sons,
[32] Robinson, E. – Musson, A. E. (1969): *James Watt and the Steam Revolution.* New York: Augustus M. Kelley, Publishers.
[33] Ruckelshaus, W. D. (1990): Risk, Science, and Democracy. In Glickman, T. S. – Gough, M.: *Readings in Risk.* Washington, DC: Resources for the Future.
[34] Scott, R. K. – Gault, J. W. – McAllister, D. F. (1987): Fault-Tolerant Software Reliability Modeling. *IEEE Transactions on Software Engineering,* vol. SE-13, No. 5, May, 582–592.
[35] Watts, S. (1991): Computer Watch on Nuclear Plant Raises Safety Fears. *London Independent,* Sunday, Oct. 13.
[36] Weil, V. (1984): The Browns Ferry Case. In Curd, M. – May, L. (eds.): *Professional Responsibility for Harmful Actions.* Dubuque, Iowa: Kendall Hunt.
[37] Weyuker, E. J. (1986): Axiomatizing Software Test Data Adequacy. *IEEE Trans. on Software Engineering,* vol. SE-12, No. 12, Dec, 1128–1138.
[38] Weyuker, E. J. – Weiss, S. – Hamlet, D. (1991): *Comparison of Program Testing Strategies.* Proceedings of the Fourth Symposium on Software Testing, Analysis and Verification (TAV4), Victoria, BC, Canada, Oct, 1–10.