Nagy megbízhatóságú elektronikus közlekedési alrendszerek RAMS paramétereinek kezelése

Ph.D értekezés tézisei

Szabó Géza
okleveles villamosmérnök

témavezető:
Dr. Bokor József
tanszékvezető egyetemi tanár

BME Közlekedésautomatikai Tanszék

Budapest, 2008

TARTALOMJEGYZÉK

1. BEVEZETÉS ÉS MOTIVÁCIÓ

1.1 Igény a nagy megbízhatóságra

Napjainkban az élet minden területén az ember életét, munkáját segítő gépek, berendezések alkalmazására kerül sor. A technika fejlődésével ezek a berendezések egyre bonyolultabbak, egyre több elektronikus elemet tartalmaznak.

Az alkalmazások kezdetétől fontos szempont volt egy berendezés megítélésénél az elvégzett funkciók ismerete mellett a minőség megítélése is. A minőség sok paraméter együttese, ezek közül egy – sok esetben az egyik legjelentősebb – a berendezés megbízhatósága. Megbízhatóság alatt azt a valószínűséget értjük, amivel a kérdéses berendezés a definiált funkcióit végrehajtja.

A közlekedés szinte minden területén és az ipar egyes területein kiemelten fontos a nagy megbízhatóság. Ezeken a területeken a berendezések hibás funkció végrehajtásának hatása emberéleteket vagy nagy értékű anyagi javakat veszélyeztet. Ilyen területekre példa a közlekedésnél a vasúti és a légi közlekedés, míg ipari rendszereknél a nukleáris erőművek működése, valamint egyes vegyi üzemekben lejátszódó folyamatok.

A nagy megbízhatóság, mint a minőség egyik aspektusának elérését a tervezés során már figyelembe kell venni, speciális rendszerstruktúrák alkalmazásával kell biztosítani a kívánt megbízhatósági szintet. Ugyanakkor a fentiekben felsorolt alkalmazási területeken – a tervezői hibák, tévedések kiküszöbölése érdekében – nem elégszenek meg a tervezői erőfeszítésekkel, hanem független szakértők ellenőrző munkáját is igénybe veszik. Ilyenkor a független szakértő többek között megbízhatóság-analízist végez a rendszerre, keresvén annak esetleges gyenge pontjait. Ez a független személy által készített elemzés többnyire a hatósági engedélyezés feltétele is. A megbízhatóság-analízis ennek megfelelően fontos szerepet tölt be a rendszertervezésben, és a megbízhatóság kezelése, elemzése külön tudományággá nőtte ki magát. Fontosságát jelzi az évenként megrendezésre kerülő számos nemzetközi konferencia, az igen nagyszámú nemzetközi irodalom.

Ugyanakkor a megbízhatósággal foglalkozó szakembereknek a technika fejlődése következtében mindig újabb és újabb kihívásokkal kell szembenézniük. Az elektronikus eszközök fejlődése részben olyan nagyságú, részben olyan új funkcionalitással rendelkező rendszerek létrehozását teszi lehetővé, amelyek a korábbi analízismódszerekkel nem, vagy nem hatékonyan elemezhetőek. Ugyanakkor az elméleti eredmények gyakorlati alkalmazása szintén nem problémamentes és számos megoldandó kérdést vet fel.

Jelen disszertációban egy, néhány éve bevezetett rendszermegvalósítás, a meghibásodás szempontjából vett adaptív viselkedés analízislehetőségeit vizsgáljuk meg. Elemezzük a már meglévő módszerek alkalmazási lehetőségeit és a rendszerek egy osztályára egyszerűbb analízist lehetővé tévő módszert mutatunk be. Megvizsgáljuk az automatikus analízis lehetőségét, majd elemezzük a módszerek alkalmazhatóságának feltételeit a vasúti rendszereknél.

1.2 Motivációs háttér, kutatóhelyi előzmények

A kutatómunka elindítását egyrészről a közlekedési ágazat nagy megbízhatóságú rendszerek iránti igénye motiválta. A közlekedés mindig is az egyik legveszélyesebb üzem volt, a kockázatok csökkentése régen is és napjainkban is folyamatosan napirenden van. A BME Közlekedésautomatikai Tanszék elsősorban a vasúti ágazat biztonsági kérdéseivel foglalkozik. Az ezen a területen alkalmazott biztosítóberendezési technika az ipari vezérléstechnikai terület egyik legösszetettebb, legnagyobb biztonsági igényű része. A biztosítóberendezések alkalmazhatóságának vizsgálata, a sikeres vizsgálat eredményeit összefoglaló alkalmassági tanúsítványok kiadása régóta tanszékünk legjelentősebb ipari megbízásai közé tartoznak. Ezek a munkák igényelték a legújabb európai szabványok alkalmazását is, és ezen keresztül lehetőség nyílott az ezzel kapcsolatos adaptációs vélemények és problémák megismerésére.

A disszertációban publikált kutatásokat másrészről egy valós rendszer, illetve az ott felmerült analízis igénye motiválta. A Paksi Atomerőmű Zrt. a folyamatos biztonsági fejlesztések keretén belül 1995-től folyamatosan terveztette át és cseréltette le az erőművi blokkok biztonsági felügyeletét ellátó védelmi rendszereket. Az új védelmi rendszerek a korszerű processzoros technikán alapulnak, nagy integráltságúak, számos korszerű szolgáltatást képesek nyújtani. Ugyanakkor a korábban leírtaknak megfelelően itt is igény volt, hogy a bevezetésre kerülő rendszert független szakértő cég vizsgálja felül. Ezt a feladatot az MTA-SzTAKI Rendszer- és Irányításelméleti Kutató Laboratóriuma kapta. A felülvizsgálat egyik része volt a rendszer valószínűségi alapú megbízhatóság-analízise is, melyben a szerző, mint külső szakértő vett részt. A védelmi rendszer módosításai a mai napig újabb és újabb elemzési feladatokat is igényelnek.

A disszertációban megjelenő eredmények kötődnek még a BME Elektronikus Jármű- és Járműirányítási Tudásközpont (EJJT) munkájához. A közúti közlekedésben részt vevő járművek is egy biztonságkritikus folyamat részesei, így egyes rendszereik (különös tekintettel a napjainkban egyre nagyobb teret kapó elektronikus fékrendszerekre és elektronikus kormányrendszerek tervezésére) megvalósításánál, üzemeltetésénél a kockázati alapú követelményállítás, a követelményeknek való megfelelés és a megfelelés megbízhatósági alapú bizonyítása kiemelten fontos. Ez a tény motiválta az EJJT vezetését is, amikor az EJJT indulásakor, 2005-ben önálló projektet indított a "járműrendszerek biztonsági szintjének meghatározása" témaelnevezéssel. Ebben a projektben, mint a projekt vezetője vett részt a disszertáció szerzője.

1.3 A megbízhatóság-elmélet áttekintése

A nagy megbízhatóságú rendszerek tervezési és ellenőrzési kérdéseivel (illetve általánosan a rendszerek megbízhatóságával és rendelkezésre állásával) külön tudományterület, a megbízhatóság-elmélet foglalkozik. Ez a tudományág felbontható egyrészt hardver és szoftver kérdéseket taglaló részre. A hardver kérdésekkel foglalkozó szakemberek a fizikai rendszert igyekeznek védetté tenni a véletlenszerűen fellépő (esetleg egy időben többszörösen jelentkező) fizikai meghibásodásoktól. Itt nem csak a megvalósított rendszerstruktúra lehet kritikus, de az alkalmazott hibafeltárási mechanizmusok, a felfedett hibák megszüntetésére tett intézkedések is [Apostolakis et. al.,1978], [Storey, 1996]. A szoftver kérdések között

elsősorban a tervezés fázisában bekövetkező emberi hibák és tévesztések hatásainak kivédése a cél. Itt részben a programtervezés- és programfejlesztés fázisában alkalmazott módszerek és eljárások, valamint a felépítendő szoftverstruktúra meghatározása a cél [Bittanti, 1987]. Mindkét terület foglalkozik a tervezési elvek mellett az ellenőrzés módszereivel is, és külön-külön modellezi a fellépő hibákat, rendellenességeket [Tobias és Trindade, 1998]. Mivel a két terület erősen összefügg, a két diszciplína ötvözésével néhány éve jött létre a "hardware-software co-design" néven emlegetett új tudományterület [Csertán et. al., 1996].

A megbízhatóság-elmélet egy másik megközelítés szerint felbontható tervezési és megbízhatóság-analízis részekre. Ennek a felbontásnak az előnye kettős: egyrészt együtt kezeli a hardver és a szoftver objektumokat, másrészt igazodik a tervezés során alkalmazott feladatmegosztáshoz is. A fenti felbontás tervezési részénél nehéz általános érvényű szabályokat adni a rendszerek létrehozásához, éppen ezért szakirodalom szintjén is igen kevés forrás említhető. Ezzel szemben az egyedileg tervezett rendszer jól analizálható általános módszerekkel, így a megbízhatóság-analízis tudományterület igen aktív.

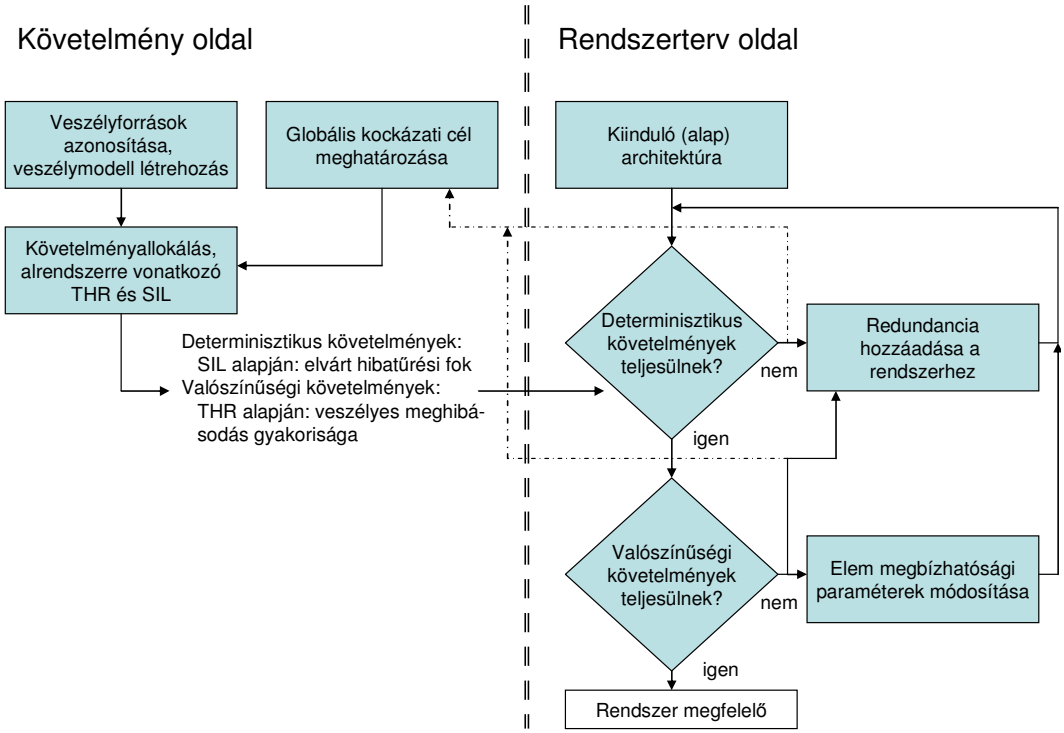
A megbízhatóság-analízis technikák közül napjainkban az egyik legelterjedtebben alkalmazott módszer a hibafa-analízis. Az eljárás kiforrott módszertannal és hatékony szoftver eszközökkel rendelkezik [Chunning és Dinghua, 1990]. A hibafa-analízis kutatások napjainkban újabb és újabb, eddig nem vagy csak körülményesen kezelhető területeket vonnak be az analízisbe. A hagyományos kétállapotú modellel dolgozó hibafa-analízis kiterjesztésre került többállapotú rendszerekhez [Aven, 1985]. Napjaink kutatásaiban a hangsúly a dinamikus rendszerviselkedések modellezésére helyeződött. Ilyen dinamikus viselkedési módot képviselnek a hidegtartalékok esetei, a késleltetetten bekövetkező események vagy a számítógépek pillanatnyi hiba miatti újraindulásai is [Dugan et. al., 1990]. A disszertációban tárgyalt hiba-adaptív rendszerkomponensek szintén a dinamikus viselkedésű objektumokhoz tartoznak, és talán mivel alkalmazásuk még nem terjedt el széleskörűen, analízisük sem megoldott.

Ugyanakkor a gazdasági szempontok fokozottan igénylik az erőforrásokkal való takarékosságot, így a karbantartás optimalizálása is előtérbe került. Ennek következményeként az analíziseknek nem csak a rendszer megbízhatóságának átlagos értékeit, hanem időbeli változását is szolgáltatniuk kell. A korábban említett újabb területek analízisbe való bevonása igényli a megfelelő időfüggő modellek kidolgozását is.

Szintén részben gazdasági szempontú az analízis automatizálásának igénye. A megbízhatóság-analízis modell létrehozási és elemzési fázisokból áll. A nehézség a modell létrehozási fázisban jelentkezik, itt a tervezéshez való szoros kötődés miatt nehéz általános módszereket létrehozni [Kocza és Bossche, 1997].

2. A KUTATÁS CÉLJAI

A kutatás a nagy biztonságú rendszerek életciklusában kiemelt fontosságú kockázati alapú követelményállítás és a követelmény-teljesülés vizsgálata területén (lásd 1. ábra, [Szabó, 2008]) kíván új eredményeket felmutatni.



1. ábra: A biztonsági követelmények specifikálása és a specifikáció teljesítése

Jelen disszertáció a megbízhatóság-analízis (biztonsági követelmények teljesülésének vizsgálata) témakörén belül három részproblémára összpontosít: 1. Definiálja a hiba-adaptív funkciókat, bemutatja megbízhatósági szempontból vett elemzésük lehetőségeit, és analízis-kiterjesztést javasol egységes kezelhetőségük érdekében [Szabó és Gáspár, 1999b]; 2. A hiba-adaptív funkciókhoz kapcsolódóan komplex megbízhatósági időfüggési modelleket vezet be [Gáspár és Szabó, 1998b]; 3. Szoftver alapú rendszerek hibafa-analíziséhez automatikus modellgenerálási algoritmust javasol [Gáspár és Szabó, 1999b], [Szabó és Tarnai, 2000], [Szabó és Csiszár, 2000a].

A megbízhatóság-elmélet alkalmazási területei elsősorban a közlekedés különböző ágazatai (elsősorban légiközlekedés és vasúti közlekedés), valamint a nukleáris erőművi technika. A közlekedés ágazataiban alkalmazott rendszerek közül a vasúti biztosítóberendezések azok, amelyek kiemelten igénylik a nagy megbízhatóságra való tervezés alkalmazását, és amelyeknél a megvalósított biztonsági szint bizonyítása is elengedhetetlen [Hudoklin és Rozman, 1985]. Minden megbízhatósági vizsgálat kritikus pontja az elfogadási kritérium meghatározása. Vasúti alkalmazások esetén az elfogadási szint származtatására többféle lehetőség kínálkozik, ezeket a lehetőségeket elemzi a disszertáció [Szabó és Tarnai, 1999], [Szabó, 2008], [Szabó et. al., 2008].

3. ÚJ TUDOMÁNYOS EREDMÉNYEK

3.1 Hiba-adaptív komponensek megbízhatóság-analízise

A hibatűrési igényű vezérlőrendszerekben, különösen a biztonságorientált ipari rendszereknél a rendelkezésre állás vagy működőképesség szintjének növelése az egyik fontos cél. Ahogy a korábbiakban már utaltunk rá, a rendelkezésre állás és a működőképesség is mérhető valószínűségként, és sok esetben már a követelmények meghatározásánál specifikálják azokat a megbízhatóságra vonatkozó valószínűségi határértékeket, amelyeket a rendszernek teljesítenie kell. Ezek a határértékek korábbi munkákból levont tapasztalatokon alapulnak vagy hatóság által előírt értékek.

A megbízhatóság növelésének általános technikái a nagyobb rendelkezésre állású komponensek alkalmazása (safe-life technika), nagyobb fokú redundancia alkalmazása, a tesztelési periódusidő csökkentése stb. A korszerű, számítógép-alapú irányítási rendszerekben alkalmazható módszer a fenti módszerek helyett vagy mellett a hiba-adaptivitás. A hiba-adaptivitás ebben az összefüggésben a berendezés azon képességét jelenti, hogy képes az általa végrehajtott funkció megváltoztatására (átkonfigurálására) a rendszerben jelen lévő, detektált hibák hatására. Ennek a hiba-adaptív viselkedésmódnak az előfeltétele a hibák (vagy azok egy részének) detektálása, és az így nyert információ eljuttatása a feldolgozó helyekre. Általános elv szerint a hibadetektálás eredményeképpen jelentkező többletinformáció (a jel detektáltan hibás vagy nem) bináris státuszinformációként hozzárendelhető magához a jelhez.

Az adaptív komponensek a dinamikus rendszerkomponensek családjához tartoznak, és speciális kezelést igényelnek a megbízhatóság-analízis (pl. hibafa-analízis) számítások során. Az adaptív komponenseket tartalmazó rendszer analízise céljára a hibafa-analízis eljárást választottuk, részben azért, mert eljárásmódszertana jól kidolgozott, és a módszertani elvek támogatására sok hatékony szoftver-eszköz létezik, részben pedig azért, mert napjainkban a megbízhatóság-elmélet új kutatási irányainak egyike éppen a különböző dinamikus viselkedések (pl. számítógép újraindulás, hideg- és melegtartalékok esete) modellezése és analízise, és a kutatók nagy része is ezt a módszert favorizálja - esetenként Markov-láncokkal kombinálva. A Markov-láncokat alkalmazó modellek nehezen felépíthetőek, de jól analizálhatóak – ezért esetenként a hibafa-modellt (amely könnyen felépíthető és szemléletes rendszerreprezentáció) Markov-láncokká konvertálják, és úgy analizálják.

A hagyományos hibafa-analízis technika kétállapotú hibamodellel dolgozik: a meghibásodás által kiváltott esemény vagy bekövetkezik, vagy nem. Amikor a hiba-adaptív viselkedésmódot modellezzük, a kétállapotú modell már nem megfelelő, mivel az eseménynek három lehetséges állapota van: nem következett be; bekövetkezett, de erről nincsen biztos információnk (nem került detektálásra); illetve bekövetkezett, és a bekövetkezésről biztos információval rendelkezünk (detektálódott). A három állapot kezelhető a hagyományos eszközökkel is, különválasztva a detektált és a nem detektált meghibásodásokat és az adaptivitást a klasszikus AND és OR kapukkal modellezve. Sajnos az átkonfigurálódó logikák egy részének modellezéséhez elengedhetetlen NOT és XOR kapuk használata is – ezek a kapuk azonban a hibafa-analízis alap-elemkészletében nincsenek benne, és a

legtöbb létező módszer nem is képes velük számolni. A detektál és nem detektált meghibásodások (illetve meghibásodási módok), két különálló eseményként való kezelése azzal a hátránnyal is jár, hogy a komplex alapesemény modellek, amelyek a meghibásodási valószínűség időfüggését írják le, nem használhatóak [Gáspár és Szabó, 1998b].

A valós életben sok olyan rendszer található, amelyek viselkedése (meghibásodási módjai, vagy pontosabban rendszerfunkció-degradációi) nem írhatóak le kétállapotú modellekkel. Az ilyen rendszerek analíziséhez többállapotú hibafa-analízis technikát fejlesztettek ki, amely általánosságban minden eseménynél *n* lehetséges degradációs állapotot kezel, és a degradációs állapotok számának azonossága sem követelmény. Ennek az analízistechnikának az alkalmazása általános esetben meglehetősen bonyolult, ami komoly alkalmazási hátrányt jelent (ellentétben a kétállapotú hibafa-analízissel, amely a leggyakrabban alkalmazott megbízhatóság-analízis technika, a többállapotú hibafa-analízist, illetve a többállapotú rendszeranalízist nagyon ritkán alkalmazzák). Ugyanakkor bizonyos szűkítő peremfeltételekkel alkalmazva a módszert, megoldást jelenthet az adaptivitás modellezésében is.

Utolsó módszerként a jelen kutatás során speciálisan a bemutatott problémakörhöz kifejlesztett, zárt képletek technikájának nevezett analízis-eljárás kerül bemutatásra, amely a vezérlőrendszerek egy osztályára (elválasztott redundanciát tartalmazó ipari biztonságkritikus rendszerek) a többi módszernél gyorsabb és pontosabb számítást biztosít.

Noha a szakirodalomban található néhány, a dinamikus rendszerviselkedés modellezésével foglalkozó cikk, a hiba-adaptív viselkedésmódra vonatkozó analízis-eljárásokkal nem lehet találkozni. A téma elméleti kérdéseivel kapcsolatos cikkeim, [Gáspár és Szabó, 1998a], [Szabó és Gáspár, 1999a], [Szabó és Gáspár, 1999b] ennek következtében az általános hibafa-analízis kutatásokon alapulnak, míg a gyakorlati alkalmazás lehetőségét az elmélet alapján tárgyaló cikkeim [Szabó és Gáspár, 1998a], [Szabó és Gáspár, 1998b] a kutatás elméleti eredményein.

I. Megállapítottam, hogy a számítógép alapú vezérlőrendszerekben megvalósított hiba-aktív és hiba-adaptív funkciók megbízhatósági analízise hibafa-analízis módszerrel elvégezhető.

I.A: Megállapítottam, hogy a kérdéses funkciók modellezésére alkalmazható a makro-modellek módszere, a Markov-láncokká konvertálás, vagy az általános többállapotú hibafa-analízis.

I.B: Zárt alakú képleteket hoztam létre a hiba-aktív és hiba-adaptív funkciók optimális modellezéséhez és analíziséhez. Az általam létrehozott zárt alakú képletek szeparált redundanciákat tartalmazó vezérlőberendezések megbízhatósági analízisénél alkalmazhatóak.

3.2 A megbízhatósági paraméterek időfüggése

A megbízhatósági paraméterek jelentős része az idő függvényében változtatja az értékét. Ez két összetevőre bontható: egyrészt a meghibásodási ráta értéke is folyamatosan változik, másrészt a paraméterek nagy része a meghibásodási ráta exponenciális függvényeként írható le (egyes paraméterek, mint pl. a tesztelhetőség általában időinvariánsak). A rendszer-megbízhatóság időfüggésének vizsgálata az

olyan helyeken kiemelten fontos, ahol előre definiált megbízhatósági limitértékeket kell teljesíteni, és ahol több részrendszer megbízhatósága az idő függvényében külön-külön változtatható.

A fentiek alapján kijelenthetjük, hogy nagy megbízhatóságú rendszerekben igen fontos az egyes komponensek paraméterei mellett a megbízhatóság időbeli változásának ismerete, a megfelelő valószínűségi modell alkalmazása az analízis során. A következőekben ezért bemutatjuk az időfüggést leíró általános, széles körben használt modelleket és ezek kiterjesztését az adaptív logikák analíziséhez (komplex modellek).

Amennyiben egy alapeseménynél detektált és nem detektált meghibásodási valószínűségekkel dolgozunk, és szükségessé válik a rendelkezésre állás időfüggésének számítása is, az előző részben megismert időfüggést leíró modelleket adaptálni kell a problémakörhöz. Az ugyanazon alapeseményhez tartozó detektált és nem detektált meghibásodások nem foghatók föl két független eseményként, és így közvetlenül nem alkalmazhatók rájuk az általános célú modellek. Ugyanakkor a létrehozandó komplex modellek is az előző részben bemutatott klasszikus modellekből származnak [Gáspár és Szabó, 1998b].

II. Megállapítottam, hogy a hiba-aktív és hiba-adaptív logikákat tartalmazó rendszerek időfüggő megbízhatóság-elemzése komplex meghibásodási modelleket igényel.

II.A: Megállapítottam, hogy a komplex meghibásodási modelleknek a detektált és nem detektált meghibásodások valószínűségének időbeli változását, mint két összefüggő eseményt kell leírniuk.

II.B: Komplex meghibásodási modelleket hoztam létre a periodikusan tesztelt komponensek számára.

3.3 Automatikus hibamodell-generálás

A nagy megbízhatóságú rendszerek (atomerőművi védelmi rendszerek, vasútbiztosító berendezések, repülőgép fedélzeti rendszerek stb.) tervezésénél nagyon fontos tervezési-ellenőrzési lépés a megbízhatósági szint determinisztikus és/vagy valószínűségi alapú igazolása [Bokor et. al., 1997]. Ehhez az igazoláshoz sokféle módszertan került kifejlesztésre, pl. a Hibamódok és hatások analízise (FMEA), Markov analízis, Eseményfa analízis, Hibafa-analízis stb. A módszerek közül egyértelműen a hibafa-analízist használják a legszélesebb körben, részben jól kidolgozott módszertana, részben a rendelkezésre álló szoftver eszközök miatt.

A hagyományos hibafa-analízis manuális hibamodell létrehozásán alapul. Ez az analízis-fázis mély rendszerismeretet, nagy rendszer- és analízis módszertani tapasztalatot igényel. Mindezek mellett a manuális modell felépítés időigényes, és így drága, valamint magában hordozza az emberi hibák, tévesztések lehetőségét. Az egész analízis-eljárás jelentősen gyorsítható, és hibamentessé tehető, amennyiben a modell létrehozása automatikusan történik. Különösen fontos lehet, hogy a hibamentes modellgenerálás verifikálható is, így az egyes analízisek hitelességének

a bizonyítására a későbbieken már csak a generálás feltételeinek betartását kell ellenőrizni, illetve maga a teljes analízis is bármikor reprodukálható.

Az automatikus hibafa-generálás a rendszerváltozatok egységes kezelését is biztosítja, és így kimerítő analízist tesz lehetővé elfogadhatóan rövid idő alatt. Ennek egyik következményeként a rendszertervezés fázisában a megbízhatóság analízis kvázi on-line módon támogathatja a fejlesztési munkát, pl. fejlesztési változatok azonnali megbízhatóság-elemzésével.

Esetünkben az automatikus hibafa-generálást még egy problémakör motiválta: a korszerű, számítógép alapú biztonsági rendszerekben adaptív viselkedésű funkciókat alkalmaznak, amelyek modellezése a hibafa-analízisben csak igen terjedelmes rész-hibafákkal lehetséges, jelentősen lassítva és bonyolítva ezzel a modell-létrehozás fázisát, és ezen keresztül az analízist.

Természetesen a világon sok helyen foglalkoztatja a kutatókat és gyakorlati szakembereket az automatikus modell-létrehozás problémaköre. Napjaink legújabb eredményei között a kifejezetten számítógépek, illetve számítógépes rendszerek alacsony szintű (komponens szintű) modellezését lehetővé tévő (e mellett a tervezést is segítő) RIDL grafikus nyelv és a hozzá tartozó hibamodell generálás kifejlesztése, az erőművek mechanikus részeinek modellezéséhez kifejlesztett KB3 tudásalapú rendszer, az analizálandó rendszer és környezete kapcsolatát modellező Formal Risk Analysis (FRA) módszer, valamint a rendszer-blokkdiagramm alapján dolgozó IRAS említhető.

A fenti munkák nagy mélységű, kimerítő analízist tesznek lehetővé, de nem veszik figyelembe a számítógépes alapú vezérlőrendszerek azon sajátosságát, hogy a megvalósított, magas szintű funkciók a hardver konfiguráció változtatása nélkül megváltoztathatók, valamint azt az ilyen rendszereknél felmerülő igényt, hogy az analízisnél az egyes rendszerkomponensek (processzor egységek, kommunikációs modulok stb.) már csak néhány meghibásodási paraméterrel legyenek modellezhetőek. Ezek az okok, valamint az előző alfejezetben bemutatott általános motiváció vezetett az alább bemutatandó eljárás kifejlesztéséhez [Gáspár és Szabó, 1999a], [Gáspár és Szabó, 1999b], valamint vasúti rendszerekben történő alkalmazásának vizsgálatához [Szabó és Tarnai, 2000].

A kifejlesztett algoritmus lépései:

1. lépés: A rendszer azon pontjának kiválasztása, amelyre az analízist szeretnénk végrehajtani. A modell-generálás típusának kiválasztása. Két fő analízis típust lehet megkülönböztetni, amelyek eltérő hibamodellt igényelnek: analízis a működés elmaradás vizsgálatára, valamint analízis a téves működések vizsgálatára.

A csúcsesemény, a kiválasztott funkció nem megfelelő működése akkor következik be, ha az a hardver egység, amelyik a funkció végrehajtásáért felelős, nem működik megfelelően, ***vagy*** ha ugyanezen hardver egység hibátlan működése mellett nem kap megfelelő parancs (bemeneti) jelkombinációt. Következésképpen a hibafában ennek modellezésére elágazás szükséges: létre kell hozni egy, a hardver meghibásodási módjait leíró ágat (HW ág), valamint egy funkcionális ágat, amely azokat a hibákat tartalmazza majd, amelyek következtében a funkció nem kap megfelelő bemeneti jelkombinációt (funkcionális ág). A két ág között OR hibafa-kapu teremt kapcsolatot.

2. lépés: A két ág létrehozása. A HW meghibásodásokat leíró ág a szabálygyűjteményben tárolt, az adott típusú hardver elem meghibásodási módjait és a szükséges paramétereket leíró adatok alapján tölthető fel. A másik ág (funkcionális ág) továbbágazik (vagy továbbágazhat) a modellezett logikai funkciónak megfelelően.

3. lépés: Az aktuálisan modellezett funkció első bemenetének keresése. A továbbiakban az így kiválasztott funkciót kezeljük aktuálisként. Ha ennek a funkciónak a végrehajtásáért más hardver egység felelős, mint az előző funkció végrehajtásáért, a hibafát két ágra kell szétválasztanunk ismételten, a hardver és a funkcionális ágra, a két ág között OR hibafa-kapu kapcsolattal (lásd az első lépésnél bemutatott okot). Ha az aktuális funkciót ugyanaz a hardver hajtja végre, mint az egy szinttel magasabban lévő funkciót, a hardver ág beszúrására nincs szükség (ez már a hibafa egy magasabb szintjén megtörtént).

4. lépés: Az aktuálisan végrehajtott funkció első bemenetének megkeresése. Ha az így megtalált funkció INPUT típusú, további funkcionális modellezésre nincs szükség, csak az input funkciót megvalósító hardvernek megfelelő hardver ágat kell létrehozni, azt is csak akkor, ha a bemeneti funkciót nem ugyanaz a hardver hajtja végre, mint ami az előzőleg vizsgált funkciót. Ennek megfelelően a bemeneti funkciók a funkcionális leírás végeit jelentik. Ha az aktuálisan megtalált funkció nem INPUT típusú lenne, ismételten vizsgálni kellene, hogy szükséges-e a hardver ág létrehozása, majd a funkcionális ágban modellezni kellene a hibaviselkedést is. Figyeljük meg, hogy innentől kezdve a 3. lépés ismétlődik egészen addig, amíg egy bemeneti funkcióhoz nem jutunk el.

5. lépés: Ha az aktuálisan vizsgált funkció bemenete INPUT funkcióhoz kapcsolódott, annak vizsgálata után, hogy szükség van-e a hardver ágra, egy speciális eljárás, az un. rollback funkció kerül végrehajtásra a generáló algoritmusban, mivel az INPUT a funkcionális leírás egyik végét jelenti, itt továbbmenni nem lehet. A rollback eljárás visszafelé megy a funkcionális leíráson, keresve egy olyan funkcionális elemet, amelynek még nem mindegyik bemenete volt feldolgozva/vizsgálva. Ennek a kivitelezéséhez minden egyes funkcionális leírásbeli elemhez egy számlálót rendelünk, amely azt mutatja meg, hogy a vizsgálat a funkcionális elem melyik bemenete irányában folytatódott. Ha ez a szám megegyezik az összes bemenet számával, az azt jelenti, hogy a funkció teljes egészében modellezésre került, és a rollback eljárás eggyel magasabb szintre térhet vissza. Ha a számláló értéke kevesebb az összes bemenet számánál, az érték eggyel növelődik, majd a 3. lépés kerül ismételten végrehajtásra, csak most nem a funkció első bemenetére, hanem a számláló által leírt sorszámúra. (Pontosan fogalmazva a 3. lépés mindig a funkció első, még nem modellezett bemenetére kerül végrehajtásra.) A hibafába új ág beszúrása szükséges, ha találtunk kaput még nem modellezett bemenettel. Hogy pontosan megmondható legyen, a hibafát melyik ponton kell folytatni, minden egyes funkcionális leírásbeli elemhez egy-egy mutatót kell rendelni, amelyik megmutatja, melyik hibafa-kapu modellezi az adott funkció bemeneti meghibásodásai és kimeneti meghibásodása közötti viszonyt.

A modellezési folyamat akkor fejeződik be, amikor a rollback eljárás vissza tud térni a kiindulási funkcióhoz úgy, hogy annak is minden bemenete feldolgozásra került.

A létrehozott algoritmust valós feladatokon, a megbízhatóság-analízisek során világszerte általánosan alkalmazott RiskSpectrum programkörnyezetben verifikáltam

[Szabó és Csiszár, 2000a], [Szabó és Csiszár, 2000b], valamint speciális vasúti alkalmazási lehetőségeit is vizsgáltam [Szabó és Tarnai, 2000].

III. Megállapítottam, hogy a számítógépes alapú ipari vezérlőrendszerek hibafa-modelljének generálása automatikus módon, a funkcionális specifikáció elsődleges feldolgozásával is lehetséges.

III.A: Megállapítottam, hogy az automatikus modell-létrehozás igényli a rendszer hardver és funkcionális leírását, és a két leírás közötti kapcsolatok megadását is. A leírásoknak formalizáltaknak kell lenniük a feldolgozhatóság érdekében.

III.B: Megállapítottam, hogy a modell-generálás a funkcionális leírás ágainak bejárásával, az egyes funkciókat végrehajtó hardver egységek, illetve egységhatárok figyelésével és hibamodellezésével valósul meg. A hibamodellezés formalizált szabályalap segítségével történhet.

III.C: Algoritmust hoztam létre az automatikus hibafa-generálás megvalósítására.

III.D: Az algoritmus működőképességét RiskSpectrum környezetbe integrált programcsomag segítségével ellenőriztem.

3.4 Megbízhatósági határértékek származtatása vasúti biztosítóberendezések vizsgálatához

A különböző közlekedési ágazatok (vizi-, légi-, közúti és vasúti közlekedés) eltérő megbízhatósági igényeket támasztanak a járműveken és az irányításban alkalmazott rendszerekkel szemben. A biztonság szempontjából legkritikusabb két alkalmazás a repülőgépek fedélzeti berendezései és a vasúti irányítás berendezései (biztosítóberendezések).

A repülőgépek fedélzeti berendezéseinél nem lehet olyan rendszerállapotot kijelölni, amelynek elérése biztonságot eredményez, így ezeknek a berendezéseknek a működőképességét mindenképpen fenn kell tartani. Ez a cél hibatűrő redundáns rendszerekkel érhető el.

A vasúti biztosítóberendezési technikában ezzel szemben biztonsági állapotnak fogadják el azt az állapotot, amikor nincsen vonatmozgás. A biztosítóberendezésben fellépő meghibásodás esetén a rendszer leállítása és a biztonsági állapot felvétele megfelelő reakció. Ezt a viselkedésmódot a hibabiztos rendszerek valósítják meg. Ugyanakkor meg kell jegyezni, hogy a folyamatos üzem fenntartása ebben az esetben is fontos lehet: nem biztonsági szempontból, hanem rendelkezésre állási (gazdaságossági) szempontból.

Új biztosítóberendezések létesítésénél, vagy módosított berendezések újbóli üzembe helyezésénél a berendezés specifikációnak való megfelelőségét bizonyítani kell. Az eljárás neve érvényesítés (validation). A megfelelőség bizonyítása kiterjed a specifikáció mindhárom területére: bizonyítani kell a funkcionális megfelelőséget, a műszaki követelmények teljesítését és a megbízhatóságra vonatkozó követelmények teljesülését is. A funkcionális és a műszaki megfelelőség bizonyítása a hardver

egységek és a kapcsolódó berendezések megfelelő, hibamentes működését feltételezi. Ezzel szemben a megbízhatósági követelmények teljesítésének vizsgálata a berendezés részegységeinek, alkatrészeinek bekövetkező meghibásodásait tételezi fel, és ilyen feltételek mellett vizsgálja a rendszer működését [Görög et. al., 1998].

Az alkalmazott vizsgálati módszerek:

- Determinisztikus vizsgálat,
- Determinisztikus vizsgálat valószínűségi adatokkal,
- Valószínűségi alapú vizsgálatok.

A valószínűségi határadatok képzése az alábbi módokon történhet:

1. A még elfogadható kockázati szintből való származtatással.
2. Más iparágban, más területen alkalmazott határértékek adaptálásával.
3. Már létező, hosszabb ideje működő berendezések biztonsági szintjének meghatározása segítségével.
4. A már üzemelő berendezések nem valószínűségi alapú vizsgálati módszereiből származtatással.

IV. Bebizonyítottam, hogy biztosítóberendezések valószínűségi alapú minősítéséhez tartozó elfogadási határértékre a korábban minősített rendszerek alapján becslés adható.

IV.A: Megállapítottam, hogy a korábban tiszta determinisztikus eljárással vizsgált berendezés alapján sem a valós biztonsági szint, sem a berendezés rendelkezésre állása nem becsülhető.

IV.B: Bebizonyítottam, hogy a korábban MÜ8004 alapú eljárással vizsgált berendezés biztonsági szintjére felső korlát számítható, amennyiben a berendezésben két egyidejű, nem detektált meghibásodás veszélyes állapotot eredményezhet. Megállapítottam, hogy az így nyert érték alkalmas újabb berendezések valószínűségi alapú vizsgálatához elfogadási küszöbértéknek. A felső korlát értéke nem függ a berendezésben alkalmazott elemek megbízhatóságától, csak a vizsgálatnál a második hiba fellépési idő számítására használt képletben alkalmazott segédszorzótól. Javaslatot adtam a felső korlátra, a javasolt valószínűségi határérték 10^{-6}.

IV.C: Megállapítottam, hogy a korábban MÜ8004 alapú eljárással vizsgált berendezés rendelkezésre állási szintje nem becsülhető.

4. REFERENCIÁK

4.1 A disszertáció és a tézisek témakörében megjelentetett saját publikációk

[Bartha et. al., 2005]: Bartha T. – Varga, I. – Soumelidis, A. – **Szabó, G**.: Implementation of a Testing and Diagnostic Concept for an NPP Reactor protection System. *In: Dependable Computing – EDCC-5 (Eds. M. Dal Chin, M. Kaaniche, A. Pataricza). Proceedings of the 5th European Dependable Computing Conference. Springer*, pp. 391-402, Budapest, 2005.

[Bokor et. al., 1997]: Bokor, J. - **Szabó G.** - Gáspár P. - Hetthésy J.: Reliability Analysis of Protection Systems in NPPs Using Fault-Tree Analysis Method. *Proceedings of the IAEA Symposium on Computerized Reactor Protection and Safety Related Systems in Nuclear Power Plants*, pp 91-104, Budapest, 1997.

[Gáspár és Szabó, 1998a]: Gáspár P. - **Szabó G.**: Analysis of Adaptive Multi-State Logic in Fault-Tolerant Systems. *Proceedings of the Probabilistic Safety Assesment and Management - PSAM 4 Conference*, pp. 13-17, New York, 1998

[Gáspár és Szabó, 1998b]: Gáspár P. - **Szabó G.**: Complex Failure Models for Dependability Assessment. *Digest of FastAbstracts, International Symposium on Fault Tolerant Computing, FTCS-28*, pp 94-95. Munich, 1998.

[Gáspár és Szabó, 1999a]: Gáspár P. - **Szabó G.**: Automatic Fault-Tree Generation as a Part of a Complex Development System. *Proceedings of the 3rd Inernational Scientific Conference Elektro '99, Section Information & Safety Systems*, pp. 19-24, Zilina, 1999.

[Gáspár és Szabó, 1999b]: Gáspár P. - **Szabó G.**: On-line System Verification Applying an Automatic Fault-Tree Generation Method Integrated into Development Tools. *Proceedings of the European Safety and Reliability Conference-ESREL* pp. 809-814, Münich, 1999.

[Görög et. al., 1998]: Görög B. - **Szabó G.** - Tarnai G.: Biztosítóberendezési funkciók PLC-s megvalósításának biztonsági és megbízhatósági szempontú elemzése. *Vezetékek Világa, Magyar Vasúttechnikai Szemle, 1998. Vol. 3. pp. 6-10.*

[Szabó és Csiszár, 2000a]: **Szabó G.** – Csiszár Z.: Fault-Tree Synthesis: a Practical Approach. *TU Budapest, Research News, Special Issue 2000.*

[Szabó és Csiszár, 2000b]: **Szabó G.** – Csiszár Z.: Automatikus hibafa generálás – Tanszéki kutatási jelentés. *BME Közlekedésautomatikai Tanszék*, 2000.

[Szabó és Gáspár, 1998a]: **Szabó G.** - Gáspár P.: Probabilistic Dependability Analysis of Adaptive Functions: A Fault-Tree Based Approach and Its Application in Transportation. *Periodica Politachnica Ser. Transp. Eng., 1998. Vol. 26, No 1-2, pp. 187-200.*

[Szabó és Gáspár, 1998b]: **Szabó G.** - Gáspár P.: Practical Aspects of Dependability Analysis for Vehicle Systems. *Proceedings of the 6th Mini Conference on Vehicle System Dynamics, Identification, and Anomalies, VSDIA*, pp. 437-446. Budapest, 1998.

[Szabó és Gáspár, 1999a]: **Szabó G.** - Gáspár P.: Fault-tree analysis of System Functionality modelled as Binary Adaptive Functions*. Proceedings of the European Safety and Reliability Conference-ESREL* pp. 1033-1038, Münich, 1999.

[Szabó és Gáspár, 1999b]: **Szabó G.** - Gáspár P.: Practical Treatment-Methods of Adaptive Components in the Fault-Tree Analysis*. Proceedings of the Annual Reliability and Maintainability Symposium*, pp. 97-104, Washington D.C., 1999

[Szabó et. al., 2008]: **Szabó G.** – Sághi B. –Darai L.– Jakubovics J. – Héray T. – Kirilly K. – Buzás M. – Gál I.: Biztosítóberendezések időszakos vizsgálatainak koncepciója. *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2008.

[Szabó et. al., 2004]: **Szabó G.** – Szabó K. – Zerényi R.: Safety Management Systems in Transportation: Aims and Solutions. *Periodica Politechnica, Ser. Transp. Eng, 2004.* Vol. 32. No. 1-2, pp. 123-134., 2004.

[Szabó és Tarnai, 1999]: **Szabó G.** - Tarnai G.: Dependability Analysis of Interlocking Systems - A Comparison of the Probabilistic and the Deterministic Approaches. *Proceedings of the 3rd Inernational Scientific Conference Elektro '99, Section Information & Safety Systems*, pp. 7-12, Zilina, 1999.

[Szabó és Tarnai, 2000]: **Szabó G.** - Tarnai G.: Automatic Fault-Tree Generation as a Support for Safety Studies of Railway Interlocking Systems*. Proceedings of the IFAC Symposium on Control in Transportation Systems*, pp. 453-458, Braunschweig, 2000.

[Szabó és Tarnai, 2002]: **Szabó G.** – Tarnai G.: A vasúti biztosítóberendezések biztonságigazolási módszereinek fejlődése, az új, eurokonform szabályozás alkalmazásának kérdései. *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2002/4. szám, 5-9 oldal, 2002.

[Szabó és Tarnai, 2003]: **Szabó G.** – Tarnai G.: A vasúti biztonság bizonyítására vonatkozó új európai szabványok alkalmazási kérdései. *Vezetékek Világa, Magyar Vasúttechnikai Szemle*, 2003/1. szám, 2-6 oldal, 2003.

[Szabó, 1995]: **Szabó G**.: Bevezetés a hibafa-analízisbe. Oktatási segédlet*. BME Közlekedésautomatikai Tanszék*, 1996.

[Szabó, 2007a]: **Szabó G.:** Kockázati alapú fejlesztési kritériumok a járművek biztonsági rendszereinél. *Jövő Járműve*, 2007/1-2 szám, 38-41 oldal, 2007.

[Szabó, 2007b]: **Szabó G**.: Műszaki okú kockázatok kezelése a közlekedésben. *Innováció és fenntartható felszíni közlekedés c. konferencia.* Magyar Mérnöki Akadémia, 2008. Az előadás anyaga elektronikusan elérhető: http://kitt.bmf.hu/mmaws/2007/pages/participants.html.

[Szabó, 2008]: **Szabó, G**.: Setting Up the Concept of Periodic Testing and Examinations of Safety Systems. *In: Formal Methods for Automation and Safety in Railway and Automotive Systems (Eds. G. Tarnai, E. Schnieder). Proceedings of Symposium FORMS/FORMAT2008*. pp. 321-324, Budapest, 2008.

4.2 A kivonatban hivatkozott idegen munkák

[Apostolakis et. al.,1978]: Apostolakis, G. - S. Garribba - G. Volta, (Eds.): Synthesis and Analysis Methods for Safety and Reliability Studies. *Plenum*, 1978.

[Aven, 1985]: Aven, T.: Reliability evaluation of multistate systems with multistate components. *IEEE Transactions on Reliability*, Vol. R-34, No. 5., pp. 473-479. 1985.

[Bittanti, 1987]: Bittanti, S. (ed.): Software Reliability Modelling and Identification. *Springer-Verlag*, 1987.

[Chunning és Dinghua, 1990]: Chunning, Y. - S. Dinghua: Classification of fault trees and algorithms of fault tree analysis. *Microelectronics and Reliability*, Vol. 30, No. 5, pp. 891-895. 1990.

[Csertán et. al., 1996]: Csertán Gy. – Pataricza A. – Selényi E.: Design for Testability with HW-SW Co-design. *Periodica Polytechnica*, Vol 40(1), pp. 25-37, 1996.

[Dugan et. al., 1990]: Dugan, J. B. - S. J. Bavuso - M. A. Boyd: Fault trees and sequence dependencies. *Proc. of the Annual Reliability and Maintainability Symp.*, 1990, pp. 286-293.

[Hudoklin és Rozman, 1985]: Hudoklin, A. - V. Rozman: Safety Analysis of the Railway Traffic System. *Reliability Engineering and System Safety,*. Vol. 37, No. 3., pp. 7-13. 1985.

[Kocza és Bossche, 1997]: Kocza G. - A. Bossche: Automatic fault-tree synthesis and real-time tree trimming, based on computer models, *Proc. Ann. Reliability & Maintainability Symp.*, 71-75.,1997

[Storey, 1996]: Storey, N: Safety-Critical Computer Systems. *Addison-Wesley*, 1996.

[Tobias és Trindade, 1998]: Tobias, P. –D. Trindade: Applied Reliability. *Chapman &Hall /CRC*, 1998.