

BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
KÖZLEKEDÉS TUDOMÁNYSZAK

FORMÁLIS MÓDSZEREK ALKALMAZÁSA
A VASÚTBIZTOSÍTÓ TECHNIKÁBAN

PhD TÉZISEK

SÁGHI BALÁZS
okl. közlekedésmérnök

Témavezető:
Dr. habil. TARNAI GÉZA
egyetemi tanár

BUDAPEST, 2003. JANUÁR

I. A KUTATÁS ELŐZMÉNYEI ÉS A KITŰZÖTT KUTATÁSI FELADAT

Formális módszerek alatt olyan eljárásokat értünk, amelyek során matematikai jelöléseket (például logikai vagy halmazelméleti kifejezéseket) használunk egy adott rendszer jellemzőinek leírására az egyes életciklus fázisokban. A formális módszerek matematikai bázisát jellemzően egy formális specifikációs nyelv biztosítja. Ez az alap lehetőséget nyújt a rendszer tulajdonságainak (mint pl. konzisztencia, teljesség, helyesség) formális leírására mind a specifikáció, mind az implementáció vonatkozásában. A formális módszerek ennek megfelelően felölelik a rendszerek életciklusának egyes fázisaiban alkalmazható formális specifikációs, formális fejlesztési, tervezési technikákat, valamint a matematikai alapú validációs és verifikációs technikákat [Inc92] és ilyen módon lehetőséget nyújtanak ahhoz, hogy a rendszerek életciklusának egyes fázisaihoz kapcsolódó tevékenységeket rendszerezetten, szisztematikus módon lehessen elvégezni.

A formális módszerek fejlesztése az 1960-as évek közepén kezdődött. Az alkalmazások területén az első jelentős áttörés a 80-as és a 90-es évek fordulójára tehető, az utóbbi években pedig ugrásszerűen nő a formális módszerek iránti igény.

A MÁV első elektronikus biztosítóberendezésének specifikációs munkáiban való részvételem során alkalmam volt személyesen is tapasztalni a hagyományos (nagyreszt szöveges) specifikációs technikák hiányosságait.

Az elmúlt években a rendszereket fejlesztő szervezetek egy része felismerte, hogy a bonyolult rendszerek fejlesztésének és karbantartásának kéz-bentartathóságához új eljárásokra, módszerekre van szükség. Számos szervezet a formális módszerekben találta meg ezeket az eljárásokat, aminek következtében az tapasztalható, hogy a formális módszerek alkalmazási köre jelentősen nőtt a korábbiakhoz képest [Cra93].

A formális módszerek alkalmazásának elsődleges célja a vasútbiztosítás területén, hogy olyan eszközt biztosítson a megrendelők, a fejlesztők, a hatósági szakemberek és a szakértők számára, amelynek segítségével a rendszerek helyességének biztosítása és bizonyítása e speciális szakterületen megbízhatóan, költség-hatékonyan elvégezhető.

A fentiek ellenére a formális módszerek alkalmazhatóságának tekintetében általánosan is, és a vasúti biztosítóberendezések szakterületén speciálisan is egyfajta szakadék figyelhető meg a tudományos világ által nyújtott lehetőségek és a gyakorlati alkalmazások által elvártak között.

E szakadék áthidalásának érdekében napjainkban számos törekvés figyelhető meg.

A Német Kutatóközösség (DFG) kiemelt programjai között szerepel a szoftver specifikáció problematikája. Ennek keretében a Berlieni Műszaki Egyetem vezetésével vizsgálják a formális technikák alkalmazhatóságát.

Az Európai Unió által támogatott FME (Formal Methods Europe) projekt FME Rail dániai központú munkacsoportja 1998-99 folyamán öt szemináriumot tartott a formális technikák vasúti alkalmazásairól. Ezekben több mint 200 vasúti informatikus vett részt Angliából, Ausztriából, Hollandiából, Franciaországból és Svédországból [FMERail98-99].

A német Szövetségi Vasúti Hivatal (EBA) a formális specifikációk alkalmazását alapvetően olyan támogatandó előrelépésnek tekinti a vasúti és a gyári feltétfüzetek szintjén, amely mind a vasutaknak, mind az iparnak és az EBA-nak is hasznos. Igen nagy nehézségekkel kell azonban szembenézni, ha minden egyes kérelmező speciális elképzelésekkel és megoldásokkal jelentkezik az EBA-nál. Ezért a Braunschweigi Műszaki Egyetem Szabályozástechnikai és Automatizálási Intézete (IfRA), valamint a Német Vasút Kutatási és Technológiai Központja (FTZ) által 1998 májusában szervezett, a formális módszerek vasútbiztosítási alkalmazásával foglalkozó FORMS szimpózium [FORMS98] résztvevői egy munkabizottságot hoztak létre azzal a céllal, hogy az konszenzust teremtsen a gyártók (ipar), a felhasználók (DB AG) és a felügyeleti hatóság (EBA) között, a formális módszerek alkalmazásával kapcsolatban.

A FORMS szimpóziumot 1998-as indulása után 1999-ben és 2000-ben is megrendezték. Az 1999-es FORMS [FORMS99] célja az előbbieken említett munkabizottság által kidolgozott Követelménykatalógus (a vasúti biztosítóberendezési szakterület követelményei a formális módszerekkel kapcsolatban) megvitatása volt. A 2000-ben megtartott szimpózium [FORMS00] célja pedig az egyes formális módszerek vasúti alkalmazhatóságának összehasonlító értékelése volt.

A fenti törekvések azonban mindeddig nem érték el kitűzött céljukat. Ennek elsődleges okát abban látom, az eddigi kutatások nem veszik figyelembe a vasúti biztosítóberendezési rendszerek bizonyos jellegzetességeit, illetve a biztosítóberendezések fejlesztésének egyes sajátosságait.

Kutatásom célja ennek megfelelően az volt, hogy

- tisztázzam és egyértelműen leírjam a vasúti biztosítóberendezések szakterületének néhány olyan jellegzetességét, amelyek a formális módszerek alkalmazására hatással vannak, továbbá hogy
- olyan irányelveket határozzak meg, amelyek kijelölik a formális módszerek alkalmazásának lehetséges módjait a vasútbiztosító technikában.

A formális módszerek alkalmazási módszertanával foglalkozó irodalmak közül ki kell emelni J. Wing [pl. Win90] munkáit, amelyekben a formális módszerek alapfogalmait az alkalmazási módszertan szempontjából definiálja. A formális módszerek gyakorlati alkalmazásával, annak problémáival, illetve a formális módszerekkel kapcsolatos tévhitekkel foglalkozik A. Hall [Hal90]. A formális módszerek biztonságkritikus rendszerek területén történő alkalmazásával több publikációjában foglalkozik J. Bowen [Bow92, Bow93a, Bow93b, Bow94a, Bow94b].

A formális módszerek vasútbiztosítási alkalmazásával elsősorban a fent említett kutatócsoportok és munkabizottságok foglalkoznak [FMERail, FORMS].

A szakirodalomban számos, a formális módszerek alkalmazására vonatkozó szempont található, legátfogóbban [NASA95, NASA97]-ben. További alkalmazási szempontokat tárgyal [Ehr99, Bow93b, Bow94b, Cra93, Tho95, Pat01, Lar96, Hal90, Win90]. Ezek a szempontok azonban több, kutatási témám szempontjából fontos tényezőt nem vesznek figyelembe, és nem képeznek egységes rendszert.

A FORMS munkabizottsága által kidolgozott Követelménykatalógusról [Anf99] elmondható, hogy a követelmények egy része inkább a rendszerfejlesztéssel általában, nem pedig kifejezetten a formális módszerekkel kapcsolatos elvárás, továbbá hogy a dokumentum többségében olyan általános érvényű követelményeket fogalmaz meg, amelyek nemcsak a vasútbiztosítási szakterületen, hanem bármely más alkalmazási területen is érvényesek.

Az előbbieket miatt vált szükségessé az irodalomból ismert szempontoknak újabakkal való kiegészítése, és a bővítés révén rendelkezésre álló szempontok rendszerezésével egy egységes alkalmazási szempontrendszer kidolgozása, továbbá a Követelménykatalógus kritikai megjegyzésekkel, illetve kiegészítésekkel történő ellátása annak érdekében, hogy alkalmasabbá váljon eredeti céljának elérésére.

II. A KUTATÁS MÓDSZERE

A kitűzött kutatási cél meghatározta számomra a kutatás irányát, és a kutatómunka egyes fázisaiban alkalmazandó módszereket. A kutatás egyes lépéseinek sorrendje tükröződik az új tudományos eredmények egymásra épülésében is.

A formális módszerek vasúti biztosítóberendezési alkalmazásával foglalkozó szakirodalmat megvizsgálva azt tapasztaltam, hogy a formális módszerek e területen való alkalmazhatóságának egyik gátja az, hogy a biztosítóberendezések fejlesztési folyamatának ismert leírásai nem minden szempontból tükrözik a valóságos fejlesztési folyamatot. Ezért a formális módszerek vasútbiztosítási alkalmazásához előzetesen meg kellett vizsgálnom a vasúti biztosítóberendezések életciklusát. E vizsgálatok eredményeként az ismert életciklus-modellek továbbfejlesztésével olyan modellt dolgoztam ki, amely a biztosítóberendezések fejlesztési folyamatát adekvát módon képezi le (1. tézis), így alapul szolgálhat a formális módszerek alkalmazhatóságának további vizsgálataihoz.

Ezt követően meghatároztam azokat a tényezőket, amelyek a hagyományos fejlesztési módszereken túlmutató módszerek alkalmazását teszik szükségessé a rendszerfejlesztésben általában, fokozottan a biztonságkritikus rendszerek területén, illetve ezen belül speciálisan a vasúti biztosítóberendezések szakterületén.

Megvizsgálva a formális módszerek alapvető jellemzőit, és az előbbi igényt figyelembe véve, meghatároztam azokat az előnyöket, amelyek a formális módszereknek a vázolt területeken történő alkalmazásával elérhetők.

Ezután megvizsgáltam azokat a szempontokat, amelyek az alkalmazhatóságra, illetve az alkalmazás hatékonyságára, sikerére nézve hatással lehetnek. A szakirodalomban található szempontokat újabakkal kiegészítve, egységes alkalmazási szempontrendszer hoztam létre (2. tézis).

Ezt követően elvégeztem a formális módszerek vasútbiztosítási alkalmazásának szakirodalmában alapvető szerepet betöltő Követelménykatalógus [Anf99] kritikai elemzését. Vizsgálatom eredményei azt mutatták, hogy a Követelménykatalógusban szereplő követelmények, illetve azok megfogalmazása nem teszi lehetővé, hogy a dokumentum elérje kitűzött célját. Ezért a Követelménykatalógust olyan kritikai észrevételekkel és értelmező jellegű kiegészítésekkel láttam el, amelyek révén eredeti célkitűzésének elérésére alkalmasabbá vált (3. tézis). Ezen eredmény elérése érdekében a

Braunschweigi Műszaki Egyetemen személyes konzultációt is folytattam a Követelménykatalógus kidolgozóival.

A formális módszerek vasútbiztosítási alkalmazásának vizsgálatához elengedhetetlen volt az ismert gyakorlati alkalmazások áttekintése. A gyakorlati alkalmazásokat a disszertációban kidolgozott, egységes alkalmazási szempontrendszer, illetve az általam kiegészített Követelménykatalógus szerint értékeltem.

Megvizsgáltam a Petri-hálóknak mint elterjedt modellezési eszköznek a jelfogós vasúti biztosítóberendezési rendszerek működésének leírására való alkalmasságát. Ennek kapcsán értékeltem a Petri-hálón alapuló hagyományos logikai modellezési eljárást és új modellezési technika alkalmazására tettem javaslatot (4. tézis).

Az általános érvényű alkalmazási szempontrendszeren alapulva, a vasúti sajátosságokat, illetve az ismert gyakorlati alkalmazások tanulságait figyelembe véve irányelveket határoztam meg a formális módszerek vasútbiztosítási alkalmazásához (5. tézis).

Végezetül, modellt dolgoztam ki a formális módszerek vasúti biztosítóberendezési területen történő bevezetésére (6. tézis). A modell elkészítéséhez előzetesen meghatároztam a vasúti biztosítóberendezések életciklusának azon fázisait, amelyeknek a formális módszerek bevezetése szempontjából megkülönböztető szerepe van. A modell kidolgozása során figyelembe vettem a vasúti biztosítóberendezések fejlesztési folyamatának sajátosságait, illetve a fejlesztési folyamat résztvevőinek a formalizálással kapcsolatos érdekltségét is.

III. ÚJ TUDOMÁNYOS EREDMÉNYEK

1.

Megvizsgáltam az informatikai, illetve folyamatirányító rendszerekre vonatkozó, a szakirodalomban található fejlesztési életciklus modelleket. Ezeket összevetve a biztonságkritikus rendszerek, speciálisan a vasúti biztosítóberendezési rendszerek fejlesztésének gyakorlatával, megvizsgáltam e modelleknek az említett speciális területeken való érvényességét, alkalmazhatóságát.

Megállapítottam, hogy a vizsgált modellek struktúrája nem teszi lehetővé a biztonságkritikus, ezen belül a vasútbiztosító rendszerek fejlesztésére jellemző egyes részfolyamatok adekvát leképezését, ezért e modelleknek a vizsgált területen való alkalmazhatósága korlátozott.

1. tézis. *Olyan modellt dolgoztam ki a vasúti biztosítóberendezési rendszerek specifikációs folyamatára, amely az irodalomban található modellekhez képest figyelembe veszi e folyamat általánostól eltérő, alkalmazás-specifikus jellegzetességeit. A kidolgozott modell*

- *megkülönbözteti és a fejlesztési folyamatban elhelyezi a vasúti biztosítóberendezési rendszer különböző szintű specifikációit (vasúti feltétfüzet, rendszerspecifikáció és gyári feltétfüzet), illetve az előállításukkal kapcsolatos tevékenységeket;*
- *új elemként veszi figyelembe és megfelelően kezeli a vasúti specifikációs folyamat többszereplős jellegéből szükségszerűen adódó iterativitást, továbbá*
- *tükrözi a vasúti biztosítóberendezések fejlesztésének azon jellegzetességét, hogy a gyártó cégek gyakran meglévő ún. alaprendszerük továbbfejlesztésével vagy adaptálásával igyekeznek kielégíteni egy adott vasúti feltétfüzet követelményeit.*

Az 1. tézis a disszertáció 1.1. fejezetén, valamint az [1], [2], [3], [5] és [8] publikációkon alapul.

2.

A szakirodalomban számos, a formális módszerek alkalmazására vonatkozó szempont található, ezek azonban

- több fontos tényezőt nem vesznek figyelembe, és
- nem képeznek egységes rendszert.

2. tézis. *Az irodalomból ismert szempontoknak újabbakkal való kiegészítésével, és a bővítés révén rendelkezésre álló szempontok rendszerezésével olyan, a formális módszerek alkalmazására vonatkozó egységes szempontrendszert dolgoztam ki, amelyik magába foglalja a formális módszerek alkalmazásának*

- *szigorúságát,*
- *terjedelmét,*
- *műszaki szempontjait,*

- *adminisztratív szempontjait,*
- *költségeit, korlátait és nehézségeit.*

A szempontrendszer gyakorlati alkalmazhatósága érdekében az egyes szempontokat kiegészítettem az adott szempontra vonatkozó elméleti és gyakorlati alkalmazási megfontolásokkal is.

A kidolgozott szempontrendszer lehetőséget nyújt a korábban részben intuitív alapon megvalósított alkalmazások objektívebb értékelésére és ennek alapján az újabb alkalmazások számára optimális alkalmazási paraméterek meghatározására.

A kidolgozott, általános érvényű szempontrendszer alapján, egy-egy alkalmazási terület (pl. vasúti biztosítóberendezések) sajátosságait figyelembe véve mód nyílik az adott terület számára érvényes speciális alkalmazási irányelvek meghatározására is (*lásd* 5. tézis).

A 2. tézis a disszertáció 3. fejezetén, valamint a [3], [5], [7], [8], [9] és [10] publikációkon alapul.

3.

Megvizsgáltam és értékeltem a szakirodalomban alapvető szerepet betöltő, a vasútbiztosítás területére alkalmas formális módszerek kiválasztásának elősegítését célzó Követelménykatalógust [Anf99].

Megállapítottam, hogy

- a követelmények egy része inkább a rendszerfejlesztéssel általában, nem pedig kifejezetten a formális módszerekkel kapcsolatos elvárás,
- a dokumentum többségében olyan általános érvényű követelményeket fogalmaz meg, amelyek nemcsak a vasútbiztosítási szakterületen, hanem bármely más alkalmazási területen is érvényesek.

Ennek alapján a Követelménykatalógusban szereplő követelmények, illetve azok megfogalmazása nem teszi lehetővé, hogy a dokumentum elérje kitűzött célját.

A részletes értékelés során

- az egyes követelményekkel kapcsolatban módszertani és tartalmi bírálatokat fogalmaztam meg,

- a követelményekhez részben általános érvényű, részben pedig kifejezetten a vasúti biztosítóberendezési rendszerek területét érintő, értelmező jellegű kiegészítéseket fűztem.

3. tézis. *A szakirodalomban alapvető szerepet betöltő Követelménykatalógust alkalmassá tettem arra, hogy az általam megfogalmazott alkalmazási szempontrendszerrel (2. tézis) együtt a vasútbiztosítás meghatározott részfeladatai számára alkalmas formális módszerek kiválasztását és adekvát alkalmazását elősegítse.*

A 3. tézis a disszertáció 4. fejezetén, valamint a [9] publikáción alapul.

4.

Megvizsgáltam a Petri-hálóknak mint elterjedt modellezési leíróeszköznek a jelfogós vasúti biztosítóberendezési rendszerek leírására való alkalmazhatóságát. Megállapítottam, hogy a logikai rendszerek leírására kialakult szokásos modellezési eljárás jelfogós hálózatok modellezésére csak korlátozottan alkalmas.

4. tézis. *Olyan új, Petri-hálón alapuló, ún. áramutas modellezési eljárást fejlesztettem ki jelfogós hálózatok modellezésére, amelynek alkalmazása révén a hagyományos, ún. állapotmodellezési eljáráshoz képest*

- *a modell elkészítése egyszerűbbé,*
- *a modell mérete kisebbé,*
- *a modell maga áttekinthetőbbé válik,*
- *a jelfogók működése pedig valóságghűbb módon modellezhető.*

A 4. tézis a disszertáció 6. fejezetén, valamint a [6] publikáción alapul.

5.

5. tézis. *Irányelveket dolgoztam ki a formális módszereknek a vasúti feltétfüzetek, illetve a gyári feltétfüzetek elkészítése során való alkalmazására. A kidolgozott irányelvek ezen életciklus-fázisokra vonatkozóan meghatározzák a formális módszerek alkalmazásának szigorúságát, terjedelmét, műszaki és adminisztratív szempontjait. Ezenfelül, az irányelvek vonatkoznak a vasúti és a gyári feltétfüzetek közötti átjárhatóságra, továbbá a formális módszereknek a vasúti*

biztosítóberendezések életciklusának egyéb fázisaiban való alkalmazhatóságára is.

Az irányelvek meghatározásához előzetesen elvégeztem a formális módszerek ismert vasútbiztosítási alkalmazásainak értékelő elemzését.

Az alkalmazási irányelveket a 2. tézisben megfogalmazott általános alkalmazási szempontrendszer alapján,

- a vasúti biztosítóberendezési terület sajátosságainak (1. és 3. tézis), valamint
- az előbbieken említett értékelő elemzés eredményeinek figyelembevételével határoztam meg.

Az 5. tézis a disszertáció 7.1.-7.4. fejezetein, valamint a [11] és [12] publikációkon alapul.

6.

6. tézis. *Olyan többlepcsős modellt dolgoztam ki a formális módszerek alkalmazásának a vasúti biztosítóberendezési rendszerek fejlesztése területén történő bevezetésére, amelynek egyes fázisait a vasúti, illetve a gyári feltétfüzet formalizáltsági szintje határozza meg.*

A modell elkészítéséhez meghatároztam a vasúti biztosítóberendezések életciklusának azon fázisait, amelyeknek a formális módszerek bevezetése szempontjából megkülönböztető szerepe van, és figyelembe vettem

- a vasúti biztosítóberendezések fejlesztési folyamatának sajátosságait, ezen belül
- a vasúti feltétfüzetek és a gyári feltétfüzetek előállításával kapcsolatos szempontokat,
- a formális módszerek, illetve azok alkalmazásának jellemzőit, valamint
- a fejlesztési folyamat résztvevőinek a formalizálással kapcsolatos érdekeltségét.

A modell kijelöli az egyes szinteken a vasúti feltétfüzet és a gyári feltétfüzet közötti transzformáció lehetséges módját is.

A 6. tézis a disszertáció 7.5. fejezetén, valamint a [11] és [12] publikációkon alapul.

IV. AZ ÚJ TUDOMÁNYOS EREDMÉNYEK HASZNOSÍTHATÓSÁGA

Napjainkra a formális módszerek alkalmazásához gazdag módszer- és eszkörendszer alakult ki. A vasúti biztosítóberendezési alkalmazásnak azonban mindezidáig több gátja is volt; a tudományos világ által kínált lehetőségek és a gyakorlati alkalmazás elvárásai között egyfajta szakadék található. A kutatás elvégzésével és a disszertáció kidolgozásával célom az volt, hogy ezt a hiányt áthidaljam, vagy legalábbis csökkentsem.

A tézisekben megfogalmazott új tudományos eredményeket részleteiben több hazai és nemzetközi fórumon ismertettem.

A kutatási feladat eredményes megoldása elősegíti a témában folytatott korábbi tudományos eredmények gyakorlati alkalmazását, illetve az alkalmazások fokozatos bevezetését a vasúti biztosítóberendezési rendszerek szakterületén.

Az 1. tézisben szereplő fejlesztési modell elsősorban a gyakorlati alkalmazást célzó további kutatások számára lehet iránymutató.

A 2. tézisben bemutatott alkalmazási szempontrendszer egyaránt hasznos lehet a vasúti biztosítóberendezések szakterületét kutatók számára, és az ezen a területen tevékenykedő gyakorlati szakemberek számára.

A 3. tézis eredményei, az 1. tézishoz hasonlóan, elsősorban a tématerület további kutatásaiban hasznosíthatók.

A 4. tézisben kidolgozott áramutas modellezési eljárás, egy további kutatás tárgyát képező elemző módszerrel kiegészítve, előnyösen alkalmazható jelfogós kapcsolások, biztosítóberendezések, illetve azok egyes részeinek vizsgálatára.

Az 5. tézis alkalmazási irányelveit mind a további kutatásokban, mind a jövőbeni gyakorlati alkalmazások esetén fel lehet használni.

Végezetül, a 6. tézis modellje alapot teremthet a formális módszerek vasútbiztosítás területén történő bevezetéséhez; többek között alkalmas lehet egy személyi és tárgyi feltételeket meghatározó bevezetési stratégia kialakítására.

V. AZ ÉRTEKEZÉS TÉMAKÖRÉBŐL SZÜLETETT PUBLIKÁCIÓIM

- [1] Tarnai, G., **Sághi, B.**: Application of Formal Methods for Specification of Safety-Relevant Traffic Process Control Systems” *INTCOM ‘98 Symposium on Intelligent Systems in Control and Measurement* Miskolc-Lillafüred, 1998. november 21-27. pp. 237-244.
- [2] Tarnai G., **Sághi B.**: Erhöhung der Bahnsicherheit durch formale Methoden. *Periodica Polytechnica, Transportation Engineering*, Vol. 26, No 1, Budapest, 1999. pp. 175-186.
- [3] Tarnai G., **Sághi B.**: Einsatz von formalen Methoden in die Eisenbahnsicherungstechnik. *ZEL ‘2000 7. internationales Symposium*. Žilina, Szlovákia, 2000. május 30-31. pp. 80-88.
- [4] Tarnai G., **Sághi B.**: Method for the Development of a Special Railway Interlocking Subsystem. *9th IFAC Symposium on Control in Transportation Systems*. Braunschweig, Németország, 2000. június 13-15., pp. 495-500.
- [5] Tarnai G., **Sághi B.**: Formális módszerek alkalmazása a vasútbiztosító technikában. *Vezetékek Világa. Vasúttechnikai szemle*. Budapest 3/2000 pp. 11-15.
- [6] **Sághi B.**: Jelfogós sorompó illesztő kapcsolás modellezése Petri-hálóval. BME Ipari nyílt nap 2000. Poszter-előadás.
- [7] Tarnai G., **Sághi B.**: Követelményrendszerek formalizálása a vasútbiztosításban. *III. Országos Vasúti Távközlési és Biztosítóberendezési Konferencia* Miskolc-Lillafüred, 2000. október 9-11. pp. 86-98.
- [8] Tarnai G., **Sághi B.**: Chapter *Safety-critical Systems*. p. 53. In: Pataricza A. (szerk.): *Formal Methods of Informatics – KHVM 96/2000 projekt beszámoló*.
- [9] Tarnai G., **Sághi B.**: Zusätzliche Aspekte zur Anwendung von formalen Techniken in der Eisenbahnsicherungstechnik. *Signal+Draht* (Németország) **(93)** 7-8/2001. pp. 42-45.
- [10] Tarnai G., **Sághi B.**: Application Aspects of Formal Methods in Railway Signalling. *The Transport of the 21st Century – International Scientific Conference*. Varsó, Lengyelország, 2001. szeptember 19-21. pp. 199-205.
- [11] Tarnai G., **Sághi B.**: Software Specification and Development in the Domain of Railway Signalling. *Workshop on Software specification of safety relevant transportation control tasks*. 3rd Workshop in the course of the DFG-Priority Program Integration of Software Specification Techniques for Application in Engineering. Braunschweig, 2002. április 23-24.
- [12] **Sághi B.**: Irányelvek a formális módszereknek a vasútbiztosítás területén történő alkalmazásához. *Közlekedéstudományi szemle*. LII. évf. 8. szám, 2002. pp. 291-299.

VI. A TÉZISFÜZETBEN HIVATKOZOTT IRODALMAK JEGYZÉKE

- [Anf99] Formale Techniken für die Eisenbahnsicherungstechnik. Anforderungskatalog – Zusammenfassung der Arbeitsunterlagen. *Signal+Draht* (91) 10/1999, pp. 38-42.
- [Bow92] Bowen, J.P., V. Stavridou: Formal Methods and Software Safety. *SAFECOMP 1992: Safety of Computer Control Systems*, 1992.
- [Bow93a] Bowen, J., V. Stavridou: Safety-Critical Systems, Formal Methods and Standards. *Software Engineering Journal*, 1993.
- [Bow93b] Bowen, J., V. Stavridou: The Industrial Take-up of Formal Methods in Safety-Critical and Other Areas: A Perspective. *FME'93: Industrial-strength formal methods, 1st International Symposium of Formal Methods Europe*, April 1993 (Springer-Verlag, *Lecture Notes in Computer Science* 670, 1993).
- [Bow94a] Bowen, J. Formal Methods in Safety-Critical Standards. (?) 1994.
- [Bow94b] Bowen, J., M.G. Hinchey: Seven More Myths of Formal Methods: Dispelling Industrial Prejudices. *FME'94: Industrial Benefit of Formal Methods*, Springer-Verlag, October 1994.
- [Bow95] Bowen, J., M.G. Hinchey: Ten Commandments of Formal Methods. *IEEE Computer*, 28 (4) April 1995. pp. 56-63.
- [Cra93] Craigen, D., S. Gerhart, T. Ralston: An International Survey of Industrial Application of Formal Methods (Volume 1: Purpose, Approach, Analysis and Conclusion, Volume 2: Case Studies). *Atomic Energy Control Board of Canada, U.S. National Institute of Standards and Technology, and U.S. Naval Research Laboratories*, NIST GCR 93/626, 1993.
- [Ehr99] Ehrig, H., F. Orejas, J. Padberg: Relevance, Integration and Classification of Specification Formalisms and Formal Specification Techniques. In: [FORMS99]
- [FMERail98/1] 1st Workshops on Formal Methods in Railway Industry, June 8-9 1998, Nieuwegein, The Netherlands <http://www.ifad.dk/Projects/fmerail.htm>
- [FMERail98/2] 2nd Workshops on Formal Methods in Railway Industry. October 15-16 1998, London, U.K. <http://www.ifad.dk/Projects/fmerail.htm>
- [FMERail99/1] 3rd Workshops on Formal Methods in Railway Industry. February 24-26 1999, St. Pölten, Austria. <http://www.ifad.dk/Projects/fmerail.htm>
- [FMERail99/2] 4th Workshops on Formal Methods in Railway Industry. May 11-12 1999, Stockholm, Sweden. <http://www.ifad.dk/Projects/fmerail.htm>

- [FMERail99/3] 5th Workshops on Formal Methods in Railway Industry. September 22-24, 1999 Toulouse, France. <http://www.ifad.dk/Projects/fmerail.htm>
- [FORMS00] FORMS 2000 - Formale Techniken für die Eisenbahnsicherung. *Fortschr.-Ber. VDI Reihe 12 Nr. 441 Düsseldorf: CDI Verlag 2000* p.220
- [FORMS98] *International Workshop on the Formal Specification of Train Control Systems in Europe.* May 12-13 1998, Braunschweig <http://www.ifra.ing.tu-bs.de/forms/>
- [FORMS99] *Formale Techniken für die Eisenbahnsicherung. Workshop,* December 1-2 1999, Braunschweig. <http://www.ifra.ing.tu-bs.de/forms/>
- [Hal90] Hall, J.A.: Seven Myths of Formal Methods. *IEEE Software*, September 1990. 7 (5) pp.11-19.
- [Inc92] Ince, D. C.: An Introduction to Discrete Mathematics, Formal System Specification, and Z. *Oxford University Press, Oxford.* 1992.
- [Lar96] Larsen, P.G., J. Fitzgerald, T. Brookes: Applying Formal Specification in Industry. *IEEE Software*, May 1996. pp. 48-56.
- [NASA95] NASA Office of Safety and Mission Assurance: Formal Methods Specification and Verification Guidebook for Software and Computer Systems. Volume I: Planning and Technology Insertion. NASA-GB-002-95 Washington, 1995.
- [NASA97] NASA Office of Safety and Mission Assurance: Formal Methods Specification and Analysis Guidebook for the Verification of Software and Computer Systems. Volume II: A Practitioner's Companion. NASA-GB-001-97 Washington, 1997.
- [Pat01] Pataricza A., Csertán Gy., Majzik I., Bartha T.: Formális módszerek az informatikában. Jegyzet kézirat. 2001. március.
- [Tho95] Thomas, M.: IEE/BCS Workshop report 20/3/95. University of Glasgow, Dept. of Computing Science. 1995.
- [Win90] Wing, J.: A Specifier's Introduction to Formal Methods. *IEEE Computer* September 1990. pp. 8-24.