PhD Értekezés

Formális módszerek alkalmazása a vasútbiztosító technikában

Sághi Balázs

Budapest
2003

Budapesti Műszaki és Gazdaságtudományi Egyetem
Közlekedés Tudományszak

PhD Értekezés

Formális módszerek alkalmazása a vasútbiztosító technikában

Sághi Balázs
okl. közlekedésmérnök

Témavezető:
Dr. habil. Tarnai Géza
egyetemi tanár

Budapest
2003. január

Tartalomjegyzék

Bevezetés

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 nőtt a formális módszerek iránti igény.

Az elmúlt években a rendszereket fejlesztő szervezetek egy része felismerte, hogy a bonyolult rendszerek fejlesztésének és karbantartásának kézbentarthatóságához 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 Berlini 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. Ezeken 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 előbbiekben 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 oka abban kereshető, hogy az eddigi kutatások nem veszik figyelembe a vasúti biztosítóberendezési rendszerek bizonyos jellegzetességeit, illetve a biztosítóberendezések fejlesztésének egyes sajátosságait.

A *jelen disszertáció célja* ennek megfelelően az, hogy

- tisztázza és egyértelműen leírja a vasúti biztosítóberendezések szakterületének azokat a jellegzetességeit, amelyek a formális módszerek alkalmazására hatással vannak, továbbá hogy
- olyan irányelveket határozzon 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 előbbiek miatt vált szükségessé az irodalomból ismert szempontoknak újabbakkal 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.

A formális módszerek vasúti biztosítóberendezési alkalmazásával foglalkozó szakirodalmat megvizsgálva az tapasztalható, 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 kell vizsgálni a vasúti biztosítóberendezések életciklusát. E vizsgálatok eredményeként az ismert életciklus-modellek továbbfejlesztésével olyan modell kidolgozásra kerül sor, amely a

biztosítóberendezések fejlesztési folyamatát adekvát módon képezi le, így alapul szolgálhat a formális módszerek alkalmazhatóságának további vizsgálataihoz (1. fejezet).

Ezt követően kerül sor azoknak a tényezőknek a meghatározására, 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 (2.1. fejezet).

Megvizsgálva a formális módszerek alapvető jellemzőit, és az előbbi igényt figyelembe véve, meghatározhatók azok az *előnyök*, amelyek a formális módszereknek a vázolt területeken történő alkalmazásával elérhetők (2.2. fejezet).

Ezt követően vizsgálhatók meg azok a szempontokat, amelyek az alkalmazhatóságra, illetve az alkalmazás hatékonyságára, sikerére nézve hatással lehetnek. A szakirodalomban található szempontok újabbakkal való kiegészítése, illetve egységes rendszerbe foglalása révén egy egységes *Alkalmazási szempontrendszer* került kialakításra (3. fejezet).

A formális módszerek vasútbiztosítási alkalmazásának szakirodalmában alapvető szerepet tölt be az ún. *Követelménykatalógus* [Anf99], ezért szükséges e dokumentum kritikai elemzésének végrehajtása. A vizsgálatok 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 kellett ellátni, amelyek révén eredeti célkitűzésének elérésére alkalmasabbá vált (4. fejezet).

A formális módszerek vasútbiztosítási alkalmazásának vizsgálatához elengedhetetlen az *ismert gyakorlati alkalmazások* áttekintése. Ezek értékelésére a disszertáció 3. fejezetében kidolgozott, egységes Alkalmazási szempontrendszer, illetve a 4. fejezetben kiegészített Követelménykatalógus szerint kerül sor (5. fejezet).

A 6. fejezetben megvizsgáljuk a *Petri-hálóknak* mint elterjedt modellezési eszköznek a jelfogós vasúti biztosítóberendezési rendszerek működésének leírására való alkalmasságát. Ennek kapcsán értékeljük a Petri-hálón alapuló hagyományos logikai modellezési eljárást, és *új modellezési technika* alkalmazására teszünk javaslatot.

Az általános érvényű alkalmazási szempontrendszeren alapulva, a vasúti sajátosságokat, illetve az ismert gyakorlati alkalmazások tanulságait figyelembe véve határozhatók meg a formális módszerek *vasútbiztosítási alkalmazásának irányelvei* (7.1.-7.4. fejezetek).

Végezetül, a disszertáció 7.5. fejezetében egy bevezetési modellt mutatunk be a formális módszerek vasúti biztosítóberendezési területen történő bevezetésére.

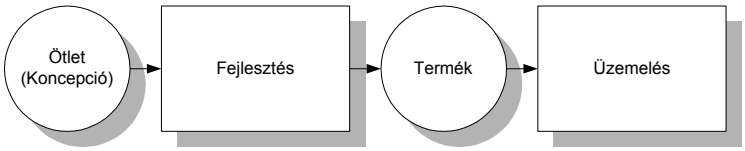
A disszertációt irodalomjegyzék és függelékek egészítik ki.

1. A rendszerfejlesztés és a formális módszerek alapfogalmai

1.1. A rendszerfejlesztés modellezése

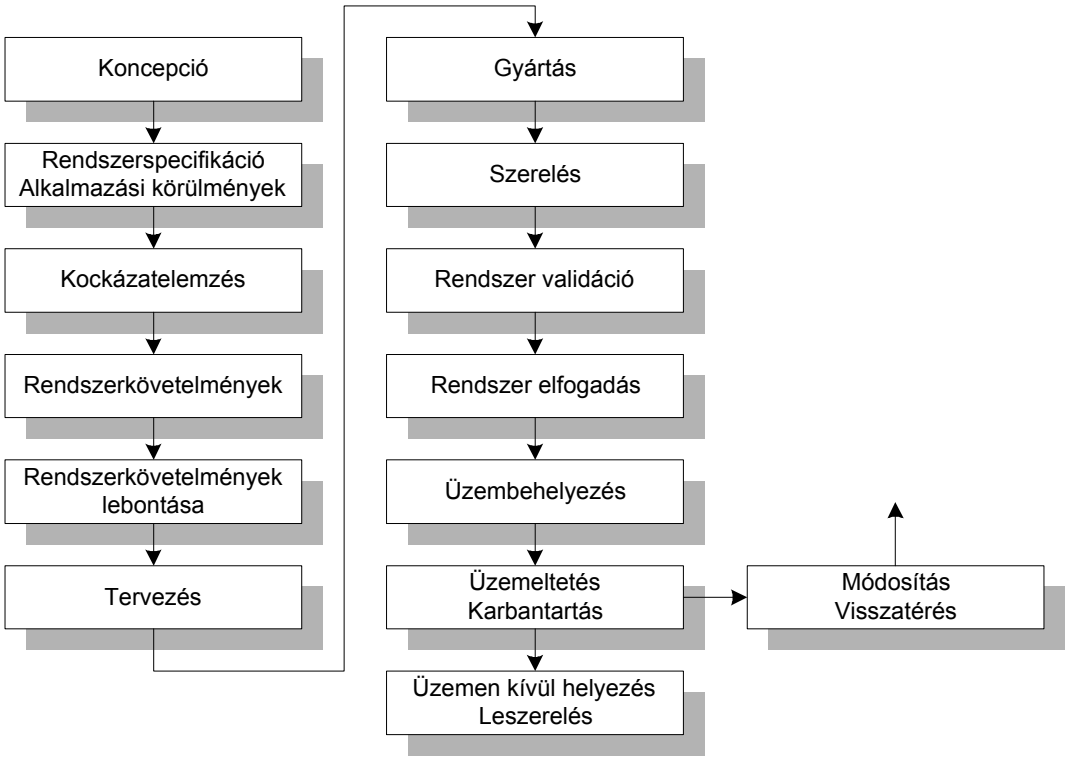
1.1.1. A rendszerek életciklusa

A múltban a folyamatirányító rendszerek fejlesztése igen egyszerű folyamat volt, amely a termék megrendelőjére és annak elkészítőjére korlátozódott (1. ábra). A termék tervezése és előállítása egyszerű, többé-kevésbé manuális eljárás volt.



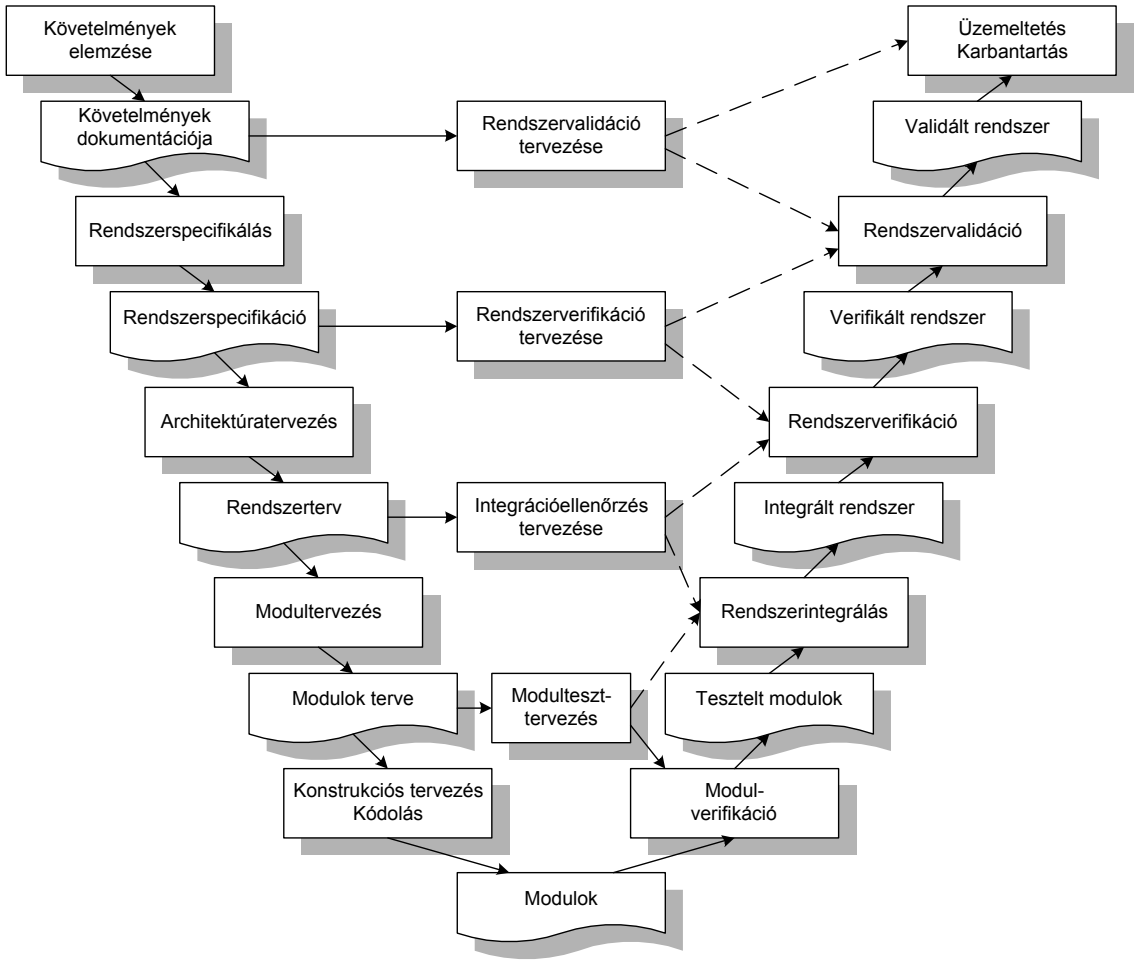
1. ábra. Egyszerű életciklus modell [Sni99]

Manapság ez a folyamat az időtartamát tekintve is sokkal hosszabb, és az érintett résztvevők körét tekintve is tágabb. A rendszerek fejlesztésének bonyolultsága miatt szükségessé vált a rendszerek teljes életciklusát átfogó fejlesztési módszertanok kidolgozása. Ennek kapcsán kialakították a megfelelő rendszer-életciklus modelleket. A rendszerek életciklusának ábrázolására a két legelterjedtebb modell az ún. fázismodell (2. ábra), illetve az ún. V-modell (3. ábra).



2. ábra. A rendszerek életciklusának fázismodellje [EN50126]

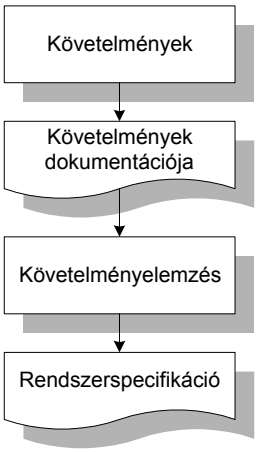
A rendszerek életciklusában két tevékenységnek, a *verifikációnak* és a *validációnak* kiemelt jelentősége van. A verifikáció során két egymást követő fejlesztési fázis konzisztenciáját vizsgáljuk, azaz, hogy az adott fejlesztési fázis eredménye megfelel-e az előző fázisnak. A validáció olyan vizsgálat, amelynek célja annak megállapítása, hogy egy adott fejlesztési fázis eredménye megfelel-e a rendszerrel szemben támasztott eredeti követelményeknek. Úgy is fogalmazhatunk, hogy a verifikáció során azt vizsgáljuk, hogy „jól építjük-e a rendszert", a validáció során pedig azt, hogy „a jó rendszert építjük-e".



3. ábra. A rendszerek életciklusának V-modellje [Pat01]

1.1.2. A biztonsági folyamat

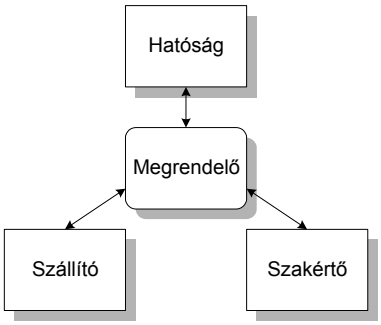
A szakirodalomban található fejlesztési modellek a megépítendő rendszer specifikálását egyszerű, néhány lépésből álló folyamatként ábrázolják (4. ábra). Az általános célú rendszerek, szoftverek esetében gyakran fordul elő, hogy a követelmények nem fogalmazódnak meg dokumentált formában, a követelményelemzés pedig a megrendelő szóbeli kikérdezésén alapul. Biztonsági felelősségű rendszerek esetében a megrendelő a követelményeket a legtöbbször dokumentálja. Vasúti biztosítóberendezések esetében a megrendelői (vasúti) követelményeket az ún. feltétfüzet tartalmazza.



4. ábra. A rendszerek specifikációjának egyszerűsített folyamata

A biztonságkritikus rendszerek, például egy vasúti biztosítóberendezés létesítésének, vagy egy meglévő berendezés módosításának biztonsági vonatkozásai egy ún. biztonsági folyamattal írhatók le. A biztonsági folyamat előre meghatározott tevékenységek sorozata, amely felöleli egy rendszer teljes életciklusát**.** Ennek a biztonsági folyamatnak alapvetően négy szereplője van (5. ábra):

- a rendszert üzemeltető vasút (megrendelő),
- a gyártó ipar (fejlesztő, tervező, szállító),
- a biztonsági értékelést végző, szükség esetén független szakértő és
- a rendszer üzemeltetését engedélyező biztonsági felügyeleti hatóság.



5. ábra. A biztonsági folyamat résztvevői

A biztonsági folyamat többszereplős volta miatt a biztonságkritikus rendszerek, azon belül a vasúti biztosítóberendezések specifikálásának folyamata, az általánostól eltérően, *iteratív* jellegű. Ezt a jellegzetességet a szakirodalomban tárgyalt specifikációs modellek nem kezelik. Az iteratív folyamat megfelelő szervezéséhez és modellezéséhez meg kell különböztetni és a specifikációs folyamatban el kell helyezni a vasúti biztosítóberendezések *különböző szintű specifikációit*:

- a vasúti feltétfüzetet,
- a rendszerspecifikációt és
- a gyári feltétfüzetet.

A vasút üzemi, illetve üzemeltetési koncepciója, valamint a végrehajtott kockázatelemzés eredményei alapján *vasúti feltétfüzetben* fogalmazza meg a biztosítóberendezési rendszerekkel szemben támasztott követelményeit. A feltétfüzetben többnyire funkcionális követelmények

fogalmazódnak meg, és a dokumentum nem tér ki a műszaki megoldás miként tjére [Anf99]. Mivel biztonsági felelősségű rendszerről van szó, a feltétfüzetben megfogalmazott követelményrendszert a felügyeleti hatósággal egyeztetni kell.

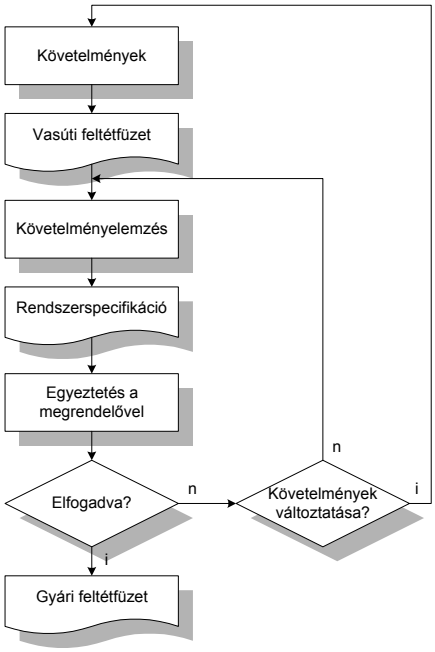
A fejlesztő a feltétfüzetből a követelmények elemzése révén előállítja a *rendszerspecifikációt*. E folyamat során a megrendelővel való, részletes kikérdezésen alapuló, és előkészített válaszokat is tartalmazó konzultációs kapcsolat többnyire elengedhetetlen. A rendszerspecifikáció a kifejlesztendő rendszert úgy írja le, ahogy a fejlesztő a megrendelő által megfogalmazott követelményeket értelmezi. Az előállított specifikációt a megrendelőnek felülvizsgálat és elfogadás céljából át kell adni.

Amennyiben a megrendelő a specifikációt elfogadja, a fejlesztő e specifikáció alapján létrehozza a belső használatra szánt *gyári feltétfüzetet*. A gyári feltétfüzet azt mutatja be, hogy a megrendelői (vasúti) feltétfüzet követelményeit milyen megoldások révén valósítják meg. A gyári feltétfüzet egyrészt részletezi a megrendelői (vasúti) feltétfüzet követelményeit, másrészt leírja azok cégspecifikus megoldási módját [Anf99].

Ha a megrendelő nem fogadja el az elkészített specifikációt, akkor a specifikációs folyamat egy részét ismét végre kell hajtani. Ha a specifikáló helytelenül értelmezte az eredeti követelményeket, akkor a követelményelemzés újbóli végrehajtására van szükség. Előfordulhat azonban az is, hogy az eredeti, megrendelői követelményeket kell megváltoztatni. Ennek oka lehet az eredeti követelményrendszerben rejlő ellentmondás vagy hiányosság, illetve az, hogy az adott követelmények az adott műszaki peremfeltételeket figyelembe véve nem valósíthatóak meg.

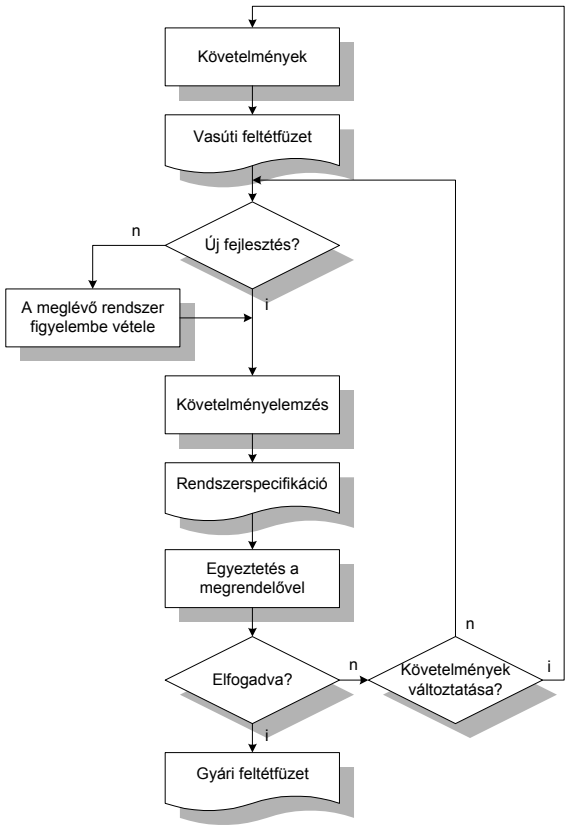
A gyári feltétfüzet alapján elkészült berendezést és annak dokumentációját, beleértve a biztonságigazolást, az üzembehelyezés előtt egy szakértőnek kell megvizsgálnia. A megfelelő szakértői jelentés az egyik előfeltétele annak, hogy a hatóság a berendezés használatbavételi engedélyét az üzemeltető számára kiadja.

A folyamat fentiek szerinti iteratív jellegét is magába foglaló *kibővített specifikációs modellt* ábrázolja a 6. ábra.



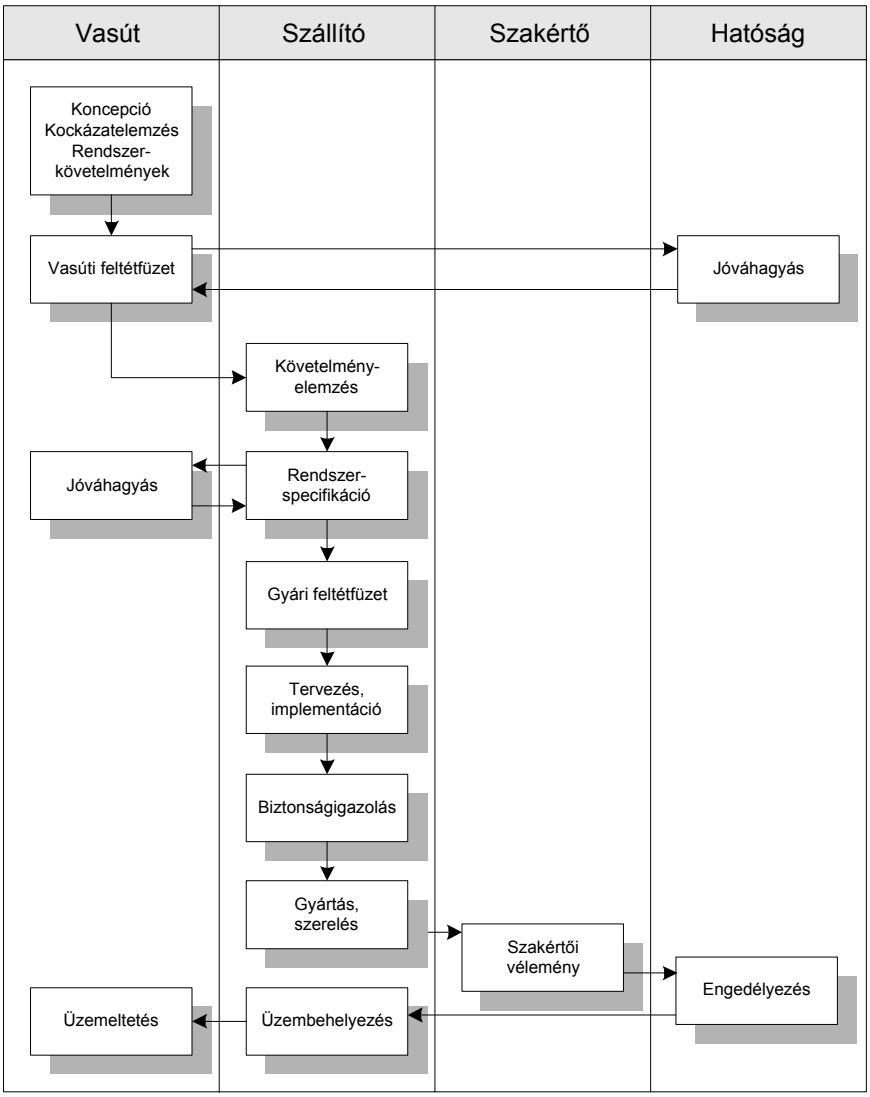
6. ábra. A specifikációs folyamat iteratív jellege [Ság98, Ság99b]

Egy már meglévő, biztonságigazolt, a hatóság által engedélyezett rendszer, illetve alrendszer azonos alkalmazási körülmények között való használatához nincs szükség a biztonságigazolás ismételt elvégzésére, és a szükséges engedélyezési eljárás is sokkal egyszerűbb. Az ebből adódó, a biztonságigazolással kapcsolatos megtakarítási lehetőségek kihasználása érdekében, továbbá a fejlesztés közvetlen ráfordításainak mérséklése céljából, a vasúti biztosítóberendezések területén egy *speciális fejlesztési gyakorlat* alakult ki. Ennek lényege, hogy valamely vasúti feltétfüzet követelményeinek kielégítésére a gyárak gyakran nem teljesen új rendszereket fejlesztenek, hanem a követelményeket meglévő rendszereik továbbfejlesztésével vagy adaptálásával igyekeznek kielégíteni. E fejlesztési gyakorlat a valóságban azt jelenti, hogy a követelményelemzés fázisának nemcsak a megrendelői követelmények, azaz a vasúti feltétfüzet a bemenő adata, hanem a már *meglévő*, továbbfejlesztendő vagy adaptálandó *rendszer* jellemzőit, illetve adottságait is figyelembe kell venni a rendszerspecifikáció kidolgozása során. Ehhez adott esetben szükség lehet a már meglévő, alapul vett rendszer feltétfüzetének és az aktuális feltétfüzetnek az összehasonlítására és egy ún. *különbségi feltétfüzetnek* a létrehozására. A vasúti biztosítóberendezési rendszerek specifikációs folyamatának modelljét, a fenti jellegzetesség figyelembevételével kibővítve, a 7. ábra szemlélteti.



7. ábra. A vasúti feltétfüzettől a gyári feltétfüzetig [Ság00a]

A vasúti biztosítóberendezések létesítésével kapcsolatos *biztonsági folyamatot*, és a kapcsolódó tevékenységek szereplők szerinti bontását a 8. ábra foglalja össze.



8. ábra. Vasúti biztosítóberendezések létesítésének biztonsági folyamata

1.1.3. Új tudományos eredmények

A fejezet alapján született új tudományos eredményeket az 1. tézisben foglaljuk össze.

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.*

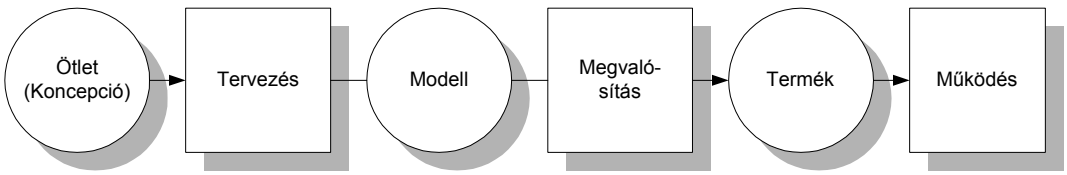
Az 1. tézis a [Ság98, Ság99b, Ság00a, Ság00c, Ság00e] publikációkon alapul. A tézisben szereplő fejlesztési modell elsősorban a gyakorlati alkalmazást célzó további kutatások számára lehet iránymutató.

1.2. A formális módszerek alapfogalmai

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 például 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, 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.

1.2.1. A „BMW”-elv

A korszerű rendszerek fejlesztéséhez szükséges precizitás eléréséhez nagy mennyiségű dokumentációra van szükség, amelyek összessége a rendszer egyfajta modelljét alkotja. Így az ötletből először konstrukciós vázlat, terv, kapcsolási rajz, programkód stb. lesz, majd ezek alapján készül el a megvalósított rendszer (9. ábra).

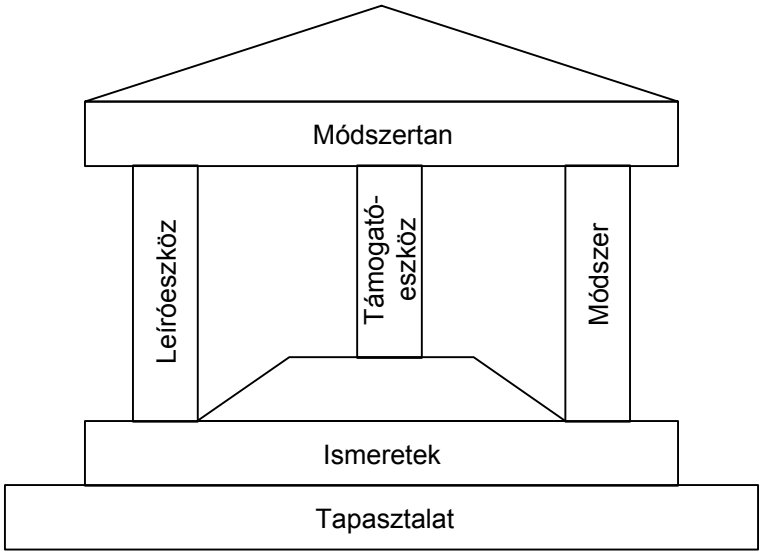


9. ábra. A modellek szerepe a rendszerfejlesztésben

Ahogy a rendszerek által ellátott feladatok és a megvalósítási lehetőségek is bővülnek, úgy lesznek egyre sokfélébbek a tervezés és a megvalósítás közti rendszermodellek is. A ma zajló fejlesztési folyamatok és feladatok komplexitása miatt a modellezhetőség és a modellezés módja tudományos–módszertani kérdés.

A rendszerfejlesztés területén az ún. *BMW-elvnek* megfelelően egy hármas tagolás alakult ki: *Leíróeszköz – Módszer – Támogatóeszköz*. A BMW elnevezés a három alapfogalom német nevének (*B*eschreibungsmittel – *M*ethode – *W*erkzeug) kezdőbetűiből adódik [Sni99].

A BMW-elv központi gondolata az, hogy bármilyen módszertan a fenti három komponens megfelelő kombinációjaként értelmezhető (10. ábra). A BMW-elv alkalmazásával a rendszerek tervezéséhez megfelelően lehet kiválasztani a legalkalmasabb módszert, a leíró és a támogatóeszközöket.



10. ábra. A BMW-elv [Mey00]

A *leíróeszköz* a viselkedés leírására, formalizálására szolgáló eszköz. Független magától a problémától, annak megfogalmazásától és megoldásától. Ez azonban egyáltalán nem zárja ki, hogy bizonyos problémák megfogalmazása számára egyes leíróeszközök alkalmasabbak legyenek, mint mások. Egy leíróeszköz adott kifejezésmódok, mint például a nyelv, jelölésmód vagy a formalizmus révén definiálható konkrétabban.

A megfelelő leíróeszköz alapvető fontosságú a tervszerű eljárás leírásához; a feladat és a megoldás leírásához, végül pedig a berendezés állapotainak leírásához és a kezelés leírásához.

Formalizmusnak, a továbbiakban *formális leíróeszköznek***,** a matematikailag definiált szintaktikával *és* szemantikával rendelkező leíróeszközt nevezzük. A szintakszis a leíróeszköznek azokat a strukturális tulajdonságait foglalja magába, amelyek a jelölésmód interpretációjára való hivatkozás nélkül tárgyalhatók. A formális szemantika adja meg a jelölésmód egyes elemeinek interpretációját, az alkalmazástól függetlenül. Az alkalmazási vonatkozások a kibővített, általános szemantikai fogalom, a pragmatika témakörébe tartoznak.

Módszer alatt egy szabályrendszerre épülő, tárgya és célja szerint tervszerű, ismeretek vagy gyakorlati eredmények megszerzésére irányuló eljárást értünk. A BMW-elv értelmében a módszer az az értelmezés, amely a kiválasztott leíróeszközt az adott problémához társítja.

A *támogatóeszköz* általában számítógépes szoftver, amely támogatja valamely leíróeszköz számítógépes alkalmazását, és ennek révén biztosítja a modell formális tulajdonságainak legalább részben automatikus értékelését/vizsgálatát. Támogatóeszközök nélkül leíróeszközök és módszerek alkalmazása csak korlátozottan lehetséges az életciklus során végrehajtandó tevékenységekben.

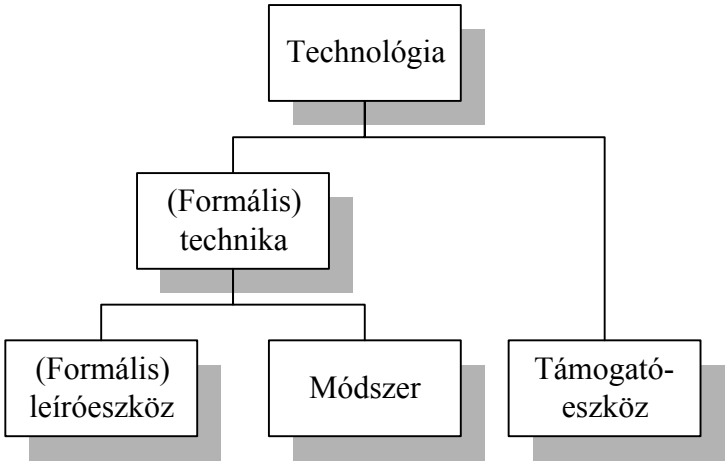
A leíróeszköz és a módszer egy alkalmas kombinációját *technikának*, formális leíróeszköz esetében *formális technikának* nevezzük:

[Formális] Technika = [Formális] Leíróeszköz + Módszer.

A BMW-elv terminológiája szerinti *formális technika* helyett mi a továbbiakban az elterjedtebb *formális módszer* kifejezést fogjuk használni. A rendszerspecifikáció vonatkozásában a (formális) specifikációs technika és a (formális) technika fogalmakat szinonimaként használjuk.

Amennyiben egy bizonyos specifikációs technika alkalmazása egy konkrét támogatóeszköz (tool) használatával jár együtt, *technológiáról* (specifikációs technológiáról) beszélünk (11. ábra). A technológia tehát magában foglalja a leíróeszközt, a módszert és a támogatóeszközt:

Technológia = (Leíróeszköz + Módszer) + Támogatóeszköz



11. ábra. A BMW-elv terminológiája

A rendszerfejlesztés fenti három alapösszetevője a fejlesztés valamennyi fázisában fellelhető. Az 1. táblázat a tervezés, a megvalósítás és a rendszerüzemeltetés fázisaiban fellelhető leíróeszközöket, módszereket és támogatóeszközöket mutatja be..

1. táblázat. A BMW-elv a rendszerek életciklusában [Sni99]

Életciklus fázis	Tervezés	Megvalósítás	Üzemelés
Kiindulás	Ötlet	Modell	Megbízás
Leíróeszköz	Szöveg, képek, szimbólumok, rajzok		
Módszer	Követelmény-elemzés (requirements-engineering), strukturált analízis	Kiviteli tervek, utasítások, folyamatábrák	Üzemeltetési módszerek, eljárások, szervezés
Támogatóeszköz	„Tool”	Compiler, számítógépek, megmunkáló gépek	Berendezések, készülékek, komponensek
A fázis eredménye	Modell	Berendezés, termék, készülék	Szolgáltatás, áruk, termékek

1.2.2. A formális specifikációs nyelv

A formális specifikációs nyelv biztosítja a *matematikai alapot* a formális módszerek számára. Egy formális specifikációs nyelvet a következőképpen definiálhatunk [Win90]:

Definíció: A $\langle Syn, Sem, Sat \rangle$ hármast formális specifikációs nyelvnek nevezzük, ha fennáll a következő reláció: $Sat \subseteq Syn \times Sem$, ahol Syn és Sem halmazok. Syn-t a nyelv szintaktikai tartományának, Sem-t a nyelv szemantikai tartományának, Sat-ot pedig az ún. kielégítési relációnak nevezzük.

Definíció: Adott a $\langle Syn, Sem, Sat \rangle$ formális specifikációs nyelv. Ha a $Sat(syn, sem)$ kapcsolat fennáll, akkor azt mondjuk, hogy *syn* egy *specifikációja sem*-nek, és *sem* pedig *specifikandusa syn*-nek.

Definíció: Adott a $\langle Syn, Sem, Sat \rangle$ formális specifikációs nyelv. Ekkor azt mondjuk, hogy egy *Syn*-beli *syn* specifikáció *specifikandus halmaza* az összes *sem* specifikandus halmaza *Sem*-ben, melyre fennáll a $Sat(syn, sem)$ kapcsolat.

Kevésbé formálisan: a formális specifikációs nyelv a következő elemekből tevődik össze: egy notáció vagy jelölésrendszer *(szintaktikai tartomány)*, objektumok összessége *(szemantikai tartomány)* és egy precíz szabályrendszer, amelyik definiálja, hogy mely objektumok elégítik ki az egyes specifikációkat *(kielégítési reláció)*. A specifikáció egy *mondat,* amelyet a szintaktikai tartomány elemei alkotnak. A specifikandus egy objektum, amely kielégíti a specifikációt. A kielégítési reláció adja meg a szintaktikai elemek értelmét.

Szintaktikai tartomány. A specifikációs nyelv szintaktikai tartományát rendszerint szimbólumok (például konstansok, változók, logikai kapcsolatok) halmazaként definiáljuk, kiegészítve grammatikai szabályok egy halmazával, amely definiálja, hogy milyen módon lehet a szimbólumokat egymással kombinálni.

A szintaktikai tartomány nem feltétlenül korlátozódik alfanumerikus jelekre; grafikus elemek, mint négyzet, kör, vonalak, nyilak és más grafikus szimbólumok segítségével pontosan ugyanolyan precízek szintaktikai tartomány definiálható, mint az alfanumerikus írásmód segítségével.

Fontos, hogy a szintakszis olyan legyen, hogy egyszerűvé tegye az algoritmus, illetve a követelmények kifejezését [Ost92].

Szemantikai tartomány. A különböző specifikációs nyelvek leginkább a szemantikai tartomány megválasztásában térnek el egymástól. *Absztrakt adattípus specifikációs nyelveket* használnak például algebrák és logikai programok specifikációjára; *konkurens és elosztott rendszerek specifikációs nyelvét* alkalmazzák például állapotszekvenciák, eseményszekvenciák, állapotátmeneti rendszerek, illetve állapotgépek leírására; és *programozási nyelveket* használnak input és output közti funkciók, számítások, relációk és gépi utasítások leírására.

Minden programnyelv, amelynek jól definiált, formális szemantikája van, specifikációs nyelv, de ennek fordítottja már nem igaz, mivel a specifikációknak általában nem kell valamilyen gépen végrehajthatóknak lenniük, mint a programoknak. Egy absztraktabb specifikációs nyelv segítségével olyan funkciók, tulajdonságok is kifejezhetők (például végtelen halmazok kezelése), amelyek gépileg nem számíthatóak, nem végrehajthatóak.

A programok formális objektumok, ezért alkalmasak formális műveletek elvégzésére (fordítás, végrehajtás). A programozók számára ezért a formális módszerek egyáltalán nem lehetnek idegenek. A különbség annyiban áll, hogy míg formális módszerek nélkül a

programozó informális követelményekkel és formális programmal dolgozik, addig formális módszer alkalmazása esetén formalizmusokat alkalmaz a követelmények specifikálására is.

Ha a specifikációs nyelv szemantikai tartománya egy program, vagy programrendszer, akkor a kielégítési relációra az *implementál* terminust használják, az implementáció kifejezés pedig egy *Sem*-beli specifikandust jelöl. Egy *prog* implementáció akkor helyes egy adott *spec* specifikációt tekintve, ha *prog* kielégíti *spec*-t. Formálisan:

Definíció: Adott a $\langle Syn, Sem, Sat \rangle$ formális specifikációs nyelv. Egy *Sem*-beli *prog* implementáció akkor és csak akkor helyes egy adott *Syn*-beli *spec* specifikációt tekintve, ha fennáll a $Sat(spec, prog)$ kapcsolat.

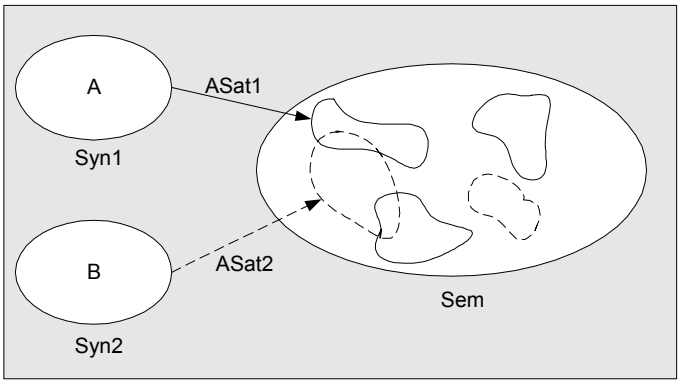
Kielégítési reláció. Gyakran van szükség arra, hogy egy specifikandust több különböző aspektusból specifikáljunk, ehhez esetleg különböző specifikációs nyelveket alkalmazva.

Például egy programmodul-gyűjtemény funkcionális viselkedését az egyes modulok funkcionális viselkedésének kompozíciójaként specifikáljuk, továbbá specifikálni akarjuk a modulok egymással való strukturális kapcsolatát is.

A specifikandus különböző nézeteinek összehangolásához először egy *szemantikai absztrakciós függvényt* rendelünk minden egyes specifikációs nyelvhez, amely a specifikandusokat ekvivalencia-osztályokra osztja. Ez a szemantikai absztrakciós függvény a specifikációk és a specifikandusok ekvivalencia-osztályai között egy *absztrakt kielégítési relációt* hoz létre. Az így létrejött reláció a specifikandus egy *nézetét* definiálja.

Különböző szemantikai absztrakciós függvényekkel lehetővé válik egy rendszer ugyanazon ekvivalencia-osztálya különböző nézeteinek, illetve a rendszerrel szemben támasztott különböző jellegű követelményeknek a leírása.

Példaként a 12. ábrán egyetlen szemantikai tartomány (*Sem*) látható. A *Sem*-beli specifikandust egy szemantikai absztrakciós függvény ekvivalencia-osztályokra bontja. Ezek közül az ábrán hármat ábrázoltunk, folytonos vonallal. Egy másik függvény más ekvivalencia-osztályokra osztja a specifikandust, amelyeket szaggatott vonallal ábrázoltunk. Az *ASat1* absztrakt kielégítési reláció a specifikandus egyik ekvivalencia-osztályát (folytonos vonallal jelölve), a *Syn1* szintaktikai tartománybeli *A* specifikációhoz rendeli hozzá, hasonlóképpen *ASat2* egy másik ekvivalencia-osztályt a *Syn2*-beli *B* specifikációhoz rendeli hozzá.



12. ábra. Példa a különböző szemantikai absztrakciókra [Win90]

A szemantikai absztrakciós függvényeknek két nagy osztálya van: az egyik csoport a rendszer viselkedését absztrahálja, a másik csoport a rendszer struktúráját.

*Viselkedési specifikáció***.** A viselkedési specifikáció a rendszer viselkedésével szemben támasztott követelményeket írja le. A legtöbb formális módszer a viselkedésbeli elvárások specifikációját, a rendszertől elvárt funkcionalitás leírását célozza meg (azaz hogyan, milyen outputokkal reagáljon a rendszer az inputokra).

A viselkedési specifikáció tárgykörébe tartoznak az olyan viselkedési aspektusok is, mint a hibatűrés, biztonság, védettség, válaszidő követelmények. Ezek az aspektusok gyakran teljesen elkülönülnek a funkcionális viselkedéstől. A teljes rendszer helyességének vizsgálatakor azonban ezeket ugyanúgy figyelembe kell venni, mint a funkcionális követelményeket, hiszen egy rendszer hiába ad helyes kimenetet a szükséges válaszidő lejárta után, az a rendszer ugyanúgy nem helyes, mintha helytelen kimenetet adott volna időben.

*Strukturális specifikáció***.** A strukturális specifikáció a specifikandus belső kompozíciójával szembeni követelményeket írja le. A strukturális specifikációs nyelvekre példák a modulkapcsolati nyelvek. A strukturális specifikációkra jellemzők a hierarchikus relációk, amelyeket például hívási gráfokkal, adatfüggőségi diagrammokkal lehet ábrázolni. Ha két rendszer azonos strukturális követelményeknek felel meg, ez nem jelenti azt, hogy a funkcionalitásuk is azonos. [Win90] kiemeli, hogy a specifikáció struktúrájának nem szükséges bármilyen közvetlen kapcsolatban lennie a specifikandus struktúrájával.

1.2.3. A specifikációs nyelvek tulajdonságai

Matematikai szempontból a formális specifikációs nyelveknek két fontos tulajdonsága van: az egyértelműség és a konzisztencia.

Minden formális specifikációnak *egyértelműnek* kell lennie.

Definíció: Adott egy formális specifikációs nyelv, $\langle Syn, Sem, Sat \rangle$. Egy *Syn*-beli *syn* specifikáció akkor és csak akkor egyértelmű, ha a *Sat* reláció *syn*-t pontosan egy specifikandus halmazra képezi le.

Informálisan: egy specifikáció akkor és csak akkor egyértelmű, ha annak pontosan egy jelentése van. Ennek a kulcsfontosságú specifikációs tulajdonságnak a definíciója szerint bármely specifikációs nyelv, amely valamely természetes nyelven alapul, vagy azzal kapcsolatos, nem alkalmas arra, hogy formális specifikációs nyelv alapját képezze, mivel a természetes nyelv önmagában foglalja a többértelműség lehetőségét.

A formális specifikációs nyelv egyértelműsége teremti meg a lehetőséget arra, hogy segítségével egyértelmű, félreérthetőségektől mentes követelményrendszerek legyenek definiálhatók.

A specifikációs nyelvek másik kívánatos tulajdonsága a *konzisztencia*.

Definíció: Adott egy formális specifikációs nyelv, $\langle Syn, Sem, Sat \rangle$. Egy *Syn*-beli *syn* specifikáció akkor és csak akkor konzisztens, ha a *Sat* reláció *syn*-t egy nem-üres specifikandus halmazra képezi le.

Informálisan: egy specifikáció akkor és csak akkor konzisztens, ha annak specifikandus halmaza nem üres.

A formális specifikációs nyelv konzisztenciája az alapja annak, hogy a formális specifikációs nyelv segítségével ellentmondásmentes követelményrendszerek legyenek készíthetőek (*lásd* 2.2.2. fejezet).

2. A formális módszerek alkalmazásának szükségessége és előnyei

2.1. A formális módszerek alkalmazása iránti igény

2.1.1. Szükség van-e a formális módszerekre?

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. Ezzel együtt sok lehetséges alkalmazási területen még ma is erőteljes tartózkodás tapasztalható, illetve *számos tévhit* tartja magát [Hal90, Bow94b]. Így például az az állítás, miszerint a formális módszereknek nincs meg a megfelelő támogatottsága. Sok formális módszert egészítettek ki számos korszerű metódussal, mint például az objektumorientáció. E folyamatos fejlesztések, kiegészítések iránti törekvések az előbbi állítás ellenkezőjét mutatják.

Ugyancsak cáfolja ezt a tévhitet, hogy számos *szabványosító szervezet* foglalkozik a formális módszerekkel: egyrészt előíró módon, másrészt bizonyos formális módszerek, notációk szabványosításával kapcsolatban. A LOTOS nyelvet például már 1989-ben szabványosították (ISO 8807).

Az Interneten szintén számos fórumot találhatunk, amelyek a formális módszerekkel, azok alkalmazásával foglalkoznak. A különböző szimpóziumok, konferenciák sokasága szintén a *formális módszerek aktualitása* mellett szól, az ott elhangzott előadások, és a kiadványok felbecsülhetetlen információs forrást jelentenek [Bow94b]. Ez igaz a folyóiratokra is; számos rangos folyóirat (IEEE Trans. on Software Eng, IEEE Computer, IEEE Software, ACM Software and Communication stb.) publikál rendszeresen formális módszerekkel kapcsolatos cikkeket. Végezetül pedig meg kell említeni, hogy formális módszereket (különösen Z, VDM, CSP és CCS) oktatnak a legtöbb nagy-britanniai felsőoktatási intézmény *számítástechnika-tudományi* kurzusán. [Bow94b]

Az előbbiek ellenére vannak olyan vélemények, hogy a formális módszerekre egyáltalán nincs szükség. Ez így egyszerűen hamis; természetesen vannak alkalmazások, ahol a formális módszerek bevetése valóban felesleges, de vannak helyzetek, amikor kifejezetten kívánatos. Valójában a formális módszerek alkalmazása minden olyan esetben ajánlott, ahol a *helyesség kérdésével* foglalkozni kell.

Ez nyilvánvalóan vonatkozik a biztonság- és a védettségkritikus rendszerekre, de igaz olyan rendszerekre is, amelyek nem tartoznak ezekbe a kategóriákba, de valami miatt nagyon szeretnénk, hogy a rendszer helyesen működjön. Ezenfelül léteznek alkalmazások, ahol a formális módszerek nem egyszerűen kívánatosak, hanem alkalmazásuk követelmény. A szabványosító grémiumok például nemcsak a szabványok egyértelműsége miatt alkalmazzák a formális specifikációs nyelveket, hanem előírják, vagy erősen ajánlják azok alkalmazását bizonyos típusú alkalmazások esetén.

A Nemzetközi Elektrotechnikai Bizottság (IEC) kifejezetten említ számos formális módszert (CCS, CSP, HOL, LOTOS, OBJ, VDM, Z) a biztonságkritikus rendszerek fejlesztésével kapcsolatban [IEC65A]. Az Európai Űrkutatási Ügynökség (*European Space Agency, ESA*) VDM vagy Z alkalmazását javasolja természetes nyelvvel kiegészítve, biztonságkritikus rendszerekkel szemben támasztott követelmények specifikációjához. Ezenfelül proponálja *formális bizonyítás* elvégzését a tesztelés előtt.

A példákat még tovább lehetne sorolni, de már ezekből is látható, hogy a formális módszerek alkalmazása követelmény bizonyos típusú alkalmazások esetén. Az ilyen alkalmazások köre pedig a jövőben nagy valószínűséggel még bővülni fog. [Bow94b]

Az előbbiek alapján megállapítható, hogy formális módszereket mindenhol érdemes használni, ahol a *rendszer* esetleges *hibájával járó költségek magasak*. Ilyenek

- a valamilyen szempontból kritikus rendszerek,
- a nagy számban előállított rendszerek,
- a beágyazott rendszerek,
- a kereskedelmi szempontból minőségfüggő rendszerek.

Majdnem valamennyi szoftver, vagy szoftverrész az előző okok legalább egyike miatt profitálhat a formális módszerek alkalmazásából. A formális módszerek alkalmazása sokféle célt szolgálhat: egyszerűbb karbantarthatóság, könnyebb konstrukció, jobb átláthatóság. [Hal90]

Az *informatikai rendszerek* tervezése során a végcél tehát a rendszer által nyújtott szolgáltatások helyességének biztosítása, és ennek bizonyítása. A matematikai módszerek alkalmazásának előnye éppen abban rejlik, hogy – legalábbis az alkalmazott modellek érvényességi körén belül –, ezt a helyességet 100% valószínűséggel bizonyítják, szemben a tesztelés (tervezett ellenőrző kísérletek) által nyújtott nem teljes bizonyossággal. Az utóbbi néhány évben a *szolgáltatásbiztonság* iránti növekvő igény az informatika területén is egyre inkább növelte a formális módszerek alkalmazása iránti igényt [Pat01].

Az elmúlt években az tapasztalható, hogy a formális módszerek alkalmazási köre is jelentősen nőtt a korábbi évekéhez képest: a rendszereket fejlesztő szervezetek egy része felismerte, hogy a bonyolult rendszerek fejlesztésének és karbantartásának *kézbentarthatóságához* új eljárásokra, módszerekre van szükség. Számos szervezet a formális módszerekben találta meg ezeket az eljárásokat [Cra93].

A *biztonságkritikus* (vagy röviden biztonsági) *rendszerek* tekintetében a formális módszerek legfontosabb jellemzője, hogy a formális notációk, technikák, illetve módszerek támogatják bizonyos rendszerjellemezők matematikai levezetését. Ez magába foglalja egyrészt a specifikáció, a terv és az implementáció tulajdonságai közti kapcsolat formális levezetését, másrészt a formális modell és a valódi problémák és követelmények közti kapcsolat informális elemzését. Ez utóbbi éppen olyan lényeges, mint az előbbi. [Tho95]

A szoftverek egyre inkább növekvő jelentőséggel bírnak a biztonságkritikus rendszerek megvalósításában. A szoftver funkcionalitásának növekedésével azonban a szoftverek komplexitása, bonyolultsága is növekszik, ez pedig a szoftverek biztonságának elérését megnehezíti. Ez az ellentmondás a formális módszerek alkalmazásával feloldható, vagy legalábbis mérsékelhető.

2.1.2. Alkalmazási igény a specifikáció fázisában

A megrendelő követelményei manapság többnyire *informális* módon írják le a létesítendő új, vagy egy a már meglévőhöz illesztendő rendszertől elvárt tulajdonságokat. E követelmények különböző *követelményosztályokba* sorolhatók [Inc92]:

- funkcionális követelmények, amelyek meghatározzák, hogy a rendszernek mit kell tennie,
- nem-funkcionális követelmények, amelyek többnyire a fejlesztő tevékenységének irányát megszabó direktívák,

- célkitűzések, amelyek a fejlesztőt egy választási lehetőség megítélésénél orientálhatják,
- az adatokkal szemben támasztott követelmények,
- tervezési irányelvek, a megvalósításra, kialakításra vonatkozó előírások. Az e szinten megjelenő tervezési irányelvek gyakran az optimálistól eltérő rendszert eredményeznek, mert feleslegesen megkötik a fejlesztő kezét.

A *biztonsági követelmények* vagy egy önálló követelményosztályban, vagy a funkcionális és a nem-funkcionális követelmények részeként szerepelhetnek.

A gyakorlatban azonban a követelmények nem minden esetben sorolhatók be egyértelműen a fenti követelményosztályokba, illetve más *problémák* is felmerülnek a felhasználói követelmények megfogalmazása kapcsán. Az „ideális dokumentáció”-tól való leggyakoribb eltérések [Inc92]:

- pontatlanság/bizonytalanság,
- ellentmondások,
- nem-teljesség,
- különböző követelményosztályok követelményeinek keveredése,
- különböző absztrakciós szintek követelményeinek keveredése,
- a megrendelő naivitása – a megrendelő alá- vagy túlbecsüli az új rendszer képességeit,
- kétértelműség, félreértés – a természetes nyelv gyenge eszköz abban az esetben, amikor precizitásra van szükség.

A tapasztalatok szerint az implementált rendszerben fellépő hibák oka gyakran vezethető vissza *specifikációs hibákra*. Az is kiderült, hogy a specifikációs hibák gyakrabban veszélyeztetik a rendszer biztonságosságát, mint az implementáció során elkövetett hibák [Hei96].

A formális specifikációs technikák alkalmasak arra, hogy a hagyományos specifikációs technikákkal kapcsolatos, az imént vázolt problémák megoldását segítsék (*lásd* 2.2.1. és 2.2.2. fejezetek).

2.1.3. Formális módszerek biztonságkritikus alkalmazások esetén

Az informatikai rendszerek egyre szélesebb körű elterjedésével mindinkább növekszik az általuk nyújtott szolgáltatások minőségével szemben támasztott igény. A létrehozott rendszerek a hardver eszközök teljesítményének növekedésével párhuzamosan mindinkább bonyolultabbak és ma már messze meghaladják azt a határt, amelyet a fejlesztő mérnökök különösebb támogatás nélkül egyáltalán képesek lennének áttekinteni [Pat01].

Az új fejlesztésű vasúti biztosítóberendezési rendszereket is a funkciók egyre növekvő *komplexitása* jellemzi. Ezáltal egyre nehezebbé válik e rendszerek hibamentességének, teljességének, helyességének és ellentmondás-mentességének vizsgálata és igazolása [Anf99].

A vasúti biztosítóberendezések, mint általában a biztonság-kritikus rendszerek bonyolult, sok alrendszerből álló rendszerek, mely alrendszerek bonyolult, komplex kapcsolatrendszerben állnak egymással. A problémát tovább nehezíti, hogy a biztonságkritikus rendszerek gyakran számos párhuzamos működésű komponensből állnak, és általános követelmény a *valósidejűség* az ilyen rendszerekkel szemben [Par98]. A funkcióknak egyre nagyobb részét valósítják meg ilyen rendszerek esetében is szoftver segítségével, ezért rendkívül nagy a *szoftver hibátlanságának* jelentősége.

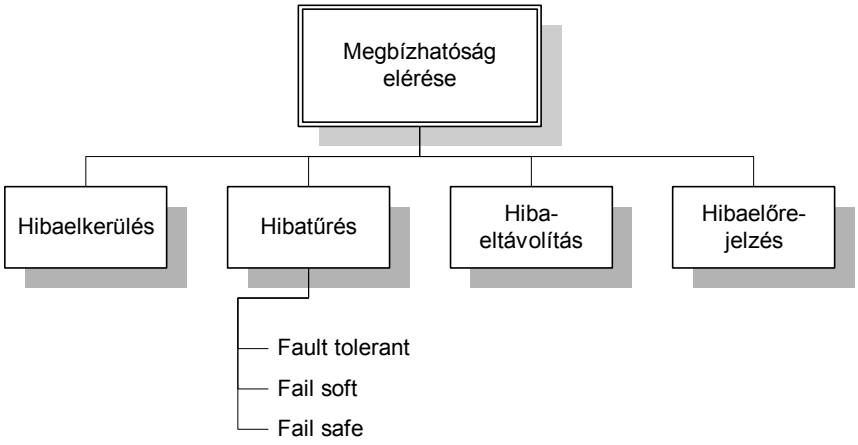
Egyes becslések szerint minden 1000 sor programkódban kb. 3,3 szoftverhiba van [Mye86]. Ez az érték egyáltalán nem meglepő, ha figyelembe vesszük, hogy egy közepes méretű programnak akár 10^{20} különböző lefutási esete is lehetséges [IEEE81]. A szoftverhibák sem egyformák: vannak kisebb és nagyobb programozási hibák, de hatásuk szempontjából nem feltétlenül a kis hibák hatása a legkisebb. A kép még sötétebbé válik, ha figyelembe vesszük a szoftver és a hardver interakciókat.

Mindezek alapján azt mondhatjuk, hogy a rendszer működése során esetlegesen bekövetkező balesetek elkerülésének leghatékonyabb módja az, ha már a tervezés és fejlesztés során eliminálju k, illetve csökkentjük a belső veszélyforrásokat, ugyanis a kész rendszer bonyolultsága már nem, vagy alig uralható [Bow93a].

Az előbbiekből adódóan a biztonságot nem később kell a rendszerhez hozzáadni, mint „adalékot”, hanem a rendszerrel együtt kell fejleszteni. Figyelembe kell továbbá venni, hogy a hardver és a szoftver biztonsága elválaszthatatlan egymástól, ezért a rendszer egészében kell tekinteni, különös figyelmet fordítva a hardver és szoftver közti interfészre [Bow93a].

A rendszer *kívánt megbízhatóságának* (beleértve a rendszer biztonságát is) elérésére négy alapvető megközelítés alakult ki (13. ábra) [Lap91]:

- Hibaelkerülés (*fault avoidance*): a fejlesztés során igyekszünk a hibák előfordulását, bekerülését kiküszöbölni.
- Hibatűrés (*fault tolerance*): olyan, általában redundancián alapuló rendszerkonstrukció, amelynek révén a rendszer a működés során fellépő hibák ellenére a specifikációjának megfelelően működik. A hibatűrésnek több különböző alesetét különböztethetjük meg [Fuk00]:
  - a rendszer megtartja a működőképességét hiba esetén is (szűkebb értelemben vett *fault tolerant*);
  - a rendszer csökkentett funkcionalitással, de tovább működik (*fail soft*);
  - a rendszer nem ad veszélyes kimenetet hiba esetén (*fail safe*).
- Hibaeltávolítás (*fault removal*): hagyományos módon, teszteléssel, verifikációval feltárjuk és kijavítjuk a rendszerben lévő hibát vagy hibákat.
- Hiba-előrejelzés (*fault forecasting*): becsléssel, jóslással állapítjuk meg, hogy rendszerben hiba fog bekövetkezni.



13. ábra. A megbízhatóság elérésének módszerei

A formális módszerek bevetése a *hibaelkerülő technikák* kategóriájába sorolható.

A vonatkozó irodalom legnagyobb része (például [Bow93a]) egyetért abban, hogy a legmagasabb fokú megbízhatóság eléréséhez a fenti *technikák kombinációit* kell alkalmazni. A szoftverek tesztelése által (*hibaeltávolítás*) a programok hibarátája csak kb. 10^{-4}/h értékre

csökkenthető (kb. évente 1 hiba előfordulása), de ahogyan a számítógépek komplexitása és sebessége nő, ez az érték tovább romlik. A *hibatűrő* technikák (például n-verziós programozás) alkalmazása kb. 10-szeres javulási faktort eredményezhet [Mos91]. A hibaeltávolító és a hibatűrő technika kombinált alkalmazásával tehát kb. 10^{-5}/h hibaráta érhető el. Ezzel szemben a biztonság-kritikus szituációk 10^{-9}–10^{-10}/h értéket követelnek meg. Hatalmas tehát a szakadék a között, amit teljesíteni lehet, és ami az elvárás lenne. A probléma megoldásának egyik módja a *hibaelkerülő* technikák alkalmazása, a formális módszerek révén, természetesen a többi, bevált technika további használata mellett. Hogy az ilyen módon kombinált eljárások milyen minőségi javulást eredményeznek, az egyelőre kutatások tárgya.

A formális módszerek alkalmazásának előnye abban rejlik, hogy a formális módszerek azokban a *korai fejlesztési fázisokban* (követelményelemzés, specifikáció, magas szintű tervezés) hatékonyak, amikor a rendszer még eléggé absztrakt és kevésbé komplex, mint a szinte uralhatatlanul bonyolult végső implementáció [Bow93a]. További előny, hogy míg a többi megközelítés (hibaeltávolítás, hibatűrés, hiba-előrejelzés) technikái a korai fejlesztési fázisokban jelentkező problémák megoldására nem kifejezetten alkalmasak, a formális módszerek azonban éppen ezekre a korai fejlesztési fázisokra koncentrálnak.

2.1.4. Üzemeltetés, karbantartás

Korábban, a mikroszámítógépek megjelenése előtt a biztonságkritikus rendszereket, így a vasúti biztosítóberendezéseket is nagyrészt *jelfogós technikával* valósították meg. Ezeknél a rendszereknél a felhasználók, azaz a vasút kötelékében álló rendszerfenntartók egyszerűen és átláthatóan elemezhették és értelmezhették a rendszer belső állapotait a jelfogós hálózat kapcsolási rajza alapján. A kapcsolási rajzok már a tervezés fázisában lehetővé tették a funkciók és a biztonság vizsgálatát, és az üzem közben esetlegesen fellépő hibák következményeinek kiderítését. A kapcsolási rajzok és a kivitelezett vezetékkötések egymásnak való megfelelősége szintén könnyen ellenőrizhető volt.

A *számítógépek* alkalmazásával ez a helyzet megváltozott. A fenntartók számára nem értelmezhetők részletesen a rendszer specifikációi. Ezért a fenntartók a rendszert, illetve annak lehatárolható komponenseit fekete-dobozként kezelik (természetesen minden „doboz” rendelkezik a megfelelő biztonsági jellemzőkkel): ha valami hiba történik, akkor a következők valamelyikét teszik:

1. újraindítják a rendszert;
2. átadják a vezérlést egy alternatív rendszernek;
3. kicserélik az érintett „fekete-dobozt”.

A hardverhibák kezelhetők, és kijavíthatók ezen a módon, de a hardverhibákéhoz hasonló tünetek jelenthetnek *szoftverhibát* is. Ilyenkor a hiba hatása gyakran eltüntethető az előbbi módszerekkel, azonban a hiba igazi oka csak a szoftver cseréjével szüntethető meg.

A biztonságkritikus rendszereket, így a vasúti biztosítóberendezéseket is, üzembehelyezésük előtt alaposan tesztelik, ám ha a működés során szoftverhiba lép fel, akkor rendkívül nehéz a hiba lokalizálása, sőt a hiba javítása sem egyszerű az ún. *újra-bekerülési hiba* veszélye miatt. Ehhez hasonlóan komoly nehézséget jelent a már meglévő szoftverek módosítása, és ennek során annak felmérése, hogy az adott programmodulban történő változtatás a rendszer mely más részeire lesz hatással.

Ezeket az aspektusokat megvizsgálva azt mondhatjuk, hogy a formális módszereknek a rendszerek fejlesztésén túl, a rendszerek *üzemeltetésében* és karbantartásában is jelentős szerepe lehet [Fuk00].

A formális technikák vasúti területen történő alkalmazásának van *szociológiai motivációja* is [Bjo00]. A vasút majdnem egy évszázadon át stabil személyzettel működött. Az alkalmazottak, ha egyszer odakerültek a vasúthoz, akkor a legtöbbször nem is váltottak többé munkahelyet. A vasúti terület másik fontos jellemzője volt korábban a lassan változó technológia. Az egész életükben a vasútnál dolgozókban felhalmozódott tudást és ismeretanyagot a tapasztalt alkalmazottak szóban oktatták, adták tovább a szükséges ismereteket az újonnan belépőknek. Akkor erre volt elegendő idő.

Mára a helyzet megváltozott. Jelentős lett a munkaerő-áramlás, gyakran jönnek új alkalmazottak, akiket természetesen ki kell képezni, és ehhez járul még az, hogy a vasúti technológia is gyorsabban változik – gyorsabban, mint amennyi időt az alkalmazottak általában a vasútnál töltenek. Ma a számítógépeknek kell „átvenniük" a vasúti dolgozók munkájának ellátásához szükséges tudást. Ezért kódolni kell ezt az ismeretanyagot, pontosan, egyértelműen, úgy, hogy az az ember számára is érthető legyen, ugyanakkor a számítógépek is fel tudják dolgozni. Ezen a területen is rendkívül nagy szerepe lehet a formális technikáknak.

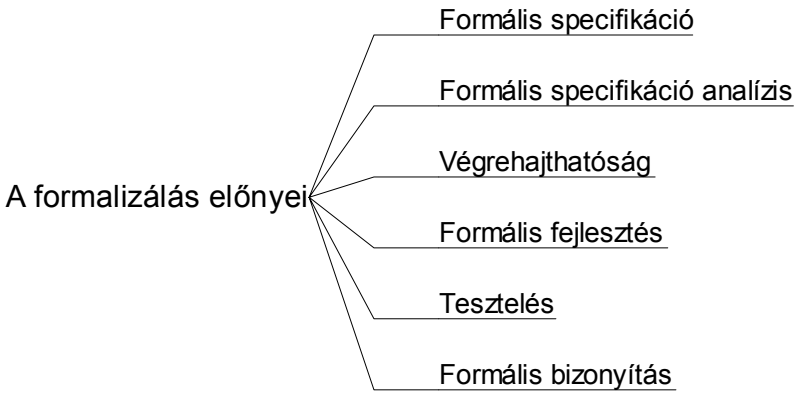
2.2. A formalizálás előnyei

A formális módszerek gyökerei az automatikus funkcióvizsgálatok kutatására, a 60-as évek második felére, illetve a 70-es évek elejére nyúlnak vissza. Az utóbbi tíz év kutatásai a rendszerspecifikáció és -fejlesztés, illetve az egyes fejlesztési fázisok számára alkalmas matematikai nyelvekre és a hozzájuk kapcsolódó módszerekre koncentráltak [Inc92].

A formális módszerek matematikai (például logikai, halmazelméleti) jeleket alkalmaznak a rendszerek leírására az egyes fejlesztési fázisokban. A matematika alkalmazása a *rendszerspecifikáció* céljára számos előnnyel jár. Ezek:

- különböző absztrakciós szintek ábrázolása könnyen megvalósítható,
- matematikai formában könnyű érvelni,
- a matematika kompakt,
- a matematika egyértelmű,
- a matematikával a valóság modellezhető.

A következő fejezetekben áttekintjük a formális módszerek alkalmazása által elérhető előnyöket (14. ábra). Először a specifikáció formalizálásával járó előnyökkel, majd a formális specifikáció analízise nyújtotta lehetőségekkel foglalkozunk. Ezután a specifikáció végrehajthatóságának előnyeit mutatjuk be, majd a formális módszerek lehetőségeit a formális fejlesztés vonatkozásában, a teszteléssel, végül pedig a formális bizonyítás lehetőségével kapcsolatban.



14. ábra. A formalizálás előnyei

2.2.1. Formális specifikáció

A hagyományos specifikációs technikák legnagyobb hátránya a szükséges precizitás és egyértelműség hiánya. A formális technikákban alkalmazott matematikai szintakszis, illetve szemantika a specifikációs dokumentumokat *matematikai pontosságúvá*, a jól definiált szemantika révén pedig *egyértelművé* teheti [Ehr99]. Ez kiterjed a célzott rendszer

- funkcióira,
- időzítéseire, teljesítményére, illetve
- esetlegesen belső struktúrájára is [Pat01].

[Hal90] véleménye szerint az a jó specifikáció, amely csak azt specifikálja, hogy a rendszernek mit kell tennie, nem pedig azt, hogy hogyan, tehát a specifikációnak nem szabad foglalkoznia a specifikálandó rendszer struktúrájával. Vasúti biztosítóberendezések vonatkozásában ez igaz lehet a vasúti feltétfüzetekre, amelyben a vasút több lehetséges szállító számára fogalmazza meg a biztosítóberendezéstől elvárt funkciókat, így az nem foglalkozhat a rendszerstruktúrával. A struktúrának a specifikáció szintjén való megjelenése tehát alkalmatlanná teszi a formális specifikációt vasúti feltétfüzet megfogalmazására.

Más tapasztalatok, például [Cic99] azt mutatják, hogy a specifikáció formalizálásával bizonyos *strukturális tervezési feladatok* előre kerülnek a specifikáció fázisához, ez pedig kifejezetten előnyös lehet. A vasúti biztosítóberendezések ún. gyári feltétfüzete esetében (amely a vasút által elvárt funkciók cégspecifikus megoldási módjait specifikálja) például már megjelenhet a specifikált rendszer strukturális leírása is.

A formális módszerek alkalmazása – egyebek mellett – segít a megrendelő *informális követelményeinek tisztázásában* is. A formális specifikáció által kikristályosodnak a megrendelő bizonytalan követelményei, napvilágra kerülnek a követelményekben megbúvó ellentmondások, többértelműségek és nem-teljességek. Az informális specifikációval összehasonlítva a specifikálónak jobbak a lehetőségei folyamatosan kérdéseket intézni a megrendelőhöz, és az arra kapott válaszok szisztematikus feldolgozásával tovább pontosítani a specifikációt. Mind a megrendelő, mind a specifikáló folyamatosan tehet fel kérdéseket. Ezek megválaszolásával eldönthető, hogy a specifikáció tükrözi-e a megrendelő elképzeléseit, illetve hogy a specifikandusok a kívánt tulajdonságokkal bírnak-e [Win90].

A formális specifikáció esetében nehéz „mellébeszélni” vagy „kozmetikázni”. Ha pontatlanság, ellentmondás, többértelműség van a gondolkodásban, akkor az könyörtelenül kiderül: nem lehet koherens specifikációt készíteni [Hal90].

A formális specifikáció alkalmazásával a fejlesztendő rendszer mélyebb ismerete érhető el azáltal, hogy a formalizálás egyszerre kényszeríti a fejlesztőt absztrakcióra és precizitásra [Win90].

A formális specifikáció bármilyen *hiba megkeresését* könnyebbé teszi. Egy informális specifikációban nagyon nehéz megmondani, hogy mi hibás és mi nem, mert nem egyértelműek a kijelentések. Ha szükséges, a specifikáló könnyen meg tudja védeni az általa készített informális specifikációt, mivel az könnyen átértelmezhető a felmerült kritikának megfelelően. A formális specifikáció egyértelműsége miatt a hibák könnyebben megtalálhatók, és egy adott hiba feltátása esetén sokkal könnyebben egyetért mindenki abban, hogy az valóban hiba. A gyakorlati tapasztalatok szerint a hibák könnyű feltárása a formális módszerek egyik kulcsfontosságú előnye. Bármilyen formális bizonyítás, vagy formális fejlesztési lépés nélkül, pusztán az a tény, hogy a specifikáció formalizált, számos előnnyel jár: a formális specifikációk vizsgálatával több hiba fedhető fel, mint az informális

specifikáció vizsgálatával [Hal90]. A *hibák korai felismerése* által meggátolható, hogy bizonyos hibák „végigvonuljanak” a teljes fejlesztési folyamaton [Lar96].

A tapasztalatok szerint könnyebb megépíteni egy rendszert a formális specifikáció alapján, mint más dokumentumok alapján. Ez akkor is igaz, ha maga a fejlesztés nem formális, tehát például a program kódolása manuálisan történik [Hal90].

Ezenkívül sokkal egyszerűbb a kész rendszernek egy formális specifikációval való összevetése, mint bármilyen más tervezési dokumentummal való összevetése [Hal90].

Ezek a tulajdonságok a formális specifikációt olyan előnyössé teszik, hogy érdemes a specifikáció fázisát akkor is formalizálni, ha a fejlesztés további szakaszaiban egyáltalán nem alkalmazunk formális módszereket. Sok projekt esetében a fejlesztésnek a specifikáció az egyetlen formális fázisa.

Mindezen előnyök ellenére a legtöbbször még a formális specifikációk sem tökéletesek. Amikor a projekt az implementáció fázisához ér, napvilágra kerülhetnek a specifikáció hiányosságai. Amikor ez megtörténik, akkor nagyon fontos, hogy a *specifikációt* is megfelelően *módosítsuk*, ugyanis nagy a kísértés, hogy a problémát egyszerűen csak az implementáció szintjén hárítsuk el. Ez utóbbi esetben azonban vészesen növekedni fog a specifikáció és az implementáció közti divergencia, ez pedig azt okozza, hogy a rendszer karbantartásához a specifikáció egyáltalán nem lesz használható. Ha a specifikáció és az implementáció folyamatosan megfelel egymásnak, akkor a specifikáció nagyon értékes dokumentációvá válik a rendszer egész életciklusát tekintve [Hal90].

A formális specifikációk segítségével a megrendelők tisztábban látják, hogy mit fognak kapni. A specifikáció azt fogalmazza meg, hogy a megrendelő mit akar, még mielőtt a rendszer megépítésre kerülne. Ezt az előnyt akkor használhatjuk ki, ha a specifikáció olvasható a megrendelő számára. Ennek három módja lehet:

- a specifikáció természetes nyelvre való fordítása,
- a specifikáció következményeinek demonstrációja (matematikai bizonyítása) (*lásd* 2.2.2. fejezet),
- a specifikáció animációja, szimulációja (*lásd* 2.2.3. fejezet).

Az első módszer szinte mindig szükséges. A matematikai specifikációt ki kell egészíteni egy természetes nyelven készült leírással, amely megmagyarázza, hogy mit jelent a specifikáció a valós világ fogalmai szerint. Erre a tevékenységre megfelelő időt és forrást kell biztosítani. A tapasztalatok azt mutatják, hogy a formális specifikáció alapján készült informális leírások jobban követhetőek, pontosabbak, rövidebbek és jobban használhatók a megrendelő számára, mint az eredetileg informálisan készült specifikációk. Egy jól elkészített formális specifikációból a matematika később teljesen elhagyható, és az így kapott természetes nyelvű leírás sokkal jobban specifikálja a rendszert, mint egy hagyományos informális specifikáció [Hal90].

A formális leírás további előnye, hogy általa a specifikáció függetlenedhet az adott természetes nyelvtől, ez pedig elősegíti a nemzetközi átjárhatóságot. A nyelvi eltérésekből származó átfordítási problémák például nagyon megnehezíthetik valamely vasúti biztosítóberendezési rendszer alkalmazását különböző országokban. A formális specifikáció ezeket a problémákat legalábbis részben képes megoldani. Ugyanez igaz a különböző vasutak közti biztonságfilozófiai eltérések kezelésére is.

2.2.2. Formális specifikáció analízis

A specifikáció megírásának első fázisa minden esetben a *matematikai modell* megfogalmazása. Ez önmagában is kreatív tevékenység, amely hozzájárul a rendszer működésének mélyebb megértéséhez. Ugyanakkor a létrejött matematikai modellen a specifikációs minőséget is ellenőrizni lehet [Pat01].

A legtöbb formális módszer olyan formális specifikációs nyelven alapul, amelyhez jól definiált logikai következtetési rendszer is tartozik. A következtetési rendszer lehetővé teszi a formális módszer alkalmazója számára, hogy a rendszer viselkedését megjósolja anélkül, hogy a rendszert magát működtetni, illetve egyáltalán megépíteni kellene. Az explicit módon definiált következtetési szabályoknak nagy előnye, hogy a *következtetési folyamat* nagymértékben automatizálható [Win90].

Amennyiben tehát a rendszerspecifikáció matematikai precizitással (formális szintaktikával) és formális szemantikával áll rendelkezésre, *formális analízis* révén bizonyos rendszertulajdonságok már a specifikációs fázisban vizsgálhatók [Ehr99]. Ez a formális módszerek alkalmazásának egyik fontos perspektívája a biztonsági rendszerek területén, különösen ha törvényi előírásoknak vagy szabványoknak kell megfelelni, illetve az azoknak való megfelelőséget igazolni kell [Tho95].

A specifikáció *bizonyítható tulajdonságai* közé tartozik a specifikáció konzisztenciája, illetve a definiált operációk teljessége. A szolgáltatás minősége, illetve kifejezetten a rendszer biztonsága [Jaf91] szempontjából e két specifikációs tulajdonságnak kiemelt jelentősége van [Pat01].

- *Konzisztencia* vagy *ellentmondásmentesség*: a specifikáció által a célrendszer funkcionalitásával szemben támasztott követelmények egyidejűleg kielégíthetők [Pat01], azaz a rendszer mentes egymással ellentétes követelményektől [Par98].
- *Teljesség* vagy *zártság*: a specifikáció minden esetre kiterjed [Pat01], azaz minden lehetséges bemenethez létezik specifikált viselkedés [Par98];

[Win90] szerint a gyakorlatban a specifikációk gyakran *nem teljesek*, legalábbis matematikai logikai értelemben nem. Ennek az az oka, hogy a specifikálók gyakran hagynak dolgokat specifikálatlanul, egyrészt szándékosan, azért, hogy az implementálónak bizonyos fokú szabadságot biztosítsanak. Másrészt akaratlanul is specifikálatlanok maradnak bizonyos részek, ugyanis a specifikáló nem látja előre az összes lehetséges, specifikálandó esetet. Végül pedig azért sem teljesek a specifikációk, mert azokat a specifikálók fokozatosan, iteratív módon készítik, többek között a változó megrendelői követelmények miatt.

A specifikációk tekintetében meg kell találni az egészséges *egyensúlyt* az éppen elegendően és a túlságosan specifikált között. A specifikálónak annyiban kell teljességre törekednie, hogy az implementáló ne választhasson a termék szempontjából elfogadhatatlan megoldásokat. Ezért a specifikáló nem lehet túlságosan nagyvonalú. Ugyanakkor a túlzott specifikálás túl kevés szabadságot hagy az implementálónak, és ez gyakran lehet oka az ún. implementációs eltérítésnek. Implementációs eltérítésen azt értjük, hogy a specifikáció a rendszer kívülről nem megfigyelhető tulajdonságát is specifikálja, és ezáltal esetleg szükségtelen kényszereket támaszt a specifikandussal szemben [Win90].

Formális specifikáció esetén, mint láttuk, *bizonyítani* lehet, hogy a specifikáció teljesít-e bizonyos kulcsfontosságú követelményeket. A biztonság és a védettség tekintetében ez bizonyos integritást jelenthet. Természetesen ez csak akkor lehetséges, ha a megrendelői követelmények maguk kifejezhetők formálisan. Mivel a hibák elhárítása a specifikáció szintjén jóval olcsóbb, mint a későbbi fejlesztési fázisokban, a specifikáció tulajdonságainak

bizonyítása legalább akkora, ha nem nagyobb jelentőséggel bír, mint az implementált rendszer helyességének bizonyítása [Hal90].

Fontos megjegyezni, hogy a formális módszerek alkalmasak arra, hogy egy rendszer *teljes viselkedését* vizsgálják, nemcsak a rendszer viselkedésének egy nem teljes halmazát, mint a hagyományos technikák (végrehajtás, szimuláció, prototyping) [NASA97].

A formális specifikáció analízisnek *két alapvető formája* terjedt el:

- a modellellenőrzés és
- a tételbizonyítás [Pat01].

Modellellenőrzés. A modellellenőrzés egy olyan technika, amely a rendszer egy véges modelljén bizonyítja be, hogy a megkívánt tulajdonság teljesül [Pat01]. Bár maga a modell véges, nem elégséges absztrakció esetén, a gyakorlati feladatok során hatalmas állapotterek jönnek létre, amelyeknek kimerítő bejárása reménytelen. Ennek megfelelően a modellellenőrzés során a fő technikai kihívás a nagy állapotterek kezelése. A modellellenőrzésnek a gyakorlatban két általános eszköze terjedt el.

- Az első, a *temporális modellellenőrzés*, alapvetően a temporális logikán alapul, és a rendszereket mint véges állapotú rendszereket modellezi. Valamennyi temporális modellellenőrző rendszer magja egy olyan hatékony keresési eljárás, amely azt nézi meg, hogy a vizsgált véges állapotátmeneti rendszer a specifikáció modellje-e, ideértve azokat az eseteket is, amikor két különböző reprezentáció ekvivalenciáját vizsgáljuk.
- Egy alternatív megközelítés *automaták* formájában történő specifikáción alapul, melyben a rendszer automatamodelljét és a specifikáció automatatmodelljét hasonlítjuk össze. Az egyezés kritériumának számos megfogalmazása létezik, például
  - a generált, illetve felismert nyelvek tartalmazása,
  - a finomítási, illetve
  - a megfigyelhetőségi ekvivalencia.

A temporális logika bázisú modellellenőrzést át lehet fogalmazni automataelméleti formára, ilymódon a két megközelítés ekvivalenssé tehető. A modellellenőrzés megközelítés jelentősége az, hogy teljesen automatizálható és gyors, gyakran perc-óra nagyságrendű futási időben kezelve komplex problémákat is. Legfőbb veszélye a megközelítésnek az *állapottér robbanása*. A nagy áttörést ezen a területen a rendezett bináris döntési diagramok (OBDD) alkalmazása hozta, amellyel 10^{20} nagyságrendű állapottér vált számítástechnikai eszközökkel is ellenőrizhetővé. Ezt további minimalizáció és redukciós eljárások finomították az idők során. Ma a modellellenőrzők 100-200 állapotváltozót és akár 10^{120} elérhető állapotot is tudnak vizsgálni. Abban az esetben, hogyha mindezt kellő absztrakciós technikával egészítik ki, akkor elvileg, és lassan gyakorlatilag is, a vizsgálható állapotok száma korlátlanná válik [Pat01].

Tételbizonyítás. A tételbizonyítás alapötlete az, hogy a rendszerleírást és a megkívánt tulajdonságok specifikációját egyaránt valamilyenfajta *matematikai logikában* írják le. Ezt a logikát formális módon építik fel; axiómákat és következtetési szabályokat tartalmaz. A tételbizonyítás feladata ezután az, hogy a megkívánt tulajdonságot az adott rendszerben az axiómákból levezesse. E bizonyítási sorozat folyamán axiómákat, szabályokat, illetve ezekből levezetett definíciókat és köztes lemmákat lehet használni. Bár a bizonyításokat kézzel kell megcsinálni, a tételbizonyítást gép segíti azáltal, hogy csak megengedett lépéseket szabad a kezelőnek végrehajtania. Így az esetleges tévesztés okozta hamis bizonyítások kizártak.

A tételbizonyító rendszerek spektruma a nagymértékben automatizált általános célú rendszerektől a célrendszerekig terjed. Előnyük az, hogy a számítások szimbolikus jellege

miatt elvben végtelen állapotteret is kezelhetnek, hiszen például a struktúrán alapuló teljes indukció megengedi végtelen terek kezelését is.

Ezen alkalmazásokat gyakran használják processzorok tesztelésénél (például IBM PowerPC, System/390, Motorola 68020, AMD5K86, Motorola CAP stb.) [Pat01].

2.2.3. Végrehajthatóság

A formális módszerek egy része támogatja a specifikációk végrehajthatóságát, azaz számítógépen való futtathatóságukat. Egy *végrehajtható specifikációs nyelv* definíciójától fogva kötöttebb a kifejezőerőt tekintve, mint egy nem végrehajtható, ugyanis a segítségével leírt funkcióknak számíthatóknak és véges tartományokon definiáltnak kell lenniük. A végrehajtható specifikációk, e korlátozás ellenére, jelentős szerepet töltenek be a rendszerek fejlesztési folyamatában. A specifikáló számára a végrehajtható specifikáció azonnali visszacsatolást jelent; ez megkönnyíti az adott formális technikával való munkát. A végrehajtható specifikáció annak a lehetőségét kínálja, hogy a formális specifikációt mint a *rendszer első prototípusát* kezeljük, ami által tesztelni lehet a specifikandust [Win90].

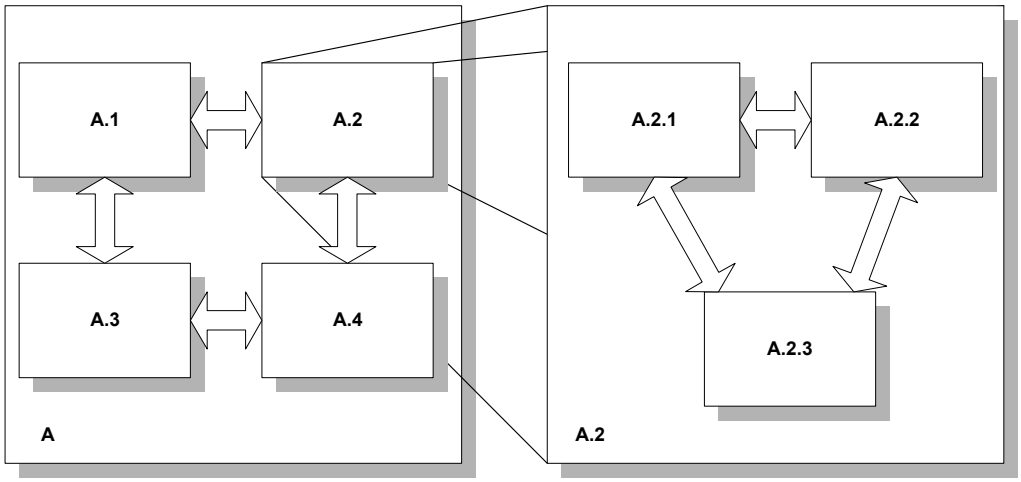
Amennyiben a formális specifikáció nem futtatható, gyakran lehetőség van arra, hogy adekvát transzformációkkal egy legalább részben futtatható verziót állítsunk elő [Ehr99]. A futtatható specifikáció arra is alkalmas lehet, hogy a követelményrendszer formalizálásának helyességét igazoljuk. A specifikáció megerősítésére [Fuk00] szimulátor alkalmazását javasolja. A Siemens AG Közlekedéstechnikai Ágazata által kifejlesztett GRACE fejlesztőrendszer [Red99] egyik alkalmazása szintén a specifikációnak a megrendelővel történő egyeztetésére és helyességének ellenőrzésére irányul, a *formális specifikáció szimulációja* segítségével.

2.2.4. Formális fejlesztés

Formális fejlesztésnek azt a tevékenységet nevezzük, amikor a formális módszereket a fejlesztési folyamat során alkalmazzuk oly módon, hogy a specifikációt szabályok és tervezési kalkulusok felhasználásával finom lépésekben végrehajtható programmá finomítjuk. E folyamat során a dekompozíció és a finomítás (15. ábra) kiemelt jelentőségű tevékenységek [Win90, Ehr99].

A *dekompozíció* az a folyamat, amelynek során a rendszert kisebb modulokra bontjuk. A specifikálónak ilyenkor pontosan rögzítenie kell a modulok közötti interfészeket. Minden interfész-specifikáció pontosan leírja a modul felhasználói számára azokat az információkat, amelyek szükségesek a modul használatához, mindezt a modul implementációjának leírása nélkül. Ezenfelül a specifikáció biztosítja az implementáló számára szükséges információkat az implementáláshoz, anélkül, hogy az implementálónak tudnia kellene arról, hogy mely más egységek fogják a modult felhasználni. Így mindaddig, amíg a modul interfésze változatlan, a modul implementációja változtatható anélkül, hogy az a többi modult érintené.

A *finomítás* a különböző absztrakciós szintek kezelését foglalja magába; ami egy adott absztrakciós szinten egyetlen modul, az egy finomabb felbontásban modulok csoportja. Minden finomítási lépésben meg kell mutatni, hogy egy adott szintű specifikáció (vagy a program) kielégíti a magasabb szintű specifikáció(ka)t. A kielégítés bizonyítása gyakran további feltételezéseket, bizonyítási kötelezettségeket generál, melyeket teljesíteni kell. A formális módszerek megfelelő keretet biztosítanak a bizonyítási kötelezettségek megállapításához és azok végrehajtásához [Win90].



15. ábra. Dekompozíció és finomítás

A Vienna Development Method (VDM), a Z, és a Larch tipikusan olyan formális módszerek, amelyek kiválóan alkalmasak rendszerek fejlesztésére, tervezésére [Win90].

Az újrafelhasználhatóságnak, vagyis generikus modulok elkészítésének és alkalmazásának egyik előfeltétele a *parametrizálhatóság*. A rendszerspecifikáció matematikai megfogalmazása révén bizonyos rendszertulajdonságok paraméterezése is könnyebbé válhat [Ehr99]. Ez az előny nemcsak a specifikációs fázisban, hanem a rendszer teljes életciklusa során igen jól hasznosítható. E tulajdonság különösen fontos az *ismételt alkalmazások* és az utólagos *illesztések* esetében.

A fejlesztendő rendszer *kódjának generálása* nem automatizálható, ha a specifikáció nem elegendően precíz. Ha azonban a specifikációt formális szintaktikával és szemantikával állították elő, a kódgenerálás algoritmizálható, és így automatizálható is egy fordítóval *(compiler)*, amely a formális specifikációból a megfelelő programnyelv forráskódját állítja elő.

A formális notáció arra kényszeríti a fejlesztőt, hogy már a fejlesztés korai szakaszában a rendszerstruktúrára és a lényeges rendszerjellemzőkre koncentráljon. A formális specifikáció támogatja az eltérések, inkonzisztenciák és azok következményeinek szisztematikus keresését [Cic99].

A formális módszerek megkövetelik, hogy a rendszer összefüggéseiről szóló feltételezések explicit módon legyenek megfogalmazva. Ez különösen fontos beágyazott *(embedded)* rendszerek esetében, márpedig a biztonsági rendszerek nagy része ilyen. A formális módszerek nemcsak támogatják a feltételezések explicit kifejtését, hanem kibogoznak bármilyen implicit feltételezést a formális érvelés folyamán [Tho95].

A formális technikák alkalmazásával a hibákat korábban lehet detektálni az életciklusban, mint a hagyományos fejlesztési tevékenységek esetén. A hibák nagy része már a magas szintű tervezés *(high-level design)* során felfedhető, amíg korábban azok csak a programozás, illetve kódolás során kerültek volna napvilágra. Természetesen a szigorúbb formális módszerek több hibát tudnak felfedni; esetenként garantálhatják bizonyos hibák meg nem létét [NASA97].

A formális módszerek alkalmazása elsősorban a *rendszer helyességének biztosításában* segít. A formális módszerekkel, ezen túlmenően, olyan minőségbeli javulás érhető el (egyszerűség, strukturáltság), amely kihathat a teljesítményjellemzőkre, valamint a könnyebb kezelhetőségre is [FME97].

A rendszerfejlesztés rendkívül fontos, és sajnos gyakran negligált része a *dokumentáció*. A dokumentációnak, különösen későbbi változtatások esetén hatalmas jelentősége van. A

dokumentáció formalizálása kevesebb félreértéshez és így kevesebb hibához vezethet [Bow93b].

2.2.5. Tesztelés

A formális leíróeszközök és a számítógéppel támogatott módszerek alkalmazása a tesztelés néhány alapvető problémájának megoldását is egyszerűbbé teszi.

Ha a formális modellek futtathatóak, akkor ezek végrehajtása mint *a rendszer első tesztje* tekinthető, aminek révén az implementált rendszer későbbi tesztjei jelentősen rövidebbek lehetnek [Ehr99].

A formális specifikáció önmagában alkalmas arra, hogy teszt-seteket lehessen belőle generálni *feketedoboz* típusú (black-box) *tesztelés* céljára.

A pusztán az implementáció analízisén alapuló tesztelési eljárások önmagukban nem elegendőek: a specifikációt is figyelembe kell venni. Ugyanis például egy implementáció útvonaltesztelése eredményes lehet önmagában, de egy ilyen módszer szisztematikusan nem képes felfedni esetlegesen hiányzó útvonalakat. A *specifikáció és az implementáció összevetése* egyéb tesztelési, elemzési feladatok ellátásában nyújt segítséget, mint útvonaltesztelés, modulteszt és integrációs teszt. Az egységtesztelés és az integrációs tesztelés eredménye nagymértékben függ attól, hogy az egyes modulok specifikációja mennyire precíz [Win90].

A *tesztelési környezet* meghatározásához a rendszerspecifikáció határai képezik az alapot. A már korábban kifejlesztett szomszédos, kapcsolódó rendszerek formális modellje, mint a környezet modellje, bővített és validált tesztelési környezetként kínálkozik számunkra.

Ha a rendszert formális leíróeszközök segítségével írták le, és verifikált fejlesztő eszközök állnak rendelkezésre, *a hagyományos tesztek mennyisége jelentősen csökkenthető*. A formális módszerek révén a specifikációs és a fejlesztési fázisban sok hiba elkerülhető, így a későbbiekben már nem szükséges e hibák megtalálására teszteket alkalmazni.

A formális módszerek természetesen *nem teszik feleslegessé a tesztelést*. A megrendelő minden esetben igényli a rendszer működésének tényleges adatokkal történő bemutatását az üzembehelyezés előtt annak érdekében, hogy meggyőződhessen a rendszer helyes működéséről. Hasonló módon szükség van a rendszer üzemelése során karbantartási célú tesztek futtatására. Bizonyos biztonságkritikus rendszerek esetében ezeket a teszteket szabványok írják elő [EN50126, EN50128, EN50129].

2.2.6. Formális bizonyítás

Biztonsági felelősségű rendszerek esetén be kell tudni *bizonyítani*, hogy a rendszer implementációja megfelel a rendszerspecifikációnak. Hagyományos módon többnyire nem lehetséges ezt a bizonyítást szigorú matematikai alapon elvégezni, ugyanis bár a rendszer implementációja a szoftver esetében mindenképpen formális dokumentum, a specifikációval való összevethetőség a specifikáció nem-formális volta miatt meglehetősen nehéz. Ha azonban mind a *specifikáció*, mind az *implementáció formális szemantikával* van megfogalmazva, ez az egymásnak való *megfelelőség* matematikai transzformációk révén *bizonyítható* [Ehr99].

Problémát jelent, hogy egy nagyobb rendszer helyességét *általában nem lehet teljes körűen bizonyítani*, csak kisebb részekét. Az egyik kulcskérdés itt, a kisebb, kritikus részek számára megfelelő környezet biztosítása [Win90].

Vannak olyan tulajdonságok is, amelyek megléte *csak* formális okfejtéssel állapítható meg. Sok követelményre jellemző, hogy olyan általános állításokat tartalmaz, mint például „a program mindig naplózza a felhasználói akciókat” vagy „a program nem veszíthet el üzenetet”. Az ilyen követelmények teljesítése nem ellenőrizhető teszteléssel vagy szimulációval, de formálisan bizonyítható [Hal90].

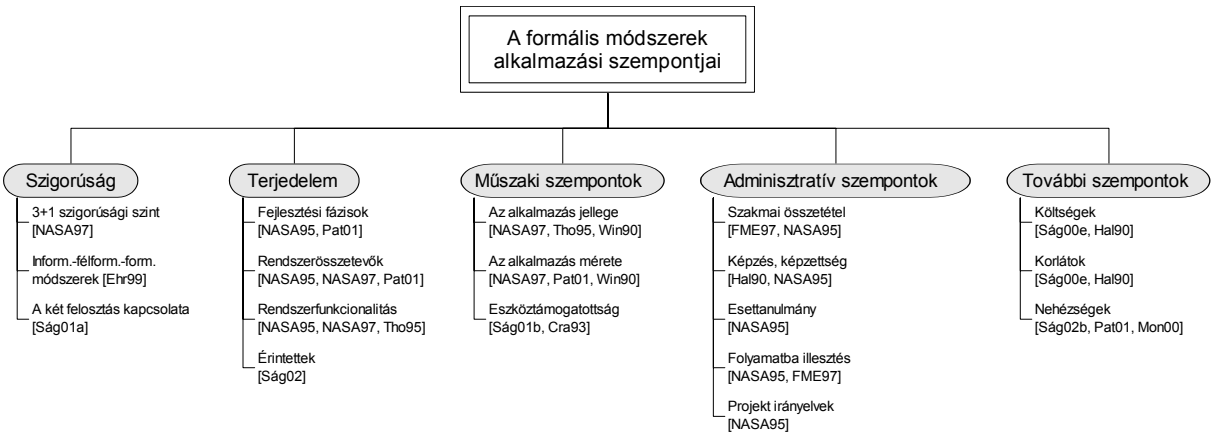
3. Alkalmazási szempontok

A formális módszerek alkalmazhatóságát, illetve az alkalmazás hatékonyságát egy-egy projekt esetében többféle tényező befolyásolja [Ság02a] (16. ábra). E fejezet célja a szakirodalomban megtalálható ilyen szempontok tárgyalása, új szempontok meghatározása, valamint a szempontok egységes rendszerbe való foglalása.

Az alkalmazás szempontjai közül kiemelt jelentősége van a választott formális módszer *szigorúságának* és annak, hogy a formalizálás mire terjed ki. Ez utóbbinak számos dimenziója van: az *alkalmazási terjedelem* megkülönböztethető a projekt *fejlesztési fázisai* szerint, a rendszer *összetevői* és *funkciói* szerint, valamint a formalizálás által *érintettek köre* szerint. A formalizálás szigorúsága és terjedelme olyan egymástól független szempontok, amelyek kombinációi döntően befolyásolják a formális módszerek alkalmazási lehetőségeit.

A szigorúságon és a terjedelmen kívül más tényezők is befolyásolhatják egy adott módszer alkalmazásának hatékonyságát. E szempontok egy része *műszaki*, másik része inkább *adminisztratív* jellegű. Műszaki szempontból fontos az adott alkalmazás jellege, illetve az alkalmazás mérete és struktúrája, illetve az adott formális módszer eszköztámogatottsága. Az adminisztratív szempontok között szerepel a projektben résztvevő személyzet szakmai összetétele, képzettsége, az esetleges bevezető esettanulmány tapasztalatai, a fejlesztési folyamatba való integrálhatóság és az adott projektre vonatkozó irányelvek. Természetesen ezek az adminisztratív és műszaki szempontok szorosan kapcsolódnak egymáshoz és egymásra is hatással vannak.

A formális módszerek további alkalmazási szempontjai között feltétlenül meg kell említeni a formális módszerek alkalmazásával kapcsolatos költségeket is. A formális módszerek alkalmazásától akkor várhatunk eredményeket, ha tisztában vagyunk a formális módszerek alkalmazási lehetőségeivel, ha nem támasztunk irreális elvárásokat a formális módszerekkel szemben. Ehhez meg kell ismerni a formális módszerek és alkalmazásuk alapvető korlátait. Végezetül pedig a formális módszerek széleskörű elfogadtatásához előnyös, ha megvizsgáljuk azokat a tényezőket, amelyek a formális módszerek bevezetését megnehezítik.



16. ábra. A formális módszerek alkalmazási szempontjai ([Ság01b] alapján)

3.1. A formalizálás szigorúsága

A formális módszerek a formalizálás szigorúságának különböző szintjein alkalmazhatók [NASA95, NASA97]. Egy a formalizálás *alacsonyabb szintjén* alkalmazott leírás viszonylag rugalmasabb, könnyebb olvasni és megérteni. Hátránya ezzel szemben a precizitás és az egyértelműség hiánya. A formalizálás *szigorúságának növelésével* a precizitás és az egyértelműség javulhat, mivel a specifikáció és a következő fejlesztési/tervezési fázisok a szubjektív interpretálástól függetlenebbek és a módszeres analízis számára adekvátabbak lesznek. Ezáltal azonban az olvashatóság és az érthetőség megnehezedik. Azt is figyelembe kell venni, hogy minél szigorúbb a formalizálás, annál nagyobb a számítógépes támogatás iránti igény. A következő osztályozás a formalizálás szigorúságát egy négyszintű rendszerben mutatja be [NASA97].

0. szint: A természetes nyelven vagy egy programnyelven írt és esetleg diagramokkal, képletekkel kiegészített dokumentáció manuális áttekintése és elemzése. Az e szinten végzett tevékenység nem formális, azonban a hagyományos gyakorlatot jól tükrözi, és így jó elvi és strukturális alapul szolgálhat a magasabb szinteken végzendő tevékenységek megszervezéséhez.
1. szint: Logikai, illetve diszkrét matematikai jelölések alkalmazása a precízebb fogalmazás érdekében. Az analízis ezen a szinten informális.
2. szint: Formális specifikációs nyelv alkalmazása, automatizált eszközökkel támogatva (például szintaktikai-, típusellenőrzés).
3. szint: Teljesen formális specifikációs nyelv alkalmazása, szigorú szemantikával, és az ennek megfelelő, adekvát formális bizonyítási módszerrel.

A 0. szint technikáit (intuitív - fél-formális szintaktika, intuitív szemantika) informális technikáknak, az 1. és 2. szint technikáit (fél-formális - formális szintaktika, intuitív – fél-formális szemantika) fél-formális technikáknak, a 3. szint technikáit pedig (formális szintaktika és szemantika) formális technikáknak nevezhetjük [Ehr99]. A [NASA97] és az [Ehr99] által javasolt szigorúsági felosztás közti kapcsolat a 2. táblázatban látható [Ság01a].

2. táblázat. A formalizálás szigorúságának szintjei [Ság01a]

<table>
<tr><td rowspan="4">Szemantika</td><td></td><td colspan="3">Szintaktika</td></tr>
<tr><td></td><td>Intuitív</td><td>fél-formális</td><td>formális</td></tr>
<tr><td>Intuitív</td><td colspan="2">0. szint
„Manuális” áttekintés, elemzés.
Nem formális tevékenységek, a hagyományos gyakorlatot tükrözi.</td><td>1. szint
Logikai, diszkrét matematikai jelölések alkalmazása a precizitás érdekében.</td></tr>
<tr><td>fél-formális</td><td colspan="2" rowspan="2">(Értelmetlen)</td><td>2. szint
Formális specifikációs nyelv alkalmazása, automatizált eszközökkel támogatva.</td></tr>
<tr><td>formális</td><td>3. szint
Teljesen formális specifikációs nyelv alkalmazása szigorú szemantikával, formális bizonyító módszerekkel.</td></tr>
</table>

Az informális, fél-formális és formális notáció jellemzőit a 3. táblázatban foglalhatjuk össze.

3. táblázat. Az informális, a fél-formális és a formális notációk jellemzői [Ehr99]

	Informális notáció	**Fél-formális notáció**	**Formális notáció**
Szintakszis	intuitív	formális	formális
Szemantika	intuitív	intuitív	formális
Értelmezhetőség	könnyű	jó	nehéz
Félreérthetőség	nagyon félreérhető	könnyen félreérthető	nem félreérthető
Precizitás	kicsi	közepes	nagy

Meg kell jegyezni, hogy a szigorúbb formalizálás nem feltétlenül jelent egyúttal magasabb rendű minőséget is a szigorúság alacsonyabb szintjéhez képest. A legmagasabb szintű formalizálás adott esetben nem jelenti egyúttal a leginkább adekvát és produktív választást is. Ha például a formális módszereket csak dokumentálási eszközként használjuk, kielégítő lehet az 1. szint is. Ha egy olyan rutin feladatról van szó, amely a hagyományos folyamatok és módszerek révén megfelelően szabályozott, a formális módszerek alkalmazása maradhat akár a 0. szinten is. Ezzel szemben egy új fejlesztésű, kritikus komponens számára a legjobb választás valószínűleg a 3. szint [NASA97].

A tapasztalatok szerint kapcsolat van a formalizálás szigorúsági szintje és a generált modellméret között. A szigorúbb matematikai módszerek általában nagyobb modellméretet generálnak, mint a kevésbé szigorú specifikációs, modellezési nyelvek [Ság01a].

A formális módszerek szigorúságának fokával kapcsolatos jellemző a specifikációs nyelv *absztrakciós szintje*. [Bow94b] szerint minél magasabb egy formális nyelv absztrakciós szintje, annál egyszerűbb, elegánsabb specifikációk készíthetők vele, ugyanakkor annál alkalmatlanabb a matematikai következtetések végrehajtására. A magasabb absztrakciós szintű nyelvek közé tartoznak a valamilyen szakterület speciális igényeit figyelembe vevő nyelvek, az alacsony absztrakciós szintű nyelvek pedig a tisztán matematikai, nem specializált formalizmusok.

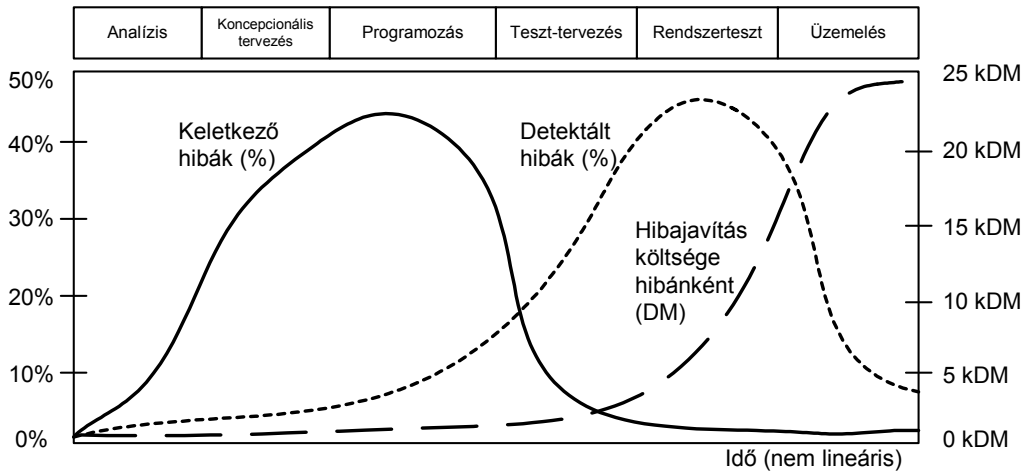
3.2. A formalizálás terjedelme

A formális módszerek alkalmazási terjedelmének vizsgálata során a következő tényezőket érdemes figyelembe venni:

1. fejlesztési fázisok [NASA95],
2. rendszerösszetevők [NASA95],
3. rendszerfunkcionalitás [NASA95],
4. a formalizáció által érintett személyek köre [Ság01b].

3.2.1. Fejlesztési fázisok

A formális módszerek alkalmazhatók a rendszer teljes életciklusában, vagy csak az életciklus meghatározott fázisában, illetve fázisaiban [NASA95]. A formális módszerek alkalmazása akkor kínálja a legnagyobb előnyöket, ha az alkalmazásra már a korai fejlesztési fázisokban sor kerül. Mivel a hibák eltávolításának költsége jelentősen növekszik a projekt előrehaladásával, a hibák korai feltárásával az életciklus költségek jelentősen csökkenthetők (17. ábra) [Pat01].



17. ábra. Hibák és költségek a rendszertervezés egyes fázisaiban [Pat01]

A korai fázisokban való alkalmazás további előnye a precizitás növekedése, ami kifejezetten kívánatos, azonban a hagyományos módszerek révén nem biztosítható [NASA97].

A formális specifikáció önmagában való alkalmazása is (formális fejlesztés vagy bizonyítás nélkül), számos esetben nagyon hasznosnak bizonyult a gyakorlatban. Természetesen kívánatos lenne, hogy a formális technikákkal ne csak a specifikációs fázist, hanem a további fejlesztési fázisokat is, egészen az implementációig lefedjük [Anf99].

A formális specifikáció megléte lehetőséget nyújt ahhoz is, hogy amikor később több tapasztalat halmozódott fel a formális módszerekkel kapcsolatosan, akkor a *fejlesztés folyamatát* is formalizálni lehet, hiszen kiindulásként rendelkezésre áll a formális specifikáció [Bow93b].

Az utóbbi időben sok olyan kutatási projektet hajtottak végre, amelynek célja egy-egy már meglévő rendszer *utólagos formális specifikációja és elemzése* volt. Ezek közül számos talált a vizsgált rendszerben hibát, vagy hibákat, melyek a használat során sem feltétlenül kerültek napvilágra. A tapasztalatok szerint, ezek többsége nem rögzített feltételezésekre, inkonzisztenciákra és szándékolatlan nem-teljességre volt visszavezethető [Win90]. [Cra93] 1993-ban készült tanulmányában például azt állapítja meg, hogy a formális módszerek elsődleges alkalmazási területe a már meglévő rendszerek formális módszerekkel való utólagos támogatása. Példaként lehet említeni az IBM több mint 30 éves CICS rendszerét. Az IBM újraspecifikálja a rendszert Z specifikációs nyelvet alkalmazva azért, hogy a rendszer karbantartását megkönnyítse [Nix88].

Végül meg kell jegyezni, hogy az egyes fejlesztési fázisokban való alkalmazást azonban nem elkülönülő egyedi tevékenységekként kell végrehajtani, hanem egységes módszernek kell tekinteni.

3.2.2. Rendszerösszetevők

A formális módszerek alkalmazása felölelheti egy rendszer egészét, vagy csak meghatározott részrendszereket, komponenseket. Egy komplex rendszer részei a biztonság szempontjából különböző mértékben kritikusak, és a rendszer funkcionalitása szempontjából is különböző jelentőségűek. Ezért célszerűnek látszik a formális technikák alkalmazásának *rendszerrészek szerinti bontása* [NASA95, NASA97]. Egy lehetőség például a különböző mértékben kritikus részek számára különböző szigorúsági szintek választása [Ság00a].

A formális módszerek előnyösen alkalmazhatók mind hardverek, mind szoftverek fejlesztésében. A HOL tételbizonyító eredeti célja például a Viper mikroprocesszor részeinek verifikációja volt. Más tételbizonyító rendszereket is alkalmaztak hardver-verifikációra. Ide tartozik például: Boyer-Moore, Esterel, Nuprl, 2OBJ, Veritas. A modellellenőrzés szintén jelentős a hardverek tervezése esetén, feltéve, hogy az állapottér megfelelően kicsi a kezelhetőséghez.

Jelenleg a specifikáció leginkább a rendszer egyedi tulajdonságainak megfogására képes, és egyes szakterületeken intenzív kutatások folynak annak érdekében, hogy a formális módszerek alkalmazásának hatókörét a rendszer tulajdonságainak egészére kiterjesszék [Pat01].

Az egyik lényeges ilyen megközelítés a *hardware compilation*. Ez az eljárás lehetővé teszi, hogy magas szintű programokat közvetlenül egyszerű alkatrészek (kapuk, latchek) listájára *(net-list)* fordítsunk. Az FPGA (Field Programmable Gate Arrays) technológia lehetővé teszi ennek a folyamatnak a teljesen szoftveres végrehajtását, mivel ezek az áramkörök a chipben lévő statikus áramkör tartalmának megfelelően konfigurálhatók. A fordítás folyamata maga formálisan igazolható, így nem kell minden esetben a „lefordított" hardvert vizsgálni. A jövőben az ilyen eljárások lehetővé tehetik a bizonyíthatóan helyes *hardver-szoftver együttes tervezést* (co-design) [Bow94b].

3.2.3. Rendszerfunkcionalitás

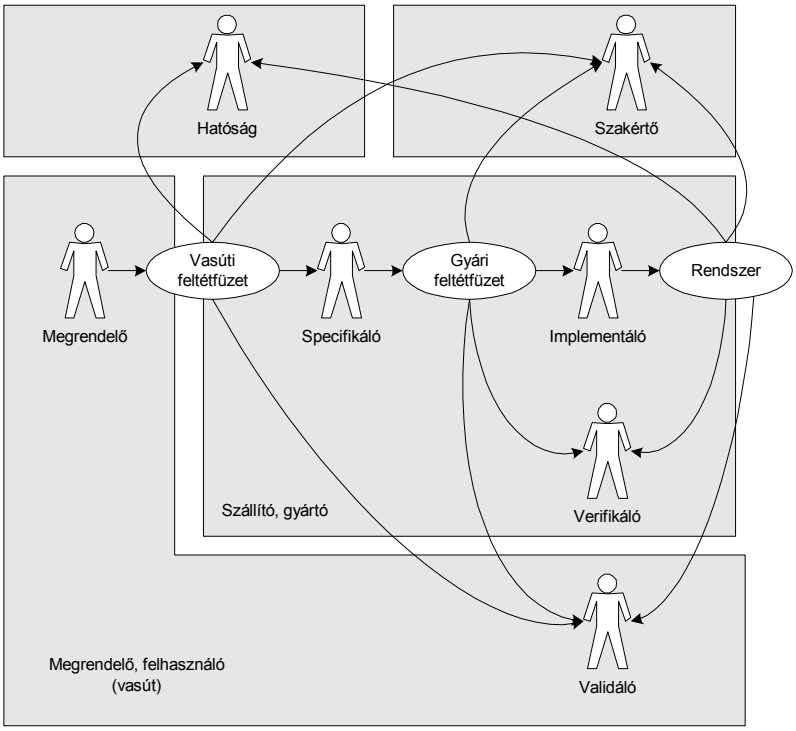
A formális módszerek hagyományosan a „helyesség bizonyításá"-hoz kapcsolódnak, vagyis azért alkalmazzák őket, hogy be lehessen bizonyítani, hogy egy rendszer a vele szemben támasztott követelményeket kielégíti. A formális módszerek azonban egy meghatározott, fontos rendszertulajdonság vizsgálatára, vagy egy negatív rendszertulajdonság vagy hiba hiányának a bizonyítására is alkalmasak [NASA95, NASA97]. Biztonságkritikus rendszerek esetében ez még fontosabb is lehet, mint a pozitív tulajdonságok bizonyítása. [Tho95] a formális módszerek egyik legfontosabb lehetőségét szintén abban látja, hogy a formális specifikáció elemzése lehetőséget nyújt a szigorú, formális *cáfolásra*.

3.2.4. A formalizálás során érintett személyek köre

A formális módszerek alkalmazóinak egy része kézzelfogható terméket készít a formális módszerek segítségével: formális specifikációt. Többen is vannak azonban, akik csak olvasni akarják a specifikációt, nem pedig saját maguk elkészíteni. A specifikáció készítőjén kívül tehát sok *specifikáció-olvasó* is van [Ság02a] (18. ábra).

Minden résztvevő, aki az ábrán szerepel, potenciális olvasója lehet a specifikációnak. A gyakorlatban egy-egy személy több szereplőként is működhet, bizonyos szereplők pedig elmaradhatnak.

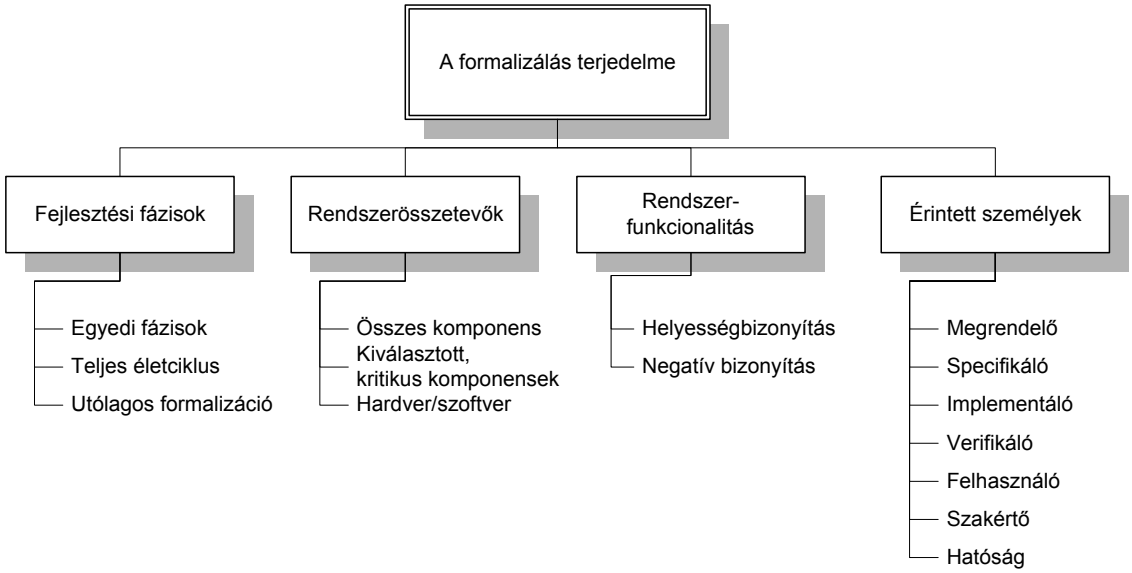
A *specifikálók* írják, értékelik, elemzik és finomítják a specifikációkat. A finomítás közben bizonyítják, hogy a lényeges tulajdonságok a finomítás során megőrződnek, és bizonyítják a specifikandus bizonyos tulajdonságait a specifikáció segítségével. A specifikáció olvasói közé tartoznak – a specifikálón kívül – a *megrendelők*, azok az emberek, akik megbízták a specifikálót, az *implementálók*, akik realizálják a specifikációt, a *felhasználók*, akik használni kívánják a rendszert, és a *verifikálók*, akik az implementáció helyességét bizonyítják. Ezek a csoportok mind előnyösen alkalmazhatják a számítógépes segédeszközöket [Ság00c]. (Tulajdonképpen a számítógépes eszközök is egyfajta specifikáció-olvasónak tekinthetők.)



18. ábra. A specifikáció alkalmazói ([Ság02a] alapján)

A formális módszerek egyik neuralgikus pontja éppen az, hogy egy-egy specifikációs nyelv bizonyos alkalmazói csoportoknak kedvezőbb, mint másoknak [Win90]. A specifikációs nyelvek készítői igyekeznek mindig legalább két csoportot megcélozni. Például a felhasználót és a specifikálót, vagy a specifikálót és az implementálót. Némelyik specifikációs nyelv nagy adag szintaktikai „cukormázat” tartalmaz, hogy a specifikáció jobban olvasható legyen a megrendelő számára.

A formális módszerek terjedelméhez kapcsolódó szempontokat foglalja össze a 19. ábra.



19. ábra. A formalizálás terjedelme

3.3. Megjegyzések a szigorúsághoz és a terjedelemhez

A formalizálás szigorúságát és terjedelmét nem minden irodalom tekinti önálló dimenzióknak. [Bow93a] például kombinálja a formalizáció szigorúságát és alkalmazási terjedelmének néhány aspektusát, így három *alkalmazási szintet* határoz meg:

- Alapszintnek a formális módszereknek kizárólag a *specifikáció szintjén* történő alkalmazása tekinthető. Bár az ezt követő fejlesztési folyamat nem formális, de itt is megmutatkozik a formális módszerek alkalmazásának előnye, mivel már a specifikáció fázisában sok hibát, inkonzisztenciát lehet kiszűrni. A rendszer formális modelljének vizsgálatával bizonyos rendszertulajdonságokra vonatkozó következtetések vonhatók le. Az ilyen formális specifikáció a fejlesztőgárdát is segíti a rendszer megértésében. E célra gyakran alkalmazzák a Z notációt [Spi92].
- A következő szint a formális módszerek alkalmazásának kiterjesztése a *fejlesztési folyamatra*, aminek során bizonyos szabályrendszer szerint a specifikáció lépésenként lebontható, illetve finomítható, egészen végrehajtható programmá. Erre példa a VDM [Jon90].
- A legszigorúbb alkalmazási szinten a teljes fejlesztési folyamat mechanizálható, illetve automatizálható. A folyamat *automatizált* (számítógéppel támogatott) végrehajtása csökkenti az emberi hibák lehetőségét. A mechanizált tételbizonyító módszereknek, mint a HOL [Gor88], vagy a Boyer–Moore [Boy88] jelentős implementációi vannak, de használatukhoz olyan szaktudás szükséges, amellyel ma csak nagyon kevés mérnök rendelkezik.

[Hal90] a „szigorúság” fogalmát a formális *fejlesztés módjának* jelölésére használja. Egy formális specifikációból kiindulva a fejlesztés folyamata lehet szigorúan formális, amennyiben a lépések mindegyike formálisan van kifejezve és bizonyítva. A fejlesztés történhet kevésbé szigorú módszerekkel is; ilyenkor a lépések nagyobbak, az igazolás pedig informális. A szigorúság foka tetszőlegesen választható meg az adott alkalmazás igényeinek megfelelően. Kritikus rendszerek esetén természetesen a szigorú, formális fejlesztési folyamat tűnik ésszerűnek.

3.4. Műszaki jellegű alkalmazási szempontok

3.4.1. Az alkalmazás jellege

A formális módszerek nem egyformán adekvátak a különböző jellegű alkalmazások esetén [NASA97]. Elvileg ugyan szinte minden alkalmazásnál bevethetők a formális módszerek, a gyakorlat azonban azt mutatja, hogy a formális módszerek által nyerhető előnyök alkalmazásonként és egy alkalmazáson belül is alrendszerenként különbözőek. Az összetettebb alkalmazások többet nyerhetnek a formális módszerekkel, mint az egyszerűbbek, hiszen az egyszerűbb problémák kevésbé szigorú módszerek alkalmazásával is kiválóan megoldhatók. Különösen jól alkalmazhatók a formális módszerek az olyan területeken, ahol az *alkalmazás bonyolultsága* nem a méretből és a struktúrából ered, hanem a bonyolult belső algoritmusokból, mint ahogyan a hibatűrő, párhuzamos vagy elosztott rendszerek esetében. Szintén az alkalmazás jellegét befolyásolja az alkalmazás matematikai bázisa. A numerikus feldolgozáson alapuló alkalmazások, különösen a lebegőpontos alkalmazások esetén a

formális módszerek viszonylag keveset nyújthatnak. Ugyanakkor a logikai és diszkrét matematikai rendszerekre a formális módszerek előnyösen alkalmazhatók [NASA95].

Egy másik, a formalizálás szempontjából fontos strukturális tulajdonság az ún. *strukturális entrópia* (rendezetlenség). Ha egy rendszernek nagy a belső entrópiája, azaz elsősorban egyes esetek véletlenszerű gyűjteményéből áll, egymás között kevés koherenciával, akkor a formalizálástól nem sok várható. Megfordítva, ha egy alkalmazás erős összetartó strukturális jellemzőket mutat, amelyek jól kifejezhetők logikailag, akkor ez a struktúra hatásosan kifejezhető a formális módszerek segítségével [NASA95].

A formális módszerek alkalmazása kifejezetten ellenjavallt bizonyos inherens rendszertulajdonságok esetén, mint például az időzítési megszorítások. A formális módszerek alkalmazása nem célravezető továbbá idő vagy eszközök hiányában; és az alkalmazás valószínűleg nem lesz költség-hatékony kiérlelt technika hiányában sem [Tho95].

Figyelembe kell továbbá venni, hogy az egyes formális módszerek nem egyformán alkalmasak a különböző alkalmazási szakterületek számára. Például egy adott módszer megfelelő szekvenciális programok leírására, de nem alkalmas párhuzamos működések leírására. Az *alkalmazási terület* pontos ismerete nélkül fennáll a veszélye annak, hogy az alkalmazó nem megfelelő módszert választ [Win90].

3.4.2. Az alkalmazás mérete

Az alkalmazás mérete a formalizálás költségei és bonyolultsága szempontjából az egyik legfontosabb tényező.

A kezdeti időkben a rendelkezésre álló technikák alapvetően olyan kisméretű problémákra korlátozták az alkalmazást, amelyek méretükben és bonyolultságukban egyaránt messze alatta maradtak a reális problémaméreteknél felmerülőknek [Pat01].

Jelenleg úgy tűnik, hogy a formális módszerek a *kis, illetve közepes méretű rendszerek*, illetve alrendszerek fejlesztésénél alkalmazhatók. Az ilyen méretű alkalmazási példák között szerepelnek integrált áramkörök, mikroprocesszorok, oszcilloszkópok, operációs rendszer kernelek, elosztott adatbázisok és biztonsági rendszerek.

Nem nagyon alkalmaztak azonban formális módszereket nagy méretű szoftverek vagy hardverek specifikációjában. Ennek a problémának két dimenziója van: a specifikáció mérete és a specifikandus komplexitása. Megfelelő számítógépes támogatás megléte esetén a *specifikáció terjedelmi problémái* kezelhetők: nagyméretű specifikációk kezelése ugyanolyan feladat, mint más nagyméretű dokumentum kezelése. A probléma másik dimenziója, a *specifikandus komplexitása* továbbra is fennáll. A rendszer komplexitása fakadhat a belső komplexitásból és/vagy az interfészek komplexitásából. A formális módszerek által nyújtott, illetve kikényszerített szisztematikus megközelítés segíthet abban, hogy mind a két fajta komplexitásból származó problémákat meg lehessen oldani [Win90].

Az alkalmazás méretének korlátai megkerülhetőek oly módon, hogy a formalizálás kiterjedését a kritikus funkciókra, illetve rendszerkomponensekre szűkítjük [NASA95]. Ehhez természetesen az szükséges, hogy a *rendszer lebontható* (dekomponálható) *legyen* kis, vagy közepes alrendszerekre, illetve komponensekre, megfelelő interfészekkel. Ez a strukturális tulajdonság elengedhetetlen bármely közepes, illetve nagy alkalmazás esetén ahhoz, hogy a különálló formális analízisek eredményei kombinálhatók legyenek, és az alrendszerekre vonatkozó következtetések kombinációjából a teljes rendszerre is érvényes következtetést lehessen levonni [Ság00c, Ság00e].

3.4.3. Eszköztámogatottság

A formális módszerek hatékony alkalmazásához elengedhetetlen a támogató szoftvereszközök megléte [Ság02a]. A formális technikák esetében az eszköztámogatás célja a termelékenység és a pontosság növelése [Bow94b].

A formális módszerek támogatására számos eszköz létezik, az ingyenesen elérhető szoftverektől egészen a legdrágább eszközrendszerekig. A megfelelő támogatóeszköz kiválasztása az egyik legnehezebb dolog a formális módszerekkel kapcsolatban [FME97].

A *biztonsági rendszerek* esetében néhány speciális követelmény is felmerül a támogatóeszközökkel kapcsolatban. A formalizmusok és az alkalmazások sokfélesége miatt számos felhasználó és potenciális felhasználó úgy érzi, hogy a jelenlegi eszközök túlságosan általános célúak. A biztonság-orientált piac azonban túl kicsi ahhoz, hogy azt lehessen várni, hogy erre a területre specifikus eszközök is kifejlesztésre kerülnek. A biztonság-kritikus rendszereket szállító cégek egy része úgy próbál ezen a problémán úrrá lenni, hogy a szükséges támogatóeszközöket maguk fejlesztik ki, figyelembe véve az adott szakterület speciális igényeit (például [Red99]) [Ság00e].

A biztonsági rendszereknél az eszköztámogatottság további kérdései a *folyamatosság* és a *karbantartás*. Ezek a biztonsági rendszerek hosszú élettartamával függenek össze. Egy olyan szállító cég, amelyik egy olyan rendszert fejleszt, amelynek legalább 10 évig működnie kell, azt igényli, hogy a fejlesztésben felhasznált fejlesztőeszközök támogatottsága ebben az időszakban szintén elérhető legyen, hogy a szállított rendszer karbantartását, módosítását vagy továbbfejlesztését el lehessen végezni. A formális módszerek eszköztámogatása és az eszközök karbantartása rendkívül költséges, és az eszközök szállítóinak hosszútávon való elérhetősége bizonytalan. A formális módszerek piaca túl kicsi ahhoz, hogy ennek a problémának a megoldását a piaci erőkre bízhatnánk, ezért ebben a tekintetben kormányzati támogatás szükséges [Tho95].

Többek közt ezek a problémák adhatnak magyarázatot [Cra93] 1993-ban végzett felmérésének tapasztalatára, mely szerint az eszköztámogatottság sem szükséges, sem pedig elégséges feltétele a formális módszerek sikeres alkalmazásának. Az általa vizsgált formális módszeres projektek esetében a *támogatóeszközök hiánya* egyetlen esetben sem riasztotta el az alkalmazókat egy bizonyos módszer alkalmazásától (az eszközöket inkább saját maguk fejlesztették ki, vagy adaptálták azokat); de a megfelelő eszköztámogatottság megléte sem volt elégséges érv egy adott módszer kiválasztása mellett. Ezen tapasztalat alapján [Cra93] úgy véli, hogy a formális módszerek széleskörű ipari elterjedéséhez a támogatóeszközök tekintetében robosztus verziókra van szükség, nem pedig kutatási prototípusokra.

Jelenleg az alapvető számítógépes támogatóeszközök széles körben elérhetők a formális módszerekhez. A jövőben az várható, hogy nagyobb hangsúlyt fognak fektetni az ún. IFDSE (*Integrated Formal Development Support Environment*) rendszerekre. Az ilyen integrált formális fejlesztést támogató környezetek a formális fejlesztés minden fázisát támogatni tudják [Bow94b].

3.5. Adminisztratív jellegű alkalmazási szempontok

3.5.1. Szakmai összetétel

A formális módszerek eredményes alkalmazása egy adott projektben a személyzet megfelelő szakmai összetételét feltételezi: szükség van olyan szakemberekre, akik megfelelő képzettséggel rendelkeznek a formális módszerek területén, de legalábbis járatosak a kapcsolódó matematikai területeken, és kellenek olyan emberek, akik ismerik az adott

alkalmazási területet [FME97]. A formális módszerek ismerete biztosíthatja a megfelelő módszer alkalmazását és a hatékony eszköz kiválasztását. Az alkalmazási terület ismerete szükséges ahhoz, hogy a formális módszereket az adott terület problémáinak megoldására alkalmazzák. E két szakterület együttműködésével lehet megválaszolni azokat a kérdéseket, amelyek a formalizálás során elkerülhetetlenül felmerülnek az eszközökkel, a stratégiával, illetve módszerrel, valamint az alkalmazási területtel kapcsolatosan [NASA95].

3.5.2. Képzés, képzettség

A formális módszerek széleskörű elterjedését számos irodalom szerint (például [Bow93a, Pat01]) a módszerek kezeléséhez szükséges matematikai ismeretek hiánya akadályozza. A formális módszerek különböző jellegű alkalmazásai nem egyforma matematikai képzettséget igényelnek.

[Hal90] szerint kifejezetten a *formális specifikációhoz* alkalmazott matematika nem bonyolult. Szerinte a specifikáció elkészítése olyan, egyszerű matematikát igényel, amelyet minden gyakorló mérnöknek ismernie kell. Például Z specifikációk elkészítéséhez a matematikából mindössze halmazelméleti és logikai ismeretekre van szükség. Természetesen a gyakorlati alkalmazáshoz a mérnököknek megfelelően képzetteknek kell lenniük, de ez bármilyen más módszerre is igaz. A formális specifikáció írásához szükséges ismeretek elsajátítására [Hal90] háromszintű képzést javasol.

1. Képzés a diszkrét matematika területén, amely az elemi halmazelméletet és a formális logikát fedi le. Azokat, akik rendelkeznek matematikai háttérrel, és csak ezek a témák ismeretlenek számukra, egyetlen nap alatt be lehet vezetni ebbe a témába. A diszkrét matematikához számos kiváló tankönyv létezik.
2. Képzés az adott formális notációban. Például egy Z vagy VDM kurzus rendszerint 1-2 hetet vesz igénybe, feltételezve, hogy a résztvevők már rendelkeznek a matematikai alapokkal. Tankönyvek szintén elérhetők.
3. Konzultációs lehetőség valódi projektekben. A képzés után a hallgatók tudják majd használni a formális módszereket, de számos gyakorlati nehézségbe fognak ütközni. Ezeket célszerű workshopok formájában megvitatni és megoldani, és ilyenkor egy tapasztalt konzulens segítsége sokat jelent. Fontos, hogy a valódi projektek esetében is lehetőleg legyen mindig valaki, aki nagy tapasztalattal rendelkezik a formális módszerek alkalmazásának területén.

[Lar96] arról számol be, hogy egy formális módszereket alkalmazó projektben a mérnökök egy hét képzés után használni tudták a formális technikát, bár a fejlesztés során folyamatosan szükség volt a formális módszerek szakértőjével való konzultációra.

[Hal90] tapasztalatai szerint a formális specifikáció készítéséhez szükséges képzés nem bonyolult és főiskolai matematikai ismeretekkel rendelkezők is kiváló formális specifikációkat írtak. Bárki, aki meg tud tanulni egy programozási nyelvet, képes arra, hogy egy olyan specifikációs nyelvet is megtanuljon, mint amilyen a Z. Egy probléma specifikálása formális nyelven sokkal rövidebb és az elkészült specifikációt könnyebb megérteni, mint ugyanazt a problémát egy programozási nyelven megoldani.

A formális specifikációhoz képest jóval komolyabb matematikai bázist igényel a *formális fejlesztési folyamat*, illetve a *formális bizonyítás*. Nem tűnik reálisnak, hogy a szoftvermérnökök többsége a jövőben könnyedén képes lesz formális bizonyításokat elvégezni. [Hal90] szerint a számítógépes támogatás javulása sem hoz ebben jelentős változást. Ezért a formális fejlesztést, illetve formális bizonyítást is alkalmazó, például biztonságkritikus projekteknél elengedhetetlennek tűnik a matematikai eljárásokat

végrehajtani képes, kompetens szakemberek igénybevétele. Egy másik lehetséges irány a matematika „elrejtése” a felhasználó elől (lásd 6.1. fejezet).

3.5.3. Bevezető esettanulmány

Amennyiben a formális módszereket először alkalmazzák egy projektben, tanácsos lehet egy bevezető esettanulmány kidolgozása, adott esetben a projekt egy leszűkített részére [NASA95]. Ez a tanulmány alkalmas lehet

- gyakorlatszerzésre,
- annak eldöntésére, hogy a fejlesztendő rendszer mely részeire érdemes leginkább alkalmazni a formális módszereket,
- annak eldöntésére, hogy melyik formális módszer a legmegfelelőbb az adott projekthez, valamint
- az adott projekt formális módszerekkel történő megvalósíthatóságának igazolására.

Fontos, hogy azokat az ötleteket, irányokat is rögzítsék az esettanulmány során, amelyek nem vezettek eredményre, vagy valamilyen okból elutasították őket. Ezek a „zsákutcák”, az elutasítások, illetve az eredménytelenségek okával együtt rögzítve, sok segítséget nyújthatnak jövőbeli projektek esetében, amennyiben segítenek elkerülni hasonló hibák megismétlését [Hal90].

3.5.4. A fejlesztési folyamatba való integrálás

A formális módszereknek a meglévő fejlesztési folyamatba való integrálása nem jelent problémát, ha a fejlesztési folyamat fázisai pontosan vannak definiálva, és már léteznek azok a tevékenységek, amelyek helyére a formális módszerek segítségével végrehajtott tevékenységek kerülnek. Például a hagyományos (vagy fél-formális) specifikáció könnyen helyettesíthető a formális specifikációval [NASA95]. A formális módszerek bevezetéséhez feltétlenül szükséges, hogy az adott szervezet megfelelően jól definiált fejlesztési elképzelésekkel, fejlesztési előírásokkal, illetve belső szabványokkal rendelkezzen. Ezek hiányában a formális módszerek alkalmazásától jelentős minőségbeli javulás nem várható [FME97].

Amennyiben a fejlesztési folyamat új, vagy nem jól szervezett, akkor a formális módszerek integrálását meg kell előznie a folyamat pontos megtervezésének. Egy bevezető esettanulmány ez alól kivételt jelenthet, mert ilyenkor a folyamat megtervezése, illetve leírása gyakran az esettanulmányt követi, hiszen az esettanulmány egyik célja éppen az, hogy meg lehessen határozni az optimális fejlesztési folyamatot [NASA95].

3.5.5. Projekt irányelvek

Egy formális specifikáció elkészítése hasonló egy program megírásához valamilyen hagyományos programnyelven. Ezért a hagyományos szoftverfejlesztés során alkalmazott megfontolások, irányelvek (például konfiguráció-menedzsment, nyelvi kötöttségek, újrafelhasználható modulok) a formális specifikációk készítésére is vonatkoznak. Mint ahogyan a hagyományos szoftverfejlesztés területén, a formális módszerek esetében is akkor a

leghatékonyabb a folyamat, ha ezeket a projektre vonatkozó irányelveket a projekt megkezdése előtt rögzítik [NAS95].

3.6. Költségek, korlátok, nehézségek

3.6.1. A formális módszerek és a költségek

A formális módszerekkel kapcsolatos költségek nagymértékben függenek az alkalmazás módjától. Ebben a fejezetben megvizsgáljuk, hogy hogyan alakulnak egy adott projekt költségei a formális módszerek alkalmazása esetén. E tekintetben meg kell különböztetni a *formális specifikáció* alkalmazását, formális fejlesztés és bizonyítás nélkül, illetve azt az esetet, amikor a formális módszereket *formális fejlesztésre,* és/vagy *formális bizonyításra* is használjuk [Ság00e].

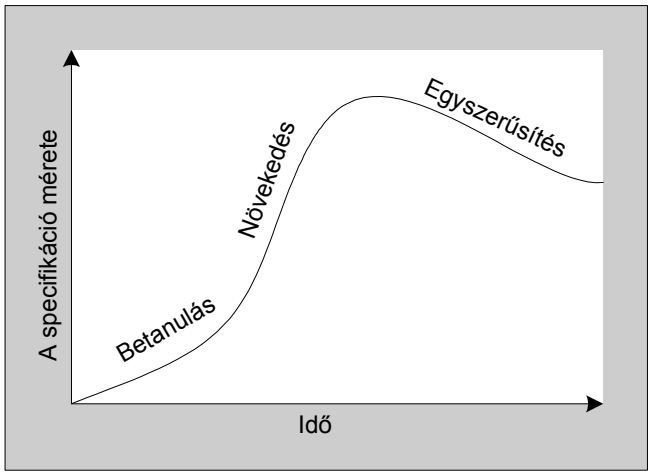
Közismert, hogy mennyire komplikált különböző módszerekkel fejlesztett rendszerek fejlesztési költségeinek összehasonlítása. Kevés összehasonlító adat áll rendelkezésre egy-egy szoftver, vagy szoftverrész formális és informális fejlesztési költségeiről. Szerencsére azonban gyűlik azon projektek száma, ahol formális specifikációt használtak. Ezen tapasztalatok egyike sem mutatja azt, hogy a fejlesztési költségek növekedtek volna, sőt, az ellenkezőjét tapasztalták. A hagyományos specifikációnak formális specifikációval történő helyettesítése a költségek megtakarítását eredményezheti egy projektben [Hal90]. Más források [NASA95, Lar96] szintén úgy értékelik, hogy a különböző kísérleti projektek szerint a *specifikációk* formalizálása általában véve költség-hatékony. Ezekhez az adatokhoz azonban mindenképpen hozzá kell számítani a formális módszerekkel kapcsolatos képzés egyszeri, de nem elhanyagolható költségét.

A formális specifikáció alkalmazása egy adott projektben tehát nem jár feltétlenül a költségek növekedésével, azonban megváltoztatja a projekt formáját [Hal90]. Formális specifikáció esetén a *specifikációs fázis ráfordításigénye növekszik*. Ennek az az oka, hogy egy formális specifikáció több információt hordoz, mint egy hagyományos specifikáció; a munkáknak nagyobb részét végzik el a specifikáció fázisában. Cserébe viszont az implementáció, az integráció és a tesztelés fázisai rövidebbek lesznek [Hal90].

Azt mondhatjuk tehát, hogy a formális specifikáció ugyan nagyobb ráfordítást igényel, mint egy hagyományos specifikáció, azonban specifikáció formalizáltsága olyan előnyökkel jár, amelyek a projekt teljes költségét tekintve megtakarítást eredményeznek [Ság00e].

A specifikációs fázis súlyának megnövekedése a következő problémával is jár: a specifikációs folyamat menedzselése nehezebbé válik, ugyanis nagyon kevéssé látszik a munkák előrehaladása. Ez különösen igaz a specifikálás elején; ilyenkor úgy látszik, hogy semmiféle előrehaladás nem történik, ugyanis rengeteg ötlet merül fel, sokat kipróbálnak, sokat elvetnek, ahogy az lenni szokott. A tapasztalatok szerint a specifikáció méretének növekedésére a 20. ábra grafikonja jellemző [Hal90].

Kezdetben látszólag alig történik valami. Egy idő után azonban az emberek kezdik megérteni a problémát és ekkor *gyors előrehaladás* érhető el. Ezt követően az előrehaladás lassul, majd – ha minden jól megy – az egyszerűsítések hatására a specifikáció *mérete csökken*. Ez az a pont, amikor a problémát valóban megértik, amikor felismerik a szabályosságokat, azonosságokat a struktúrában. Ennek hatására lesz a specifikáció *tömörebb* és jobb. Ez az elsimító fázis a végtelenségig tarthat, a jó projektmenedzsernek azonban fel kell ismernie azt a pontot, hogy mikor legyen ennek a folyamatnak vége. Fontos, hogy ne állítsa le a specifikálás folyamatát addig, amíg a specifikáció mérete növekszik, mert akkor a problémát általában még nem dolgozták fel teljes mértékben [Hal90].



20. ábra. A specifikációk méretének növekedése [Hal90]

Bár vannak kivételek, de a legtöbb tapasztalat azt mutatja, hogy a *formális fejlesztés* növeli a költségeket [Bow93b]. Például Andrew Bradley (British Aerospace), a következő összehasonlító táblázatot (4. táblázat) mutatta be a Z felhasználók találkozóján 1992-ben:

4. táblázat. A különböző fejlesztési megközelítések termelékenysége programkódsor (LOC, Lines of Code)/emberévben. (Forrás: [Bow93b])

Nem biztonságkritikus kód	1400-1600 LOC/emberév
Normális biztonságkritikus kód	700-800 LOC/emberév
Teljesen formális fejlesztés	200-400 LOC/emberév

Egy teljesen *formális fejlesztési folyamat* tehát, minden fejlesztési lépés formális igazolásával rendkívül drága – valószínűleg a legkritikusabb alkalmazásokon kívül bármi másra megvalósíthatatlan [Hal90].

Megoldásnak tűnik a formális *bizonyítás körének leszűkítése* a kulcsfontosságú rendszerjellemzőkre és –tulajdonságokra [Ság00e]. Kritikus alkalmazások esetén ezek *formális bizonyítása* költség-hatékonynak tűnik, bár erről kevés tényleges adat áll rendelkezésre, részben azért, mert a rendszerfejlesztési módszerek elemzésére a statisztikai módszerek nagyon nehezen alkalmazhatók [NASA95]. [Bow93b] szerint is a kulcsfontosságú részekre, tulajdonságokra szűkített formális bizonyítás a projekt összköltségeit tekintve megtakarításokat eredményezhet.

A formális módszerekkel kapcsolatos költségek egyik fontos aspektusa a *fejlesztési idő*. Jónéhány formális módszerekkel folyó projekt szenvedett látványos késedelmet. Az a feltevés azonban, hogy ez a formális módszerek inherens jellemzője, teljességgel irracionális következtetés. A csúszott projektek nem maguk a formális módszerek alkalmazása, illetve a formális módszerekkel foglalkozók képzetlensége miatt, hanem a módszerekkel kapcsolatos tapasztalatok hiánya miatt csúsztak. Valójában a fejlesztéshez szükséges időt becsülték jelentősen alá [Bow94b].

Természetesen vannak projektek, amelyek során a fejlesztési idő jelentősen csökkenthető volt a formális módszerek alkalmazása által. Ide tartozik az Inmos T800 lebegőpontos chip fejlesztése, ahol 12 hónapot takarítottak meg, vagy az IBM CICS rendszere, ahol Z, illetve B formális módszert alkalmaztak. Mindkét projektet független szakértők kísérték figyelemmel, az elért idő-megtakarításról szóló adatok tehát hitelt érdemlőek [Bow94b].

A *projektköltségek*, illetve a projektek időtartamának becslése okozzák a fejlesztő csapatok számára a legnagyobb fejtörést. Számos, több tényezőt figyelembe vevő modellt dolgoztak ki ezek becslésére. A legfontosabb azonban a legtöbb modell esetében a tapasztalatokra való támaszkodás. Hosszú időre visszanyúló tapasztalatok azonban még a formális módszereknél hagyományosabb fejlesztési módszerek esetén sem állnak mindig rendelkezésre. A formális módszereket ugyanakkor még nem alkalmazták elegendően sok projektben ahhoz, hogy azokból megbízható tapasztalatokat lehessen levonni a projektek időbeliségét tekintve [Ság00e].

Az értékelést az is megnehezíti, hogy nincs olyan általánosan elfogadott költség-modell, amelynek segítségével a jelenlegi projektek értékelhetők lennének, és jövőbeli projektekre vonatkozóan becsléseket lehetne tenni a költségeket illetően. Néhány szervezet házon belül alkalmaz költségmodelleket, ezek egymással való összehasonlítása azonban lehetetlen, és így széleskörű tapasztalat sem gyűjthető [Cra93].

Számos formális módszerekkel kapcsolatos felmérés (például [Cra93]) célja éppen ilyen és más tapasztalatok összegyűjtése.

A tapasztalatok begyűjtését nehezíti, hogy számos esetben a formális módszereket egy-egy nagyon speciális alkalmazási területen használják, az ott szerzett tapasztalatoknak más területekre való átvitele pedig nem megbízható [Ság00e].

Bizonyos specializált piaci szegmensek esetén azonban nem a fejlesztési költségek, illetve a fejlesztési idő a domináns tényező. Ezeket gyakran nyomják el *más faktorok*, mint például a termék minősége, a biztonságkritikus rendszerek esetében.

A biztonság szempontjából (illetve egyéb okból) kritikus rendszerek esetén a megbízhatóság és a biztonság, vagy védettség kiemelkedően fontosak. Ilyen esetekben a formális módszerek alkalmazásával járó többletköltségek elfogadhatóak; még a formális módszerek legszigorúbb fokú alkalmazása (mechanizált formális bizonyítás) is megérheti, legalábbis a különösen kritikus komponensekre alkalmazva [Bow93b].

3.6.2. A formális módszerek korlátai

A formális módszerek célszerű, hatékony alkalmazásához fontos megérteni a formális módszerek lényegi korlátait. Ezek a korlátok a következőkből származnak: vannak dolgok, amiket soha nem lehet bizonyítani, és ugyanakkor azon dolgok bizonyításánál, amelyek bizonyíthatók, a bizonyítás során hibákat követhetünk el [Ság00e].

A bizonyítás annak demonstrációja, hogy egy formális állítás következik egy másikból. A valódi világ azonban nem formális rendszer, ezért a bizonyítás nem tudja igazolni, hogy a valódi világban a dolgok úgy fognak történni, ahogy azt mi várjuk. Ez azonban nem akkora probléma, mint amilyennek látszik. Minden mérnök modelleket készít a valódi világról és a modelleket arra használja, hogy tárgyakat tervezzen. A *matematikai alapú modellek* azért előnyösek, mert a modell tulajdonságait bizonyítani lehet és a modell könnyen kezelhető a tervezés folyamán. Azt azonban nem lehet formális módon bizonyítani, hogy a valódi rendszer úgy fog viselkedni, ahogyan azt a tervező a modell alapján jósolta. Egészében vizsgálva viszont, a strukturált tervezésben használt matematikai modellek valódi világnak való megfelelőségét elég jól ismerjük ahhoz, hogy megbízzunk a matematikai modellekben, ahogyan az is igaz, hogy minél jobban kiérlelt az adott mérnöki diszciplína, annál inkább bízunk abban, aki a modellt használja [Bow94b].

A modellezési technikák korlátai a szoftverek tekintetében is könnyen beláthatók [Hal90]:

a) a modellek a programok viselkedésének csak néhány aspektusát fedik le;

b) a formális leírás és a valódi világ egymásnak való megfelelősége korlátozott.

ad a) A szekvenciális programok modellezésére például jó matematikai eszközök léteznek. A konkurens viselkedés modellezése szintén lehetséges, bár a vonatkozó matematikai eszközök használata nem annyira könnyű. Az időzítési problémák modellezése már nehézségekbe ütközik, legalábbis abban a tekintetben, hogy nem tudjuk, hogyan lehet a modellt felhasználni arra, hogy olyan szoftver szülessen, amely kielégíti a követelményeket [Hal90].

Vannak olyan *nem-funkcionális tulajdonságok,* amelyeket nem lehet modellezni, mint a teljesítmény, működőképesség, karbantarthatóság és rendelkezésreállás. Továbbá léteznek a rendszerfejlesztésnek olyan aspektusai, ahol a formális módszerek nem olyan hatékonyak, mint egyéb megközelítések [Bow94b]. Példaként a felhasználói interfészt lehet említeni: a felhasználói interfésszel kapcsolatos követelmények többségét rendkívül bonyolult formalizálni, gyakran nem is lehet. Egy felhasználói interfész megfelelősége rendkívül szubjektív kérdés, így alkalmatlan formális vizsgálatokhoz. (Meg kell jegyezni, hogy mindezek ellenére vannak sikeres próbálkozások a formális módszereknek a felhasználói interfészek területén történő alkalmazására [Dix91].)

Ezen kívül is számos olyan terület létezik, ahol a formalizálás nem praktikus, erőforrás, idő, vagy pénzügyi szempontok miatt. A legsikeresebb formális módszeres projektek a rendszerek kritikus részeire vonatkoznak. Csak kevés alkalmazás van, ahol a formalizálás a teljes rendszert érinti.

ad b) A formális módszerek a rendszer specifikációnak való megfelelőségét, azaz helyességét segítenek biztosítani. Az említett helyesség azonban nem a történet vége: a helyesség a rendszer két (esetleg több) modelljének (a követelmények modellje és az implementált rendszer modellje) ekvivalenciáját jelenti, amely modelleknek az eredeti követelményekkel, illetve a megvalósított rendszerrel való kapcsolata nehezen ellenőrizhető. Hogy a rendszer valóban jól működik-e, az egy sor egyéb olyan tényezőtől is függ, mint a kommunikáció, a képzettség, a mechanikai, elektronikai vagy kémiai komponensek viselkedése, teljesítménye mind a rendszeren belül, mind annak környezetében [Bow93a].

Szoftverek esetében a formális modell és a valódi rendszer működésének kapcsolatát három tényező korlátozza: a programozási nyelv viselkedése, az operációs rendszer és a működtető hardver. Biztonságkritikus rendszerek esetében ezek a korlátok életbevágóan fontosak [Hal90].

A formális módszerek korlátai között feltétlenül meg kell említeni, hogy mind a formalizálás során, mind a formális bizonyítás során előfordulhatnak emberi hibák, bár a tapasztalatok szerint ezek előfordulási gyakorisága kisebb, mint más fejlesztési eljárások esetén. Ennek az az oka, hogy a formális módszerek alkalmazása során sokkal könnyebb észrevenni a hibákat, mint más módszerek esetén [Hal90].

A formális módszerek fent ismertetett korlátai alapján a következő alkalmazási irányelveket határozhatjuk meg:

- a formális módszerek csak egyfajta technikát jelentenek a sokféle klasszikus technika mellett, amelyek továbbra is alkalmazhatók, sőt alkalmazandók a biztonság-orientált rendszerek fejlesztése során [Bow93a];
- a formális módszerek eszközök a cél elérésére, de nem a formális módszerek alkalmazása a cél [Tho95].

3.6.3. A formális módszerek bevezetésének nehézségei

Az ipar érthetően óvatos a formális módszerek bevezetésével. Bármilyen új technológia, módszer vagy eljárás első alkalommal történő kipróbálásakor az esetleges kudarc ára sokszor megfizethetetlen, és a kezdeti képzés költségei is rendkívül magasak. Ez utóbbi különösen igaz a formális módszerekre, ugyanis jelenleg kevés olyan mérnök, programozó és menedzser dolgozik az iparban, aki rendelkezik a formális módszerek alkalmazásához szükséges ismeretekkel [Ság00e].

A matematikai módszerek alkalmazásának az informatikán belül mindmáig alapvető korlátai vannak. Ezek a következők [Pat01]:

- A feladatok *valósághű modellezése* irreálisan nagy modellméreteket von maga után. Abban az esetben például, ha egy működtető programot a maga teljességében kívánnánk modellezni, a problématér kezelése annyi bitnyi állapotváltozó manipulációját igényelné, mint amekkora a program teljes adatterülete.
- Az *idődimenzió* kezelése folytonossága miatt kritikus. Mindmáig nem sikerült olyan, a gyakorlatban is hatékony, egységes tárgyalás- és analízismódszert találni, amely egyidejűleg képes lenne tetszőleges összetételű diszkrét és folyamatos rendszermodellek kezelésére.
- Lényeges és nyitott probléma az is, hogy egy informatikai rendszer logikai konstrukciójának helyessége még messzemenően nem garantálja a *szolgáltatások helyességét*, hiszen ahhoz modellezni kellene a rendszer *futtatási környezetét* is, beleértve a *hardver erőforrásokat* is.
- A matematikai helyességbizonyítási módszerek alkalmazásának nehézsége, hogy egy-egy részletkérdés megválaszolásához ma még egyelőre *a matematikának elkülönült fejezetei* szolgálnak. Ezek mindegyike speciális, erősen absztrakt, elméleti szemléletmódot kíván. Ez a formális módszerek alkalmazását beszorítja azon kiemelten kritikus alkalmazási körbe, ahol mind a fejlesztési ráfordítások, mind az újramodellezési ráfordítások tolerálhatók, összevetve az esetleges hibás működésből eredő konzekvenciákkal.

Minden bonyolultabb rendszer fejlesztője tapasztalja a rendszerkövetelmények és a rendszerspecifikáció későbbi fázisban való felülvizsgálatának, átdolgozásának szükségességét. Bár a formális módszerek támogatják a hagyományos módszerek tervezési elveit (például top-down módszer, lépésenkénti finomítás), eddig nem áll rendelkezésre olyan, a formális módszereken alapuló fejlesztési modell, amely a teljes rendszerfejlesztési életciklust támogatná. Amíg strukturált fejlesztési módszerek általában jól támogatják a teljes fejlesztési életciklust, az alkalmazott modellek követik a rendszerfejlesztés iteratív jellegét, addig a formális fejlesztési módszerek gyakran nem veszik ezt figyelembe [Bow94b].

Valójában a formális módszerek nem helyettesítik a hagyományos mérnöki tervező módszereket. A folyó és a jövőbeli kutatások egyik célja éppen a *strukturált és a formális módszerek integrációja*. Egy ilyen integráció „igazi" módszerhez vezethet, amely teljes mértékben támogatja a rendszerek életciklusát, miközben megengedi a formális technikák alkalmazását a specifikáció és a tervezés fázisában, valamint támogatja a végrehajtható kóddá való lépésenkénti finomítást és a tulajdonságok bizonyítását is [Bow94b].

A formális módszerek alkalmazásának bizonyos aspektusai az iparban már viszonylag elterjedtek (például formális specifikáció), így elég fejlett eszközök állnak rendelkezésre és ipari eredmények is vannak. Más aspektusok, gyakorlatok (például tételbizonyítás) még kevés hasznot hoztak a „valódi" világban, ezért kevésbé fejlettek. [Bow93a]

Gyakori eset, hogy a formális módszerek alkalmazásának egy adott vállalatnál működő fejlesztési rendszerbe való beillesztése nehézségekbe ütközik. Ennek egyik oka az, hogy a

jelenlegi *rendszerfejlesztés* ráfordítások szerinti *súlypontja* a fejlesztés végső szakaszaiban (tesztelés, hibaeltávolítás) van. A formális módszerek alkalmazása ezt a súlypontot a fejlesztési folyamat elejére tolja, ugyanis a formális technikák a fejlesztés korai szakaszában igényelnek jelentős erőforrásokat (merthogy az eredményeket is ezekben a fázisokban nyújtják). Ebből az is következik, hogy a meglévő menedzselési gyakorlat tökéletesen alkalmatlan lehet a formális fejlesztés korai szakaszainak szervezésére [Bow93a].

A formális módszerek előnyeit, lehetőségeit és korlátait ismerté kell tenni mind a műszaki gárda, mind a menedzsment számára, hogy a költséges hibákat el lehessen kerülni [Bow93b].,

A formális módszerek alkalmazásának bevezetését, széleskörű elterjedését megnehezíti, hogy a *matematikai jelölésrendszer* meglehetősen nehezen érthető és követhető [Pat01, Bow93a, Tho95]. Továbbá az eszközök kezeléséhez és a modellezéshez egyaránt olyan magas szintű felkészültségre van szükség, amely az informatikai iparban dolgozó mérnökök számára eddig nem voltak elérhető [Pat01, Bow93a]. Fontos tehát olyan kommunikációs lehetőség megkeresése, amellyel a formális specifikáció és az analízis eredményei megvitathatók a formális módszerekben nem jártas kollegákkal [Tho95].

Nehézséget jelent a formális módszerek elfogadtatásában, hogy a formális módszerek irodalmát az alapozó tudományos aspektusok taglalása uralja, kevés figyelmet fordítanak az alkalmazási problémákra. Többek között ezért is terjedt el és tartja magát *számos tévhit* a formális módszerekkel kapcsolatosan [Hal90, Bow94b].

A különböző rendszerek fejlesztésében általában *több résztvevő* is érintett: a szállító cég, a fejlesztő és természetesen a megbízó cég vezetése és műszaki szakemberei [Ság00e]. Biztonsági rendszerek esetében a hatóság szerepével is számolni kell. [Mon00] szerint az előbbiek közül minden csoportban vannak emberek, akik:

- „félnek” a matematikától,
- nem értik a módszert magát,
- nem látják tisztán a módszer nyújtotta előnyöket,
- úgy vélik, hogy bár a jelenleg alkalmazott, hagyományos módszerek nem túl jók, de nem is annyira rosszak, hogy lecseréljék azokat.

A szállító cég vezetősége számára gyakran bonyolult

- kiszámítani a költségek megtérülését,
- forrásokat találni az új módszerek bevezetéséhez,
- megindokolni a beruházási költségeket,
- meglátni azt, hogy hogyan lehet a formális módszerekkel piaci előnyre szert tenni.

A megrendelő vezetősége a legtöbbször

- a költségek csökkentésére van szorítva, és ezért persze
- elfogadja a legolcsóbb ajánlatot,
- bizonyos esetekben pedig nem is érdekli, hogy egy adott rendszert milyen módszerekkel fejlesztenek.

A fejlesztők azok, akik

- a legjobban látják a hagyományos módszerek korlátait, ennek ellenére
- nem támogatják erőteljesen a formális módszerek alkalmazását, mert
- nehéznek találják a formális módszereknek a meglévő fejlesztési folyamatba és fejlesztési technikák közé való beillesztését [Mon00].

A hatóság, speciálisan a vasúti biztonságért felelős hatóság

- a formális módszerek alkalmazását a feltétfüzetek, illetve specifikációk szintjén feltétlenül támogatja, de
- nincs felkészülve arra, hogy a különböző cégek különböző formális módszerekkel készült rendszereinek vizsgálatát el tudja látni, ezért
- arra törekszik, hogy valamilyen módon szabványosítsák a választható eszközök, illetve módszerek körét. Mindez csak a vasút, illetve a hatóság kezdeményezésére történhet, hiszen a cégeknek csak házon belül fűződik érdeke a szabványosításhoz [Suw99].

[Suw99] szerint mindaddig, amíg a fejlesztési folyamatban résztvevő valamennyi fél nem ugyanazt a nyelvet beszéli (értsd: azonos leíróeszközt, módszert használ), addig a formális módszerek alkalmazásának széleskörű elterjedése a vasútbiztosító berendezések fejlesztésében nem várható. Ezért is elgondolkoztató a megfogalmazás: „fontosabb standardizálni, mint a legjobb megoldást megkeresni”. A szabványosítási folyamatba a megrendelőn és a hatóságon kívül természetesen be kell vonni a fejlesztés területén már eredményeket elért cégeket is [Ság99b].

3.7. Új tudományos eredmények

Összefoglalva a fejezet új tudományos eredményeit azt mondhatjuk, hogy 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* 7.1.-7.4. fejezetek, 5. tézis).

A jelen tézisben bemutatott alkalmazási szempontrendszer egyaránt hasznos lehet a vasúti biztosítóberendezések szakterületét kutatók számára, és az ezen a területen tevékenykedő gyakorlati szakemberek számára. A 2. tézis a következő publikációkon alapul: [Ság00a, Ság00c, Ság00d, Ság00e, Ság01a, Ság01b].

4. A követelménykatalógus értékelése

A Braunschweigi Műszaki Egyetem Szabályozástechnikai és Automatizálási Intézete (IfRA), valamint a Német Vasút Kutatási és Technológiai Központja (FTZ) által 1998 májusában szervezett FORMS szimpózium résztvevőinek határozata értelmében egy munkabizottságot hoztak létre azzal a céllal, hogy konszenzust teremtsen a gyártók, a vasút és a felügyeleti hatóság között a formális módszerek alkalmazásával kapcsolatban. A német vasúti felügyeleti hatóság (EBA) meghívására és az IfRA koordinálásával a felügyeleti hatóság, a gyártók, az üzemeltető és a tudomány szakemberei összefogtak, hogy a megfelelő módszerek pragmatikus kiválasztását előkészítsék. Ennek első lépése annak a követelmény-katalógusnak [Anf99] a kidolgozása volt, amely megfogalmazza azokat az elvárásokat a vasútbiztosítási technika részéről, amelyek teljesítése lehetővé teszi a formális módszerek vasútbiztosításban való alkalmazhatóságát.

Bár e követelménykatalógus célja kifejezetten a biztosítóberendezési alkalmazási kérdések vizsgálata, a dokumentum kizárólag olyan általános követelményeket fogalmaz meg, amelyek teljesítése a formális módszerek bármely más alkalmazási területen történő felhasználása esetén is kívánatosak.

A vasúti biztosítóberendezések jellegzetességeit és fejlesztésük sajátosságait, továbbá az eddigi alkalmazási példákat figyelembe véve azt mondhatjuk, hogy a követelménykatalógusban megfogalmazott összes elvárás egyidejű kielégítése többnyire nem lehetséges és nem is célszerű. Ugyanakkor a biztosítóberendezések jellegzetességei jelentősen befolyásolhatják az egyes követelmények súlyát, jelentőségét.

Bár a követelménykatalógus összeállításában számos, magas képzettségű, az adott szakterületet jól ismerő szakember vett részt a kutatók, a vasút, a gyártó ipar és a felügyeleti hatóság oldaláról is, a dokumentum magán visel egy sor, a szöveges leírásokkal kapcsolatos nem kívánatos jegyet. Így például több, a katalógusban szereplő követelmény valójában a fejlesztendő rendszerrel szemben támasztott, illetve a rendszerfejlesztés módjával szemben támasztott követelmény, nem pedig a formális módszerekkel kapcsolatos elvárás. Természetesen fontos ezekre az elvárásokra is utalni, azonban ezek el nem különítése azt az érzést kelti, hogy ezek a problémák mind a formális módszerek alkalmazásával oldhatók meg.

A következőkben részletesen megvizsgáljuk és értékeljük a követelménykatalógus által megfogalmazott elvárásokat. Az egyes, a katalógusban szereplő követelmények leírása (dőlt betűvel szedve) után értékeljük azokat. Ez az értékelés az [Ság01a]-ban publikált eredményeinken alapszik.

4.1. Általános követelmények

4.1.1. Szemlélet és átalakíthatóság

A fejlesztési folyamatban résztvevő személyek számára a rendszer más és más szempontok szerinti szemlélete lehet mértékadó. Ilyen szempontok lehetnek például:

- *a struktúra,*
- *az adatok,*
- *a funkciók,*
- *a viselkedés,*
- *a megbízhatóság a „dependability” (RAMS) értelmében.*

Az alkalmazott módszernek lehetővé kell tennie a modellezett rendszer különböző nézőpontokból való vizsgálatát. Kívánatos, hogy a szoftverstruktúra és -funkciók formális technikával előállított modelljének a különböző szemléleteknek megfelelő automatikus átalakítása lehetséges legyen.

A különböző szemléleti módokhoz, alternatív módon, különböző formális technikákkal különböző modelleket lehet generálni. Ekkor azonban ezeknek a modelleknek a konzisztenciáját, illetve egymásnak való megfelelőségét bizonyítani kell, illetve a megfelelő formális technikák konzisztens integrációja révén biztosítani kell.

A követelményben felsorolt szempontok közül további értelmezésre szorulnak a funkcionalitás és a viselkedés szempontjai. [Win90] értelmezése szerint egy rendszer viselkedése a funkcionalitáson felül olyan viselkedési aspektusokat foglal magában, mint a hibatűrés, biztonság, válaszidő stb. Ez utóbbiakkal foglalkozik viszont a követelményben szereplő „megbízhatóság” szempont, valamint a következő követelmény pont, a „Teljesítményjellemzők”. Meg kell jegyezni, hogy a megbízhatósági jellemzők inkább teljesítményjellemzőként értelmezhetők.

Mindezeket figyelembe véve, a funkcionalitás és a viselkedés nem különíthetők el egymástól, ezért a továbbiakban csak a funkcionalitással foglalkozunk.

A vasúti feltétfüzetekben szereplő követelmények túlnyomó részét a *funkcionális* követelmények teszik ki. Így például az SBB elektronikus feltétfüzetekre kiadott feltétfüzetének 17 fejezetéből 11 fejezet (a terjedelem több mint 90%-a) tisztán funkcionális követelményeket ír le. A bevezetésen túl egy fejezet foglalkozik a rendszer alkalmazási körülményeivel (például működési hőmérséklet tartomány), egy a biztonsági, megbízhatósági követelményekkel, egy a karbantarthatósággal, egy a dokumentációval és egy a személyzet képzésével kapcsolatos elvárásokkal.

A Magyar Államvasutak által kiadott, elektronikus biztosítóberendezésekre vonatkozó feltétfüzet szintén leginkább a funkcionális kérdésekkel foglalkozik. A terjedelem körülbelül 80%-át a funkcionális elvárások kifejtése foglalja le. Természetesen ez a feltétfüzet is foglalkozik a biztonsági követelményekkel, a műszaki teljesítményjellemzőkkel, dokumentációval stb.

A létesítendő rendszer *struktúrájára* és *adataira* vonatkozó jellemzőket a vasúti feltétfüzetek nem specifikálják, ezek meghatározására csak a funkciók cégspecifikus megvalósítási módját bemutató gyári feltétfüzetek szintjén kerül sor. Ennek okai a következők:

- A vasút mint megrendelő nem feltétlenül kíváncsi arra, hogy a szállító cég rendszerének milyen a struktúrája, amennyiben az teljesíti a rendszerrel szemben támasztott funkcionális és nem funkcionális követelményeket.
- A rendszer struktúrájának meghatározása a vasúti feltétfüzet szintjén nem tenné lehetővé azt a gyakorlatot, hogy egy-egy vasúti feltétfüzetet több különböző cég is teljesíthet, esetleg eltérő struktúrájú rendszerekkel.

Meg kell jegyezni, hogy a vasúti biztosítóberendezések esetében a rendszerek struktúráját bizonyos mértékig meghatározza az a jellegzetesség, hogy az egyes vasútállomások vágányhálózata különböző típusú, ismétlődő külsőtéri objektumok összességéből áll. Ez azt jelenti, hogy egyfajta objektumorientáltság (a külsőtéri elemeket objektumoknak tekintve) a vasúti biztosítóberendezéseknél hagyományosan megtalálható. Ezt az objektumorientált szemléletet már a korai biztosítóberendezések is tükrözik, de vonatkozik ez a korszerű, elektronikus rendszerekre is. Ez a fajta strukturálás természetesen megjelenik a vasúti feltétfüzetekben is: a részletezett funkcionális követelmények a legtöbbször az objektumokra és azok kapcsolataira lebontva jelennek meg.

Összefoglalva azt mondhatjuk, hogy a vasútbiztosítás területén a legnagyobb jelentősége a funkcionális jellemzők formalizálásának van. Ennek okai a következők:

- A feltétfüzetek nagy részét a funkcionális követelmények teszik ki.
- Leginkább a funkcionális elvárások „szorulnak rá" leginkább a formalizálásra, mert ezekkel kapcsolatban merül fel a legtöbb félreértés a folyamat résztvevői között.
- A funkcionális követelmények az alkalmazás jellegéből adódóan (*lásd* 3.4.1. Műszaki alkalmazási szempontok – Az alkalmazás jellege) jól formalizálhatók.
- A szállító cég szempontjából a funkcionális követelményeket teljesítő rendszerrészek változnak viszonylag gyakran, ezért ezen a területen lehet hatékony a ráfordítások megtakarítása.

A megbízhatósági jellemzők elsősorban teljesítményjellemzőként értelmezhetők, az ezekre vonatkozó megfontolásokat ezért a következő pontban tárgyaljuk.

4.1.2. Teljesítmény

A már említett szempontok mellett a rendszer teljesítményjellemzőit is specifikálni kell. A formális technikának e területen is alkalmazhatónak kell lennie.

Teljesítményjellemzőként általában a rendszer számszerűsíthető jellemzői értelmezhetők. Biztosítóberendezések esetében a legfontosabb ilyen jellemzők a válaszidő, valamint a megbízhatóságra vonatkozó adatok (például MTBF). A teljesítményjellemzők specifikációja – éppen e jellemzők számszerűsíthető volta miatt – nem ütközik különösebb nehézségbe. A teljesítményjellemzők elvárt értékeire viszonylag könnyen megadható egy célérték. Ezért a formális *specifikációs* eljárásoknak e területen kisebb a jelentősége. Természetesen a formális módszerek a teljesítményjellemzőkkel kapcsolatosan is alkalmazhatók a rendszer fejlesztése és értékelése során, elsősorban annak vizsgálatára és igazolására, hogy az alkalmazott struktúra és a megvalósított funkciók teljesítik-e a megkövetelt célértékeket. E jellemzők azonban a funkcionalitástól eltérően formalizálhatók.

4.1.3. Követhetőség (érthetőség)

A formális technika alapkoncepciójának (beleértve a szintaktikát, szemantikát, korrektséget és verifikációt), és bonyolult rendszerek leírására és elemzésére való alkalmazásának elvileg eszköztámogatás nélkül is olvashatónak kell lennie a biztosítóberendezési mérnökök számára. Mindazonáltal törekedni kell támogatóeszközök használatára is. Az alkalmazott támogatóeszközök kezelőfelületét úgy kell kialakítani, hogy azt a biztosítóberendezési mérnökök elfogadják – anélkül, hogy komolyabb informatikai képzésben részesülnének. Ennek előfeltétele a könnyű kezelhetőség. Ehhez az kell, hogy mind az eszköz kezelőfelülete, mind a leíróeszköz jól vizualizálható legyen és könnyen értelmezhető szemantikával rendelkezzen.

A formalizmus érthetőségével kapcsolatban meg kell jegyezni, hogy a biztosítóberendezések fejlesztésének folyamatában résztvevő szereplők nem mindegyike vesz részt a formális specifikáció elkészítésében, többen közülük csak olvasni akarják az elkészült formális specifikációt. A formális specifikáció megfigyelhetővé tételének egyik lehetősége a formális specifikáció szimulációja (*lásd még* 4.2.3. Végrehajthatóság/Szimuláció).

4.1.4. Átjárhatóság

A technikát a vasúti, illetve a gyári feltétfüzet specifikációs fázisától kezdve a további fejlesztési fázisokon keresztül a kódgenerálásig alkalmazni kell.

Kívánatos lenne a célkódnak egy validált szoftvergeneráló eljárással történő automatikus vagy fél-automatikus generálása, aminek révén az előállított szoftverek további vizsgálatától már el lehetne tekinteni.

A verifikáció, a validáció és a tesztek elsődlegesen már a specifikációs fázisban végrehajthatók kell legyenek. Amennyiben különböző leíróeszközök alkalmazása válik szükségessé, ezeknek a módszer átjárhatósága érdekében egymással konzisztens módon összehangoltnak kell lenniük.

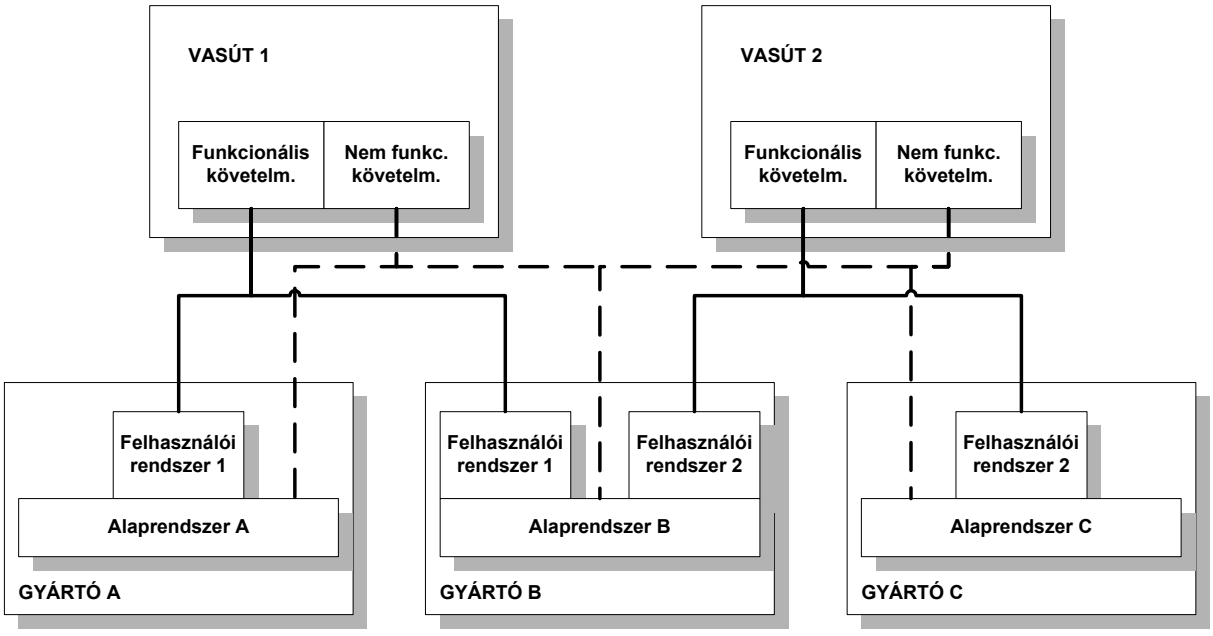
A korszerű, elektronikus vasúti biztosítóberendezések strukturálisan a következő alrendszerekre oszthatók:

- alaprendszer,
- felhasználói rendszer.

Az alaprendszer olyan alapvető, az adott alkalmazástól független funkciókat tartalmaz, mint például az operációs rendszer és a kommunikációs rendszer. E rész feladata a strukturális/belső biztonság biztosítása. Az alaprendszer hardver és szoftver részeket egyaránt magába foglal. A felhasználói rendszer az alaprendszer által működtetett szoftverrel van megvalósítva. E rész feladata az adott vasút által elvárt funkciók megvalósítása. A gyakorlat szerint a gyártó cégek egyetlen alaprendszerükre több, különböző vasutak funkcionális követelményeit kielégítő felhasználói rendszert is fejlesztenek.

Kis egyszerűsítéssel azt mondhatjuk, hogy a felhasználói rendszer teljesíti a feltétfüzet funkcionális követelményeit, míg az alaprendszer a nem funkcionális, a teljesítményjellemzőkre és a megbízhatóságra vonatkozó követelményeket.

A vasúti biztosítóberendezések fejlesztésének jellegzetessége, hogy egyetlen követelményrendszer (vasúti feltétfüzet) több olyan, különböző típusú megvalósított rendszer alapjául szolgálhat (21. ábra), amely rendszereket az egyes gyártó cégek gyári feltétfüzetekben specifikálják.



21. ábra. A vasúti biztosítóberendezések megrendelői és szállítói

A feltétfüzet követelményeit tehát rendszerint több szállító cég próbálja meg kielégíteni, a legtöbbször egy már meglévő rendszer adaptációjával, továbbfejlesztésével. Egy-egy új feltétfüzet követelményeinek teljesítéséhez a gyártó cég egy meglévő alaprendszerét veszi alapul. Ellenőrzi, hogy az adott alaprendszerrel teljesíthetők-e a feltétfüzet nem funkcionális követelményei. Ennek megállapítása rendszerint nem túlságosan bonyolult feladat, ugyanis a nem funkcionális követelmények többnyire olyan teljesítményjellemzők, amelyek jól számszerűsíthetők. Az új feltétfüzet funkcionális követelményeinek kielégítése történhet egy már meglévő felhasználói rendszer módosításával vagy továbbfejlesztésével, illetve egy teljesen új felhasználói rendszer kifejlesztésével. Ez a gyakorlat megerősíti azt, hogy a vasútbiztosítás területén elsősorban a funkcionális követelmények formális kezelése szükséges.

A *vasúti feltétfüzetek* szintjén olyan formalizálásra van szükség, amely a hagyományos specifikációs technikákhoz képest egyértelműbben képes leírni a rendszertől elvárt funkcionális követelményeket. Ehhez elegendő lehet a bemutatott szigorúsági szintek közül az 1-es is, azaz matematikai, logikai jelölések alkalmazása (fél-formális – formális szintaktika) és informális szemantika. Az 1-es szigorúsági szint alkalmazása által a jelenlegi gyakorlathoz képest egyértelműbb lehet a funkciók leírása. A formális szintakszis megkönnyíti a nemzetközi projektek esetében felmerülő nyelvi fordításokból származó nehézségek megoldását is. Az 1-es szint azonban nem teszi lehetővé a formális specifikáció formális ellenőrzését. A specifikáció ellenőrzésére (például típusellenőrzés, szintaktikai ellenőrzés stb.) a 2-es szigorúsági szint (formális szintaktika, fél-formális szemantika) alkalmazásával nyílik lehetőség. A feltétfüzet funkcionális követelményeinek formális analízise (például konzisztencia és teljesség vizsgálata), illetve a leírt funkciók szimulációja (*lásd* 4.2.3. fejezet) akkor lehetséges, ha a leíróeszköz fél-formális – formális szemantikával is rendelkezik, azaz eléri a 3-as szigorúsági szintet. A 3-as szigorúsági szint alkalmazása esetén a vasút és a hatóság, valamint a vasút és a gyártó között szükséges egyeztetés mértéke mérséklődhet. Meg kell jegyezni, hogy a 3-as szint alkalmazása a vasúti feltétfüzetek szintjén az elérhető előnyök miatt ugyan kívánatos, a közeljövőben azonban nem tűnik reális elvárásnak, hogy a vasút a feltétfüzetét a legmagasabb szigorúsági szinten formalizálja.

A gyártó, illetve fejlesztő cégek alapvető érdeke az, hogy a szállítandó rendszert hibátlanul, minél kisebb ráfordítások árán fejlessze ki. E szempontból a gyártó cégek számára a formális módszerek előnyei közül elsősorban a legalább részben formális (és így automatizálható) fejlesztés, és a formális verifikáció lehetősége bírnak nagy jelentőséggel. Ezeknek a lehetőségeknek a kihasználásához a *gyári feltétfüzet* formalizálásának szigorúsága el kell érje a 3-as szintet. Amennyiben a vasúti feltétfüzet ennél alacsonyabb szigorúságú formalizáltsággal áll rendelkezésre, akkor a gyártó cég feladata, hogy ebből egy olyan formális specifikációt állítson elő, amely alapja lehet a további formális fejlesztési eljárásnak.

4.1.5. Szabványok

Az alkalmazandó formális technikának támogatnia kell a CENELEC szabványoknak megfelelő rendszerfejlesztést. A vasúti alkalmazással kapcsolatos legfontosabb európai szabványok a következők:

- *EN 50126 Vasúti alkalmazások – A megbízhatóság, rendelkezésreállás, karbantarthatóság és biztonság (Reliability, Availability, Maintainability and Safety - RAMS) specifikálása és demonstrálása,*
- *EN 50128 Szoftver a vasúti vezérlő és védelmi berendezések számára,*
- *ENV 50129 Vasúti alkalmazások – Elektronikus vasúti biztosítóberendezések.*

—

4.1.6. Interfészek a projektmenedzsment részfeladatai számára

A technika tegye lehetővé a csatlakozást a projektmenedzsment különböző részfeladataihoz, elsősorban • *a konfiguráció- és minőségmenedzsment (*lásd *verifikáció, validáció, tesztelés és kockázatelemzés) és* • *a dokumentációmenedzsment tekintetében.*
—

4.2. Módszertani követelmények

4.2.1. A biztonsági és a nem biztonsági igényű funkciók szétválasztása

A biztonsági és a nem biztonsági igényű funkciók specifikációjának szétválasztása a hatóság szempontjából azzal a következménnyel járhatna, hogy csak a biztonságkritikus rész specifikációját, és a nem biztonsági igényű résznek az előbbire való visszahatásmentességét kellene felülvizsgálnia. Ezt az eljárást a formális technikák alkalmazása támogatja.
A biztonsági és a nem biztonsági igényű funkciók szétválasztása fontos követelmény minden biztonsági rendszerrel, illetve az ilyen rendszerek fejlesztésével szemben. Ez a követelmény azonban nem a formális módszerektől elvárt „szolgáltatásra” vonatkozik, hanem a rendszerek fejlesztésének módjára.

4.2.2. A különböző specifikációs aspektusok (funkcionális-, teljesítmény- és biztonságspecifikáció) elkülönítése

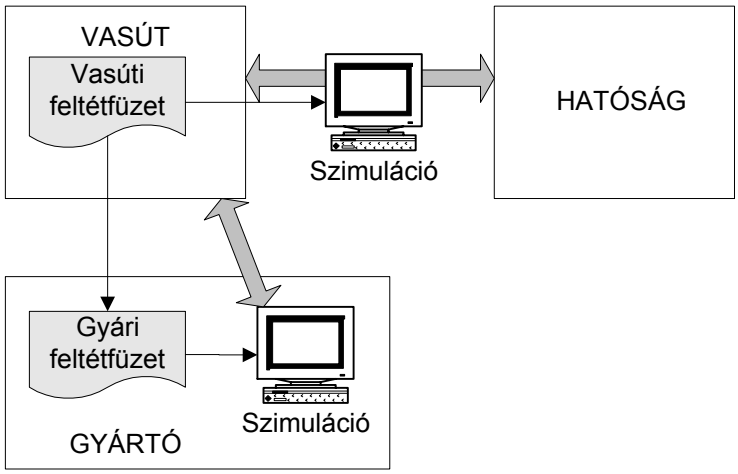
A funkcionális specifikáción kívül lehetőséget kell biztosítani az egyes funkciók temporális logikai tulajdonságainak, mint például a biztonsági követelményeknek és a teljesítmény szempontoknak a specifikálására is.
Az itt megjelenő követelmény nem választható el a 4.1.1 pontban megfogalmazott követelménytől.

4.2.3. Végrehajthatóság/szimulálhatóság

A követelmények formális specifikációja alapján a jövőbeli rendszer tulajdonságait szimulálni kell tudni annak érdekében, hogy a felhasználó, a gyártó és a felügyeleti hatóság közötti félreértéseket és homályos megfogalmazásokat már ezen a szinten el lehessen kerülni, illetve meg lehessen szüntetni. *A követelményspecifikációnak csak az ún. konstruktív része kell szimulálható legyen, a leíró részek, mint például a temporális logikai tulajdonságok ehelyett verifikálhatók kell legyenek.*
A formális specifikációk végrehajthatóságát és szimulálhatóságát célszerű külön vizsgálni a vasúti és a gyári feltétfüzet szintjén (22. ábra). A vasúti feltétfüzetben megfogalmazott funkcionális követelmények szimulációja a felügyeleti hatóság és a vasút közti egyeztetés elősegítése céljából lehet szükséges, ugyanis a

hatóság a vasúti feltétfüzetet hagyja jóvá. (Meg kell jegyezni, hogy erre irányuló gyakorlati alkalmazás eddig nem ismert).

A gyári feltétfüzet szimulációja a vasút és a gyártó cég közti egyeztetés egyik lehetséges módja. A szimuláció ebben az esetben elsősorban a gyártó számára bír nagy jelentőséggel, mert így a fejlesztés korai szakaszában feltárhatók a gyártó és a vasút közti félreértések, és ezáltal az életciklusköltségek csökkentése érhető el. Ilyen célú szimulációt alkalmaz például a Siemens GRACE rendszere [Red99].



22. ábra. A szimuláció szerepe a vasúti és a gyári feltétfüzet esetén

4.2.4. Verifikáció

A verifikáció segítségével a rendszernek az egyes fejlesztési fázisok folyamán adódó különböző megjelenési formáit konzisztencia (ellentmondás-mentesség) szempontjából vizsgálják. Valamely formális technika alkalmazása egyebek mellett a verifikálhatóság biztosítását, és ezzel a validáció bonyolultságának mérséklését is kell jelentse.

A rendszerrel szemben támasztott általános követelményeket formális módon kell pontosítani, és amennyiben a technika lehetővé teszi, már a specifikációs fázisban verifikálni.

A technika segítségével generált modelleket úgy kell előállítani, hogy a biztonsági tulajdonságok (automatikus) formális bizonyítása lehetséges legyen.

Lásd 4.1.4 Átjárhatóság

4.2.5. Validáció

A validáció a specifikáció érvényességének (a felhasználó által értelmezett helyességének) és teljességének vizsgálata. A módszernek a rendszer validációját is tartalmaznia kell.

A formális specifikáció érvényességének ellenőrzésére a vasúti biztosítóberendezések vonatkozásában az eddigiekben a következő módszerek alakultak ki:

- a formális specifikáció szimulációja (például GRACE rendszer [Red99]);
- a formális dokumentum visszafordítása természetes szöveggé (például [Eri98, Eri96]).

Egy teljes rendszer validációjának a rendszernek és a rendszerrel szemben támasztott eredeti követelményeknek az összevetését nevezzük. Ebből a szempontból vasúti biztosítóberendezések esetén az eredeti követelményeknek még a feltétfüzetet megelőző

koncepciót tekinthetjük. A nehézség abban rejlik, hogy ez a koncepció nincs formálisan megfogalmazva, komoly részben tapasztalatokon, hagyományokon alapul. Egy rendszer formális validációja akkor lenne elképzelhető, ha ez a koncepció formálisan lenne megfogalmazva.

4.2.6. Teszt

Az előállított specifikáció tesztelhető kell legyen, vagyis a megkövetelt funkciók, adatstruktúrák és -tulajdonságok, valamint a biztonságkritikus időkritériumok és folyamatstruktúrák vizsgálhatók kell legyenek.

Továbbmenve, az implementált rendszer is tesztelhető kell legyen, és a formális követelményspecifikáció segítségével a tesztesetek, -illesztősíkok és -kritériumok a teljes rendszernek a célhardveren végrehajtandó validációja számára automatikusan generálhatók kell legyenek.

Ugyanez érvényes a rendszer komponenseire és azok integrációjára is.

A követelmény helyes értelmezéséhez meg kell jegyezni, hogy tesztesetek generálása a teszt-illesztősíkok, a tesztkritériumok és a funkcionális követelmények alapján lehetséges.

4.2.7. Kockázat- és veszélyelemzés

A vasút a biztonságkritikus funkciókat illetően kockázatelemzést hajt végre, és megadja az elfogadható kockázat nagyságát, mint biztonsági célt. Ezen biztonsági célok alapján a gyártó kifejleszti a megfelelő műszaki megoldást, amelyet veszélyeztetési elemzésnek vet alá.

A veszélyeztetési elemzés eredményének táblázatos kiértékeléséből kapjuk meg a biztonsági követelmény fokozatokat (Safety Integrity Level – SIL) a műszaki megoldás egyes komponenseinek szoftvere számára. A különböző biztonsági követelmény fokozatok különböző intézkedéseket igényelnek a szisztematikus hibák mérséklésére. Ezen intézkedésekhez tartozhat adott esetben a formális technikák alkalmazása. Emellett a kockázatelemzés és veszélyeztetési elemzés formális technikák alkalmazásával történő végrehajtására is törekedni kell.

A kockázat- és veszélyelemzést segítő módszerek formalizálása előnyös lehet, ez azonban a funkcionális részek formalizálásától elkülönülten képzelhető el.

4.3. Strukturális követelmények

4.3.1. Modularitás/komponálhatóság

A specifikáció modularitását és komponálhatóságát biztosítani kell.

A verifikációnak és a validációnak modulonként is végrehajthatónak kell lennie, ami a vizsgálatok lépésenkénti vagy párhuzamos végrehajtását is lehetővé teszi.

Ez a követelmény a rendszerek fejlesztésére vonatkozik. A formális módszerekre vonatkoztatva azt mondhatjuk, hogy olyan módszer alkalmazása célszerű, amely támogatja a moduláris rendszerfejlesztést.

Meg kell jegyezni továbbá, hogy a követelményben nem veszik figyelembe azt, hogy a specifikáció és az implementáció modularitása eltérő lehet.

4.3.2. Absztrakció/finomítás

Szükség van olyan absztrakciós és finomítási mechanizmusokra, amelyek a rendszert magas absztrakciós fokon áttekinthető, és ugyanakkor szemantikailag jól definiált módon ábrázolják, és lehetővé teszik a fokozatos finomítást, illetve absztrahálást.
Az absztrakció és a finomítás fontos jellemzője a rendszerfejlesztésnek, ezért a formális módszerek szinte mindegyike támogatja ezt az eljárást.

4.3.3. Kompatibilitás a hagyományos specifikációs technikákkal

A hagyományos specifikációs kifejezési módok integrálása céljából illesztési felületeket kell kialakítani. Általában a fejlesztéseket nem szigetszerűen hajtják végre, így gyakran van szükség meglévő rendszerek hagyományos módon előállított specifikációinak figyelembevételére. Ezeket mindenképen precízebbé kell tenni, mert a verifikáció csak formális specifikációk, vagy a hagyományos specifikációk formalizálása keretében lehetséges. *A rendszerleíráshoz használt különböző formális specifikációs technikák közötti kompatibilitást szintén biztosítani kell.*
A hagyományos specifikációs technikákkal való kapcsolat általános probléma, de a vasútnál ennek kiemelt jelentősége van, ugyanis a vasút tipikusan felhasználója a különböző illesztéseknek: az új rendszerek nem elszigetelten, hanem korábban létesített rendszerekkel kölcsönhatásban működnek. Ilyen esetekben nagy jelentősége van a rendszerek közötti illesztéseknek, melyek specifikációjának és további fejlesztésének formalizálása jelentős előnyökkel járhat. Más vonatkozásban: a korábban létesített rendszerek várhatóan nem formálisan vannak specifikálva, ezért e rendszerek, de legalábbis illeszkedő részrendszereik specifikációjának formalizálása szükségessé válhat. Egy másik, ide kapcsolódó terület, a meglévő rendszerek utólagos formális verifikációja (*lásd például* [Eri96, Eri98]). Ilyen esetekben az implementált rendszer formális vizsgálatával (az implementáció természeténél fogva formális, például szoftverek esetében, vagy könnyen formalizálható, például elektronikus kapcsolások) próbálják a rendszer helyességét bizonyítani. Ehhez természetesen elengedhetetlen a rendszerrel szemben támasztott követelmények, legalább részleges, formalizációja.

4.3.4. Migráció

A meglévő specifikációk jövőbeli formális leírási módokra való transzformációját eljárásokkal támogatott módon lehetővé kell tenni. *A formális technika támogassa az adott rendszer továbbfejlesztését is.*
A jövőbeli formális leírásokra való transzformáció lehetősége csak úgy képzelhető el, hogy a jövőbeli leírási módokat kell úgy kialakítani, hogy azokra a jelenlegiek transzformálhatók legyenek. Egy adott rendszer továbbfejlesztésének lehetősége elsősorban nem az alkalmazott formális módszeren múlik, hanem a rendszer eddigi fejlesztésének módján (megfelelő modularitás, dokumentáltság stb.).

4.3.5. Újrafelhasználhatóság

Egy projekt már rendelkezésre álló specifikációja, vagy annak egyes részei más projektekben is felhasználhatók kell legyenek. A specifikációnak különböző hardverplatformokra átvihetőknek kell lenniük (portabilitás, illetve hardverplatformoktól való függetlenség).
Az újrafelhasználhatóság a vasúti feltétfüzetek követelményeivel kapcsolatosan alapvető követelmény, hiszen egy-egy feltétfüzet követelményeit rendszerint több szállító cég is megpróbálja kielégíteni. Ilyen módon a feltétfüzetben megjelenő követelmények több hardverplatformon is realizálódnak. Az adott funkciók cégspecifikus megoldási módját leíró gyári feltétfüzettel kapcsolatban a hardverplatformtól való függetlenség teljes egészében nehezen képzelhető el, ugyanis a funkciók megoldási módját alapvetően befolyásolják az alaprendszer jellemzői.

4.4. Összefoglaló értékelés

A következőkben egy összefoglaló táblázatban mutatjuk be a követelménykatalógus értékelését (5. táblázat).

5. táblázat. A Követelménykatalógus összefoglaló értékelése

		Bírálat	Kiegészítés	A követelmény értelmezése vasúti biztosítóberende-zésekre
I. Általános követelmények				
1	Személet és átalakíthatóság	**X**	**X**	**X**
2	Teljesítmény	**X**	**X**	
3	Követhetőség (érthetőség)		**X**	**X**
4	Átjárhatóság		**X**	**X**
5	Szabványok			
6	Interfészek			
		33%	66%	50%
II. Módszertani követelmények				
1	Bizt. és nem bizt. funkciók szétválasztása	**X**		
2	Specifikációs aspektusok elkülönítése	**X**		
3	Végrehajthatóság/szimulálhatóság		**X**	**X**
4	Verifikáció			
5	Validáció	**X**	**X**	**X**
6	Teszt	**X**	**X**	
7	Kockázat- és veszélyelemzés		**X**	
		57%	57%	28%
III. Strukturális követelmények				
1	Modularitás/komponálhatóság	**X**	**X**	
2	Absztrakció/finomítás		**X**	
3	Kompatibilitás a hagyományos spec. techn.		**X**	**X**
4	Migráció	**X**	**X**	
5	Újrafelhasználhatóság	**X**	**X**	**X**
		60%	100%	40%
		50%	**72%**	**39%**

Az 5. táblázatban feltüntettük az egyes, a követelménykatalógusban szereplő követelményeket, és ezekhez kapcsolódva azt, hogy

- mely követelményeket kellett bírálni,
- melyekhez volt szükséges kiegészítéseket fűzni és hogy
- melyek esetén volt célszerű a követelményt a vasúti biztosítóberendezésekre szűkebben értelmezni.

Az összesen 18 követelmény fele esetében a követelménnyel, vagy annak megfogalmazásával kapcsolatban alakult ki bíráló vélemény. A követelmények mintegy 70%-ához fűztünk kiegészítést, és körülbelül 40%-uk esetén volt célszerű az adott követelményt a vasúti biztosítóberendezések területére értelmezni.

A bírálatok, kiegészítések és értelmezések hozzáfűzése révén a követelménykatalógus jobban megfelel eredetileg kitűzött céljának, azaz segíti a megfelelő formális módszerek kiválasztását és alkalmazását a vasúti biztosítóberendezések területén.

4.5. Új tudományos eredmények

A fejezet alapján született új tudományos eredményeket a 3. tézisben foglaljuk össze.

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 tézis a [Ság01a] publikáción alapul, eredményei elsősorban a tématerület további kutatásaiban hasznosíthatók.

5. Vasútbiztosítási alkalmazások

A szakirodalmat átvizsgálva az tapasztalható, hogy sok kutatási projekt foglalkozik a vasúti biztosítóberendezések szakterületével mint a biztonságkritikus rendszerek egyik jelentős példájával. A formális módszereket kutató szakemberek is előszeretettel választják a vasúti biztosítóberendezéseket alkalmazási példaként. Ennek eredményeként a szakirodalomban számos helyen találkozhatunk a formális módszerek vasútbiztosítási alkalmazásával.

Emellett természetesen több olyan projekt is létezik, amelynek célja a *vasútbiztosítás számára* alkalmas módszerek, eljárások, például formális módszerek kutatása.

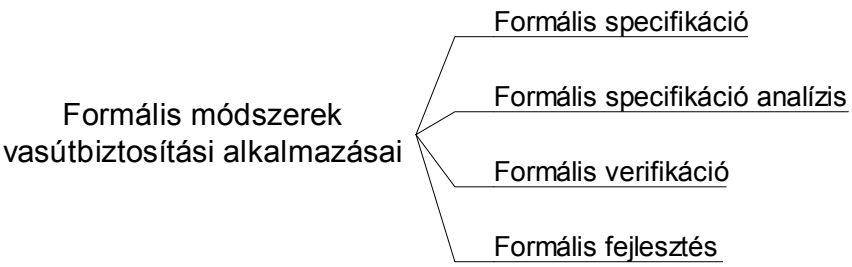
A formális módszerek vasútbiztosítási alkalmazása számára érvényes irányelvek meghatározásához *elengedhetetlen* a publikált gyakorlati alkalmazások összegyűjtése. Ezért összegyűjtöttük ezeket az alkalmazásokat, és közülük a következőkben ismertetünk tizanhat olyan jellegzetes, vagy valamilyen szempontból tanulságos alkalmazást, amelyek továbbiak szempontjából iránymutatóak lehetnek.

Az összegyűjtött alkalmazási példák mennyisége és sokfélesége miatt feltétlenül szükséges ezeknek valamilyen rendszer szerinti csoportosítása. E célból egy csoportosítási szisztémát alakítunk ki és mutatunk be az 5.1. fejezetben.

Az 5.2. fejezetben az összegyűjtött alkalmazási példákat tekintjük át, egy célszerű csoportosítási rendszerben. Az egyes alkalmazásokat a 3. fejezetben kidolgozott *Alkalmazási szempontrendszer*, valamint a 4. fejezetben értelmezett és kiegészített *Követelménykatalógus* szerinti értékeljük az 5.3. fejezetben.

5.1. Az alkalmazások csoportosítása

A formális módszerek a vasútbiztosítás területén is különböző célokból, sokféle módon használhatóak. Ezért az alkalmazási példák bemutatásához és értékeléséhez célszerű az alkalmazásokat csoportosítani (23. ábra).



23. ábra. A formális módszerek vasútbiztosítási alkalmazásainak csoportosítása

Az alkalmazási példák első körébe azok az esetek tartoznak, ahol a formális módszerek a rendszer életciklusának csak a *specifikációs fázisát* érintik. A formális specifikációs nyelveket ezekben az esetekben a specifikáció minőségének javítására (*lásd* 2.2.1. Formális specifikáció) alkalmazzák.

A következő csoportot azok az alkalmazások alkotják, amelyek esetében a formális specifikációs nyelv segítségével a vizsgálandó rendszer *formális modelljét* készítik el, és a modellen különféle elemzéseket végeznek el (*lásd* 2.2.2. Formális specifikáció analízis). Az elemzéseknek, illetve magának a formális modell felállításának a célja alkalmazásonként különböző.

A harmadik kör azokat az alkalmazásokat foglalja magába, ahol a formális módszereket a vizsgálandó rendszer bizonyos tulajdonságai meglétének, illetve meg nem létének formális bizonyítására alkalmazzák, azaz *formális verifikációt* végeznek el.

Külön csoportban érdemes tárgyalni a formális módszereknek azokat az ipari alkalmazásait, amelyek esetében a formális módszereket megvalósított *vasúti biztosítóberendezések fejlesztése* során használták, illetve használják fel.

A következő alfejezetekben bemutatunk és röviden értékelünk az egyes csoportokba tartozó, néhány jellegzetes, újabb keletű alkalmazási példát. Az alfejezetek végén további, részben korábbi keletkezésű, az adott csoportba tartozó alkalmazási példák irodalmi hivatkozásait is megadjuk.

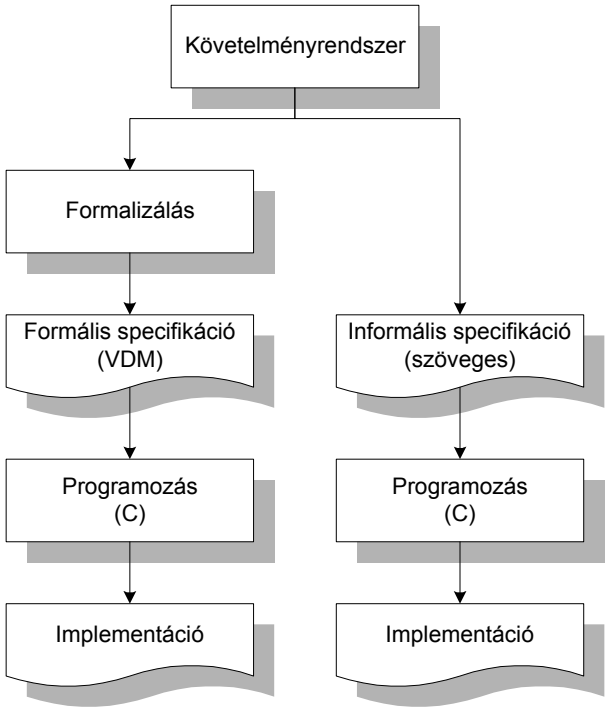
5.2. Alkalmazási példák a vasútbiztosítás területéről

5.2.1. Vasúti biztosítóberendezések formális specifikációja

5.2.1.1. [Hir99]-ben a VDM formális módszert specifikációs nyelvként alkalmazták. A bemutatott projekt célja az volt, hogy össze lehessen hasonlítani a hagyományos és a formális specifikációból kiinduló fejlesztési folyamatokat.

Eszköz	VDM
Eljárás	A programozás időszükségletének összehasonlítása, hagyományos specifikációból és formális specifikációból kiindulva

A specifikálandó és implementálandó rendszer egy automatikus vonali vonatirányító rendszer (ATC) egyik adatbázisa volt. Ennek informális követelményrendszere volt a kiindulási pont mindkét típusú fejlesztés számára (24. ábra).



24. ábra. A [Hir99] által bemutatott fejlesztési eljárás

Az informális követelményrendszert formalizálva egy VDM nyelvű formális specifikációt állítottak elő. Az egyik programozó e formális specifikáció alapján programozta a feladatot C programozási nyelven, míg egy másik programozó, ugyancsak C nyelven, a szöveges specifikáció alapján dolgozott. A programozási munka a formális specifikáció alapján kb. a harmadába került, mint a hagyományos módszer. Ezt az eredmény alapvetően a következőnek tulajdonítható: a VDM specifikáció elkészítéséhez szükséges volt a program modulstruktúrájának kialakítása, míg a szöveges specifikáció esetén ez nem szükséges, ekkor viszont a programozás során kell ezt megtenni. Az informális programfejlesztés során tehát olyan, tulajdonképpen specifikációs lépéseket kell elvégezni, amelyekre a formális esetben a specifikáció fázisában kerül sor.

5.2.1.2. [Fuk00] a VDM formális módszer olyan alkalmazásáról számol be, amelynek során egy biztosítóberendezéssel kapcsolatos informális követelményeket a VDM módszer specifikációs nyelvén formalizálják. A formális követelményrendszer működését ezután egy PC-n szimulálják. Az alkalmazás célja a rendszer megrendelői és szállítói közti könnyebb megértés elősegítése. A formális specifikációt nem alkalmazzák közvetlenül magának a biztosítóberendezési rendszernek a fejlesztéséhez.

Eszköz	VDM
Eljárás	Az informális követelményeket formalizálják a VDM specifikációs nyelvének segítségével. A formális specifikáció által leírt rendszer működését pedig PC-n szimulálják. Ez tulajdonképpen a formális specifikáció validációjának tekinthető. Ha a formális specifikáció megfelelő, akkor a későbbiekben fel lehet használni az implementáció elkészítéséhez.

5.2.1.3. [Ara00] a vasúti problémák kezelésére az objektumorientált modellezési eljárások alkalmazását javasolja. Példaként egy rádiós alapú sorompóberendezés objektumorientált modellezési eljárását mutatják be.

Eszköz	Objektumorientált modellezés, UML-, MSC-szintaktika
Eljárás	Rádiós alapú sorompóberendezés működésének objektumorientált modellezése

A rendszer ilyen módon való modellezéséhez a következő leíróeszközöket alkalmazza:

- osztálydiagrammok a rendszer struktúrájának (alrendszerek és azok kapcsolatai) leírására, UML szintaktikával;
- üzenetdiagrammok a rendszer dinamikus viselkedésének leírására, MSC-(Message Sequence Chart) szintaktikával;
- állapotdiagrammok az egyes objektumok viselkedésének leírására, UML-szintaktikával.

A rendszer objektumorientált elemzésének eredménye egy olyan modell, amelyik tartalmazza a rendszer struktúráját és viselkedését. Az objektumorientáltság lehetővé az egyes rendszerösszetevők jellemzőinek tetszőlegesen absztrakt, vagy akár a lehető legrészletesebb módon való ábrázolását. [Ara00] értékelése szerint az objektumorientált megközelítés előnyei közé tartozik, hogy

- a kapcsolódó jelölésmód könnyen megtanulható és értelmezhető a rendszerfejlesztés valamennyi résztvevője számára;
- kompakt, egyértelmű, könnyen módosítható és továbbfejleszthető modellek készíthetők, amelyek
- a rendszer fejlesztésének több fázisában (specifikáció, tervezés, implementáció) felhasználhatók.

A jelenlegi objektumorientált módszerek legnagyobb problémájának [Ara00] azt tartja, hogy a kapcsolódó leíróeszközök szintaktikája, illetve szemantikája nem teszi lehetővé, hogy a modellen formális elemzések elvégezhetők legyenek.

5.2.1.4. [Ber00] egy ún. jelzővel függésben lévő sorompó esetén a biztosítóberendezés és a sorompó berendezés közti, ún. Hp-interfész modellezését mutatja be.

Eszköz	MSC, SDL
Eljárás	A funkcionalitás formális specifikációja

A feladatot MSC (Message Sequence Chart), illetve a SDL (Specification Description Language) segítségével modellezi. Az SDL formális specifikációs nyelv valósidejű rendszerek leírására. Rendelkezik a szintaktika és a szemantika formális/automatikus ellenőrzésének lehetőségével, az elkészített modell szimulálható. [Ber00] a következő modellezési módszertant javasolja:

1. A mintapélda alapján MSC-vel az objektumok kommunikációja alapján a szcenáriók leírása.
2. A teljes rendszer modellezése SDL-lel.
3. Az alkalmazott SDL tool (SDL Design Tool Telelogic Tau 4.0) validátora segítségével az SDL és az MSC specifikáció automatikusan összevethető, bizonyítható a kettő konzisztenciája. Ez jelentheti a modell verifikációját.
4. A modell validációja az SDL modell szimulációjával történhet. Ehhez természetesen szükséges a környezet modellje, illetve lehet a valódi rendszerkörnyezetet is használni, hiszen a feladat tárgya egy interfész.

5.2.1.5. [Klo00] szintén az 5.2.1.4. pontban bemutatott feladat modellezését végzi el. A modellezési eljárás során két eszközt használtak. Az egyik a DOORS, amely Requirement Engineering/Requirement Tracing funkciókat lát el: támogatja a felhasználói követelmények lebontását, nyomonkövetését stb. A tapasztalatok szerint a DOORS tool a fejlesztőt strukturált munkára kényszeríti, és megfelelően alkalmazva megkönnyíti a specifikációs dokumentumok átvizsgálását.

Eszköz	DOORS, Statemate
Eljárás	A funkcionalitás formális specifikációja

Magához a formális modell elkészítéséhez a Statemate toolt használták, amelyet már sikerrel alkalmaztak a légiközlekedési, ill. közúti közlekedési rendszerek fejlesztésénél. A Statemate kétféle leírást támogat: activity charts a funkcionális, logikai leírásra és statecharts a reaktív viselkedés leírására. Ilyen módon lehetővé teszi:

- a formális specifikáció elkészítését,

- a specifikáció szimulációval történő validálását.

A Statemate használatának előnye a grafikus leírás és a struktúra vizuális megjelenítése az activity-chart-okon, a működés pedig jól áttekinthető a statechart-okon. Ezek a leírási módok a modellezés megfelelő strukturálását és hierarchizálását kényszerítik ki. A tool hasznos funkciója a szimulálhatóság. A Statemate hátránya a magas beszerzési költség és a „lapos betanulási" görbe. A formális verifikációs tool formális bizonyítási/elemzési lehetőséget biztosít (ennek minden előnyével), de használata komoly betanulást igényel és bizonyos modellméret fölött nem alkalmazható. (Más tapasztalatok is megerősítik, hogy a Statemate csak kis funkcionalitás leírására alkalmas.)

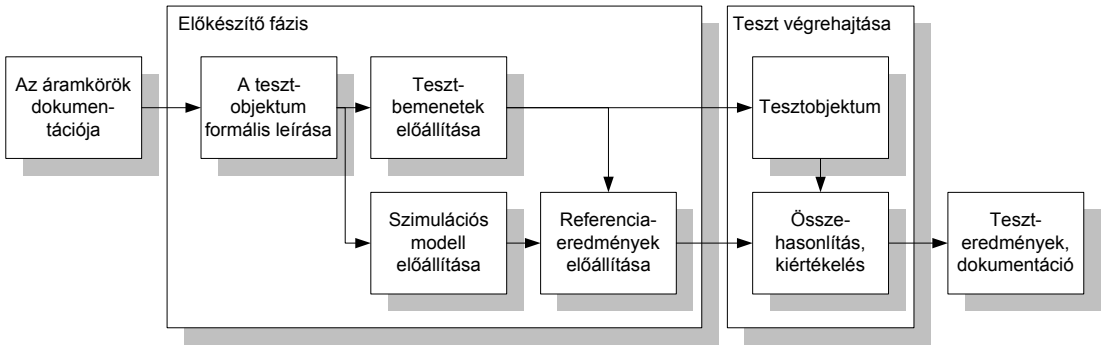
A modellezés során sikerült feltárni az eredeti specifikáció néhány hiányosságát, illetve gyenge pontját.

További, a vasúti biztosítóberendezések formális specifikációjával foglalkozó irodalmak: [Cas99, Bec96, Bol94, Fok96, Fok98, God95, God99, Gro94, Gro95, Gro98, Har95, Jan02 Kol98].

5.2.2. Biztosítóberendezések formális modellezése és analízise

5.2.2.1. A Budapesti Műszaki Egyetem Közlekedésautomatikai Tanszékén az 1970-es években fejlesztettek ki egy automatizált jelfogóegység-vizsgáló rendszert [Tar82a, Tar82b, Tar84]. E rendszer részeként logikai algebrai alapú formális leíró nyelvet és módszert dolgoztak ki a jelfogóegységek áramköreinek leírására. A jelfogóegységek kapcsolási rajza alapján, a kialakított leírónyelvet alkalmazva, elkészítették az áramkörök formális leírását. A formális leírás alapján a rendszer nagymértékben automatizáltan előállította az adott leírással reprezentált jelfogóegység teszteléséhez szükséges tesztbemeneteket, és a formális leírást mint szimulációs modellt felhasználva, teljesen automatikusan előállította a referenciaeredményeket. A rendszer a tesztelés folyamatát is automatizálta, amennyiben a kifejlesztett vizsgálóberendezés automatikusan kapcsolta a vizsgálandó jelfogóegységre az előzőleg generált tesztbemeneteket, és összehasonlította a tesztek eredményeit a referenciaeredményekkel (25. ábra).

Cél	Terméktesztelés
Leíróeszköz	Algebrai leírás
Támogatóeszköz	Saját fejlesztés



25. ábra. Az automatikus jelfogóegység-vizsgáló rendszer működése [Ság99b]

5.2.2.2. Az Egységes Európai Vonatbefolyásoló Rendszer (ETCS) informális specifikációja alapján a Braunschweigi Műszaki Egyetem Szabályozástechnikai és Automatizálási Intézete (IfRA) a Deutsche Bahn AG megbízásából egy formális modellt állított elő [Mey98a, Mey98b, Jan99].

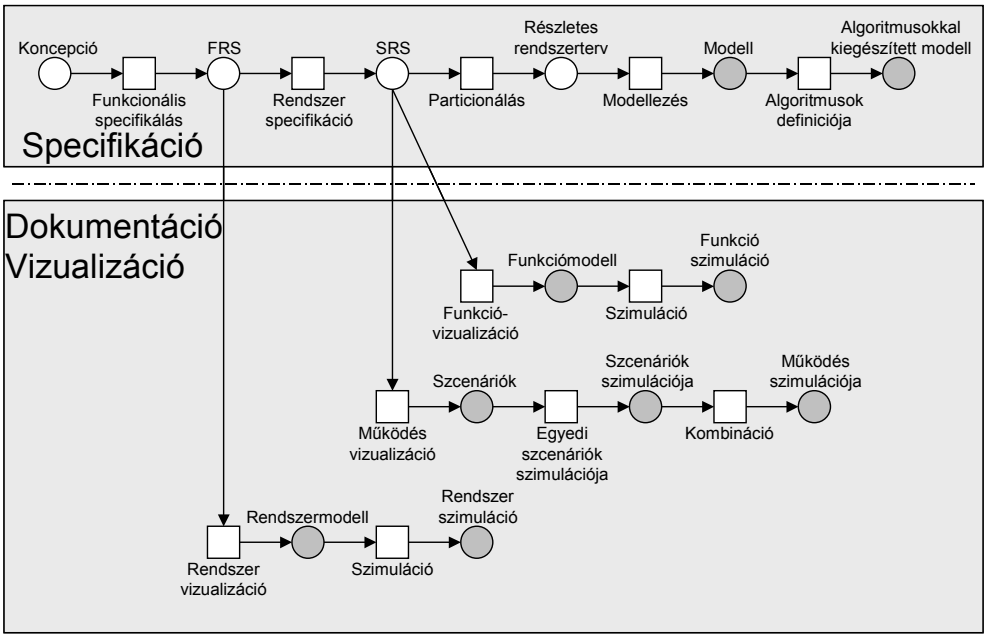
Cél	Formális specifikáció elemzése, funkcionális szimuláció
Leíróeszköz	Színezett, hierarchikus Petri-háló
Támogatóeszköz	Design/CPN

A modellezés kiindulási pontja az ETCS szöveges specifikációi voltak. E dokumentumok különböző aspektusokból specifikálják a teljes rendszer, más és más az egyes dokumentumok célja, így együttesen egy olyan követelményrendszert alkotnak, amelyet hivatkozások és kereszthivatkozások szőnek át. Ezért a specifikációs munka utolsó fázisaként, az implementáció előtt, meg kellett vizsgálni

- a követelményrendszer konzisztenciáját,
- a specifikált rendszer működőképességét, továbbá, hogy
- a rendszer megfelel a különböző vasutak üzemi elvárásainak.

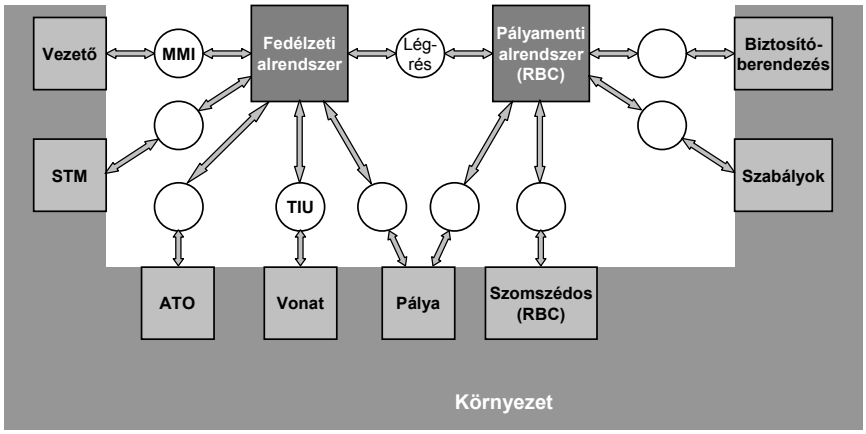
E vizsgálatok elvégzése céljából a rendszer Petri-hálókon alapuló formális modelljét alkották meg. A modell elkészítéséhez leíróeszközként színezett, hierarchikus Petri-hálókat alkalmaztak. A Petri-hálók mellett szólt, hogy azok valamennyi fejlesztési fázisban használhatók, támogatják különböző módszerek és a formális analízis alkalmazását. A modellezés számára olyan, az esemény és adat orientációt egyesítő módszert alkalmaztak, amely a rendszert az egyes Petri-háló szinteken különböző szempontok szerint képezi le. A modellezési és az analízis feladatok támogatására a Design/CPN szoftvert használták.

A modellezés két irányban folyt. Az egyik irány a rendszerfejlesztést szolgáló modellek kialakítása volt, a másik irány pedig a dokumentációs, illetve vizualizációs célú modellek fejlesztése (26. ábra). A két irányt azért volt érdemes különválasztani, mert a rendszerfejlesztés céljait szolgáló, ún. specifikációs modellek feleslegesen részletezettek a dokumentációs és vizualizációs célokhoz.



26. ábra. Specifikációs, dokumentációs és vizualizációs célú modellezés [Mey98a,b]

A teljes modell három részből tevődik össze: a fedélzeti rendszer és a pályamenti rendszer modelljéből, valamint egy erősen egyszerűsített környezeti modellből (27. ábra). A környezeti modell tartalmazza mindazon rendszerek modelljét, amelyek a rendszerhez annak illesztőfelületein keresztül csatlakoznak. A modell számszerű jellemzői a 6. táblázatban láthatók.



27. ábra. A modell három alapvető összetevője [Mey98a,b]

6. táblázat. A modell számszerű jellemzői [Mey98b]

	Fedélzeti alrendszer	**Pályamenti alrendszer (RBC)**	**Környezet**
Hálók száma	75	87	6
Hálóelemek száma	1,075	1,411	97
Helyek	734	954	65
Tranzíciók	341	457	32
Hierarchia szintek	7	7	3
Kód (sor, beleértve a commenteket)	15,500	12,500	0

Az alkalmazott modellezési megközelítés az egyes rendszerkomponensek bizonyos szcenariókhoz tartozó állapottér-elemzését teszi lehetővé, azaz, hogy az egyes komponensek milyen állapotváltozással reagálnak bizonyos bemenetekre, illetve bemeneti szekvenciákra. Egy adott komponens teljes viselkedési vizsgálata az adott modellezési megközelítés mellett nem lehetséges. Az említett állapottér-elemzés alkalmazásával sikerült feltárni egy, az eredeti, szöveges követelményrendszerben lévő kétértelműséget.

5.2.2.3. [Cic99] egy vonali biztosítóberendezés Z nyelvű specifikációs modelljét készíti el. A modell segítségével formális FMEA (Failure Mode and Effect Analysis) vizsgálatot lehet végezni.

Cél	FMEA vizsgálat támogatása formális modellel
Leíróeszköz	Z
Támogatóeszköz	Nincs adat

Az alkalmazott módszer a következő lépésekből állt:

1. Specifikáció: objektumorientált modellezési eljárással formális specifikációt állítanak elő.
2. Validáció: az előállított specifikációt analizálják és ellenőrzik a helyességét.
3. Formális specifikáció-analízis: típuskonzisztencia, szintaktikai helyesség, típus-definiálások, függvények stb.
4. A modell finomítása: a modellezést lépcsőzetesen, egyre finomabb felbontással, azaz egyre részletezettebben, egyre alacsonyabb absztrakciós szinten készítik el.

Az FMEA vizsgálatok a modell legrészletezettebb absztrakciós szintjén végezhetők el. Az egyes komponensek hibáinak következményeit végig lehet követni a modellen, és formálisan vizsgálható, hogy egy adott komponenshiba a legmagasabb szinten specifikált biztonsági követelményeket megsérti-e.

Meg kell jegyezni, hogy egy vonali biztosítóberendezés önmagában is jóval egyszerűbb, mint egy állomási berendezés, de még ezt az egyszerűbb működést is jelentősen absztrahálják a szerzők. Ugyanakkor a modell azért értékes, mert a modellezett rendszer belső, ún. strukturális biztonságával foglalkozik, a rendszer hibaviselkedését vizsgálja.

5.2.2.4. [Rei00a, Rei00b] a formális modellt hibafaelemzés támogatására használja.

Cél	FTA vizsgálat támogatása
Leíróeszköz	Statechart
Támogatóeszköz	Statemate

Egy rádiós alapú útátjáró biztosító berendezés formális modelljét készítették el a Statemate toolt alkalmazva. A Statemate tool kétféle leírást támogat: *aktivitás-diagramokkal (activity chart)* lehet a rendszer struktúráját, és az egyes komponensek közti adatcserét leírni, az *állapottérképekkel (statechart)* pedig az egyes komponensek funkcionális működését lehet leírni állapotok és állapotátmenetek formájában. Az ilyen módón felállított formális modellt a rendszer hibafájának manuális elkészítése során a rendszer működésének jobb megértéséhez használható (a Statemate toolról *lásd még* 5.2.1.5.).

5.2.2.5. [Mal99] egy olyan modellezési eljárást mutat be, amelynek során egy vasútállomás biztosítóberendezésének működését szimulálják.

Cél	Vasútállomás biztosítóberendezésének modellezése az állomás kapacitásanalízise céljából
Leíróeszköz	Petri-háló
Támogatóeszköz	Nincs adat

A modellezést objektumorientált módon végzik, az egyes külsőtéri objektumoknak megfelelően. Minden egyes objektumhoz elkészítik az objektum működési modelljét Petri-hálókkal. Ebben reprezentálják az egyes fizikai és logikai állapotokat, illetve az állapotátmenetek feltételeit. Az egyes objektumok közti kapcsolat a külsőtéri elemek topográfiai kapcsolatain alapul. Egy teljes állomás hálózata ilyen módon igen nagy Petri-hálóval írható le (egy közepes állomás – 4 vágány, 14 váltó modellezéséhez kb. 1500 csomópont és 3100 kapcsolat szükséges).

A modell alkalmazásához előzetesen meg kell határozni az állomás vágányhálózatát, és a lehetséges vágányutakat, és az azokban érintett objektumokat. Az egyes objektumok működését leíró al-hálók azonban már általánosak. A modellt az állomás, illetve a biztosítóberendezés kapacitásának modellezésére használják. Az egyes vágányok foglaltságának idődiagramját készítik vele el. Ez az elemzés az állomások tervezésére során használható fel előnyösen.

Vasúti biztosítóberendezések formális modellezésével és analízisével foglalkozik a fentieken kívül [Bas94, Bas95, Han94a, Han94b, Han94c, Han98, Mor91, Mor93, Nel96].

5.2.3. Biztosítóberendezés formális verifikációja

5.2.3.1. A [Lin00]-ben bemutatott modellezési eljárás célja annak formális bizonyítása, hogy a modellezett biztosítóberendezési rendszer kielégíti a funkcionális biztonsági követelményeket.

Cél	Biztonsági követelmények kielégítésének formális bizonyítása.
Eljárás	A biztosítóberendezés (beleértve a külsőtéri objektumokat) működésének, valamint a vonatforgalomnak a modellezésével, és a biztonsági követelmények formális meghatározásával, a biztonsági követelmények teljesítésének formális verifikációja.
Eszköz	RAISE

A modellezett rendszer a DSB (Dániai Államvasutak) által alkalmazott számítógép alapú biztosítóberendezése. A modellezéshez a következő megközelítést alkalmazták:

1. A vonatforgalom és a biztosítóberendezés modelljének felállítása.
   Az elkészített modell két alapvető részből tevődik össze: a fizikai, külsőtéri elemek (váltók, jelzők stb.) leírása, és a külsőtéri elemeket vezérlő mechanizmusok leírása, ideértve a vonatmozgások és a biztosítóberendezés működésének szabályait, ún. protokollok formájában.
2. A funkcionális biztonsági követelmények formális meghatározása.
   A funkcionális biztonsági követelményeket olyan magas absztrakciós szinten határozták meg, amely lehetővé teszi a követelmények helyességének és teljességének egyszerű vizsgálatát.
3. Annak formális bizonyítása, hogy a modellezett működés (beleértve a vonatforgalmat és a biztosítóberendezés működését is) kielégíti a biztonsági követelményeket.

Mindehhez a RAISE formális módszert alkalmazták. A vizsgálat eredményéről a szerzők nem számolnak be.

A bemutatott modellezési eljárás előnye, hogy nem egy adott állomás működését vizsgálja, hanem az egyes objektumok működési szabályai alapján egy berendezéstípus vizsgálatát végzi el. Az bemutatott modell komoly hátránya, hogy az elemek funkcionalitását, a vonatforgalom lebonyolódását, illetve a biztosítóberendezés működési szabályait tekintve olyan redukciókat alkalmaz, amelynek eredményeképp a modell nagyon távol áll a valóságtól.

5.2.3.2. [Har00] az Ansaldo Transporti által kifejlesztett elektronikus biztosítóberendezési rendszeren elvégzett vizsgálatokról számol be. A bemutatott biztosítóberendezési rendszer

(ACC) központi logikáját (SL) egy nagyon egyszerű konfigurációt feltételezve vetették alá formális verifikációs vizsgálatnak.

Cél	Elektronikus biztosítóberendezés egy részének biztonsági analízise
Eljárás	Modell ellenőrzés; a modell állapotainak vizsgálatával kvalitatív (például élőség, biztonság) és kvantitatív (időzítés) vizsgálatok elvégzése
Eszköz	Verus tool

Ehhez először a vizsgálandó központi, ún. biztonsági logika működésének formális modelljét készítették el a Verus tool, C programozási nyelvhez hasonló, formális specifikációs nyelvén. E nyelv különlegessége, hogy lehetővé teszi időzítési működések formális leírását is.

A Verus tool az így leírt modellből egy olyan véges számú állapotot reprezentáló állapotgráfot generál, amelynek állapotait a modell összes változóinak egy-egy állapota definiálja. A modellen, annak a fentiek szerint generált állapotterén ellenőrzendő kvalitatív és kvantitatív (időzítési) jellegű tulajdonságokat CTL-, illetve RTCTL-formulaként adták meg a Verus toolnak, amely azután a modell teljes állapotterét bejárva megvizsgálja a megadott tulajdonságok meglétét.

Az eljárás alkalmazása esetén még egy kifejezett kis konfiguráció (egy sorompó és egy tolatás processz, és az ezeket összefogó központi feldolgozás) esetén is relatíve nagy a modell állapottere (10^{27}). Igaz, hogy ennek a méretű modellnek a vizsgálata még nem jelent problémát, de kérdés, hogy egy valós életbeli konfiguráció állapottere kezelhető-e a tool segítségével (*lásd még* 7.1.2.2).

5.2.3.3. [Cim98] szintén a fenti rendszer, ugyancsak modellellenőrzésen alapuló vizsgálatát mutatja be. A modellezendő feladatot ebben az esetben a PROMELA modellezési nyelven írták le. A vizsgálandó modelltulajdonságok meglétének ellenőrzését a SPIN tool segítségével végezték el. Az ellenőrzés során sikerült a logikában egy hibás működést felfedezni.

Cél	biztonsági logika analízise, állapottérbejárással
Eljárás	Modellellenőrzés
Eszköz	SPIN (model checker), Promela modellezési nyelv

5.2.3.4. A Svéd Vasút 1978 óta több mint 130 elektronikus biztosítóberendezést helyezett üzembe [Eri96, Eri98, Pet98, Eri97a, Eri97b, Eri99]. Ezek a berendezések nyomvonal-elvűek, szabványos modulokból épülnek fel. Ezeknek a moduloknak a helyességét hagyományos és formális technikák kombinációjának segítségével igazolták. A modulok stabilak, nagyon ritkán változnak, ezért elég nagy ráfordítások voltak megengedhetők a modulok vizsgálatánál. A vizsgálatok elvégzése kapcsán azt állapították meg, hogy az elektronikus biztosítóberendezések helyes működésének vizsgálata sokkal nagyobb ráfordítást igényel, mint a hagyományos, jelfogós berendezéseké. Ezért 1995-ben a Svéd Vasút kezdeményezte, hogy a svéd funkcionális biztosítóberendezési követelményeket formálisan fogalmazzák meg. A cél az volt, hogy a tervezés-felülvizsgálati munka gyorsaságát és minőségét javítani lehessen. Ezenfelül az implementált szoftver formális verifikációjának elvégzése is a tervek között szerepelt. A formális specifikációs eljárás számos hibát tárt fel a biztosítóberendezési logikában, ezáltal maga a formális leírás is javította a biztosítóberendezési logika minőségét.

A specifikáció csak a funkcionális biztonsági követelményeket foglalja magába (a belső biztonsági követelményeket nem). A specifikáció leírására elsőrendű predikátum logikát

alkalmaztak megfelelő számítógépes támogatással, amely szimulációs lehetőséget is biztosított.

A specifikáció formalizálásának helyességét (a specifikáció validációja) több módon vizsgálták. Egyrészt szimulálták a formálisan leírt biztosítóberendezési működését, és a szimuláción vizsgálták, hogy a működés kielégíti-e a biztonsági követelményeket. Másrészt a formális specifikációt „visszafordították" természetes nyelvű szöveggé, és ezt a „fordítását" a vasút szakemberei vizsgálták és jóváhagyták.

Cél	Funkcionális biztonsági követelmények teljesítésének formális verifikációja.
Eljárás	Formális specifikáció, annak validációja, majd formális verrifikáció.
Eszköz	Elsőrendű predikátum logika a leíráshoz, CVT tool (Logikkonsult NP AB)

A formális verifikáció esettanulmánya számára a Brunna állomáson működő jelfogós biztosítóberendezést választották ki. A formális verifikáció során feltártak egy biztonság-kritikus tervezési hibát, melyet az adott, és további 20-30 hasonló konstrukciójú állomáson kijavítottak [Eri99].

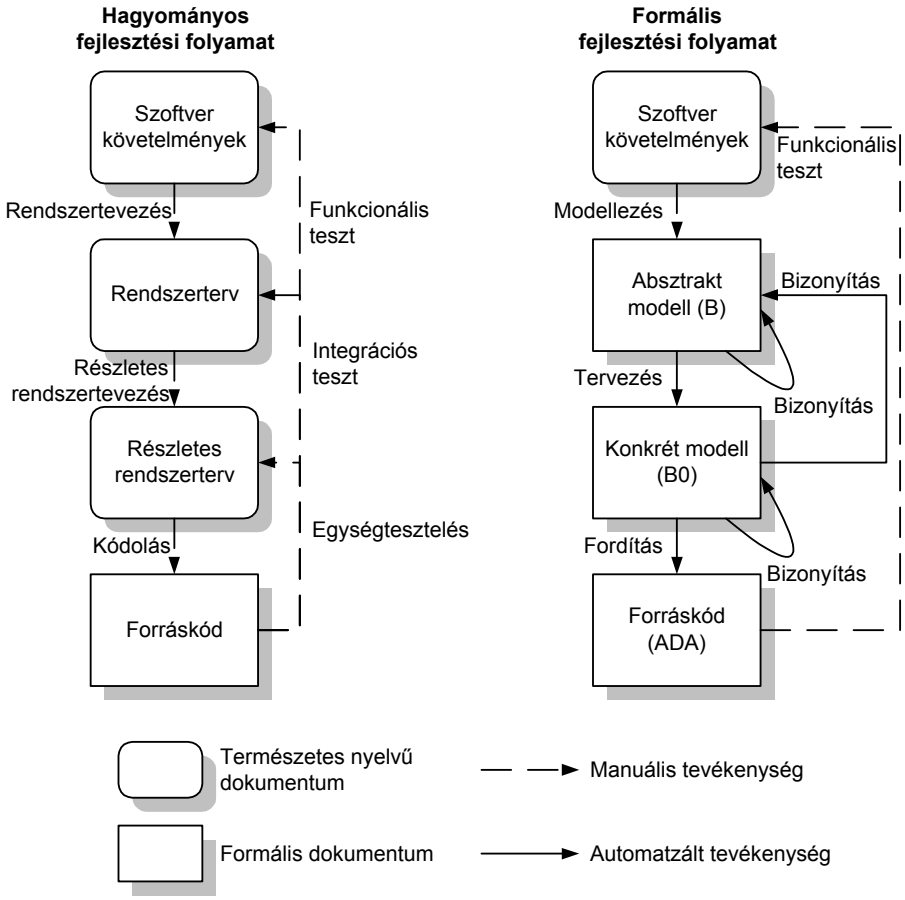
A vasúti biztosítóberendezések verifikációs problémáival foglalkozik továbbá [Ans95, Ber96, Can97, Cul93, Cul90, Cul89, Gro95, Gui84, Ing98, Ing95, Ing92, Mon95, Pet98, Pet97, Roa98, Vli98].

5.2.4. Biztosítóberendezési szoftver fejlesztése

5.2.4.1. A Matra Transport International (MTI) cégnél a formális módszerek alkalmazása a 80-as évek elején kezdődött egy városi vasúti automatikus elektronikus vonatirányító rendszer (SACEM) kapcsán, mégpedig a felügyeleti hatóság szorgalmazására. Ennél a projektnél a szoftverrel szemben támasztott követelményeket formálisan is megfogalmazták, a szoftver kódját Modula-2 programozási nyelven készítették el. A kész programot és a formális követelményrendszert részben automatizált, részben manuális vizsgálatok során hasonlították össze.

Cél	Biztosítóberendezési szoftver formális fejlesztése
Eljárás	A feladat formális specifikációja, a formális specifikáció elemzése, a helyesség formálisan bizonyítása, automatikusan kódgenerálás.
Eszköz	B-módszer

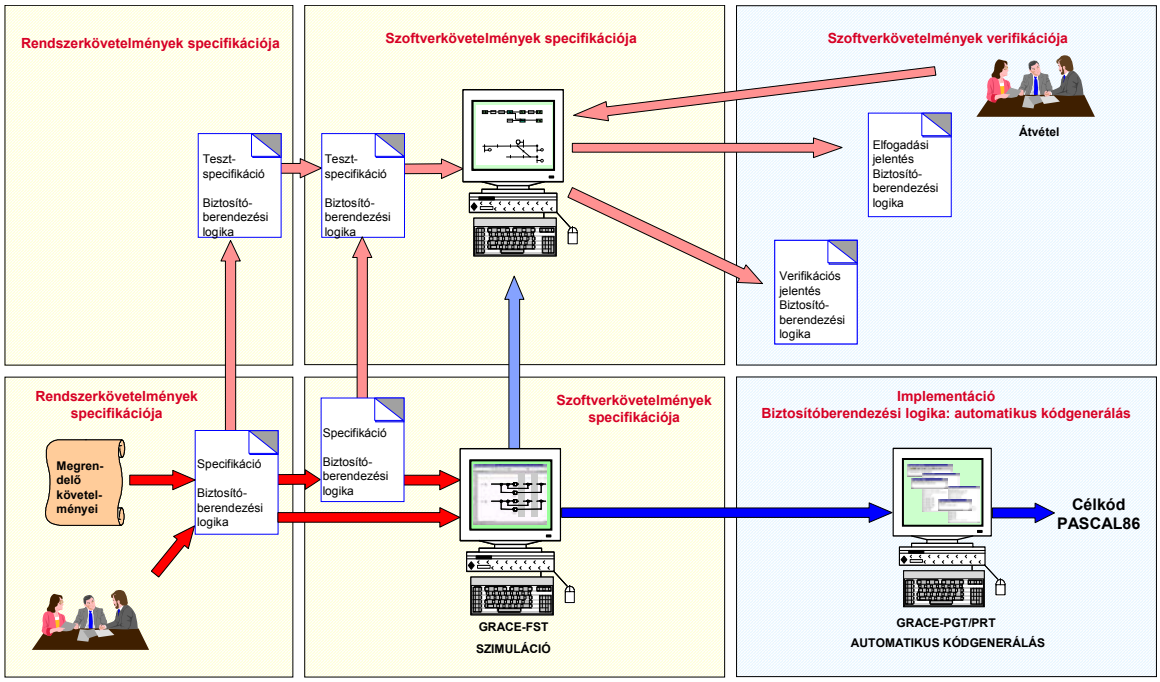
A Météor automatikus, vezető nélküli földalatti vasútját irányító rendszer esetében a Matra cég a B formális módszer alkalmazását választotta (28. ábra). E projekt esetében a követelmények megfogalmazása a B formális nyelv segítségével történt. A teljes tervezési, fejlesztési folyamat formálisan történt, a formális specifikációból kiindulva. Ezáltal a kód nagy része bizonyíthatóan helyes formában került kialakításra, és kb. csak a szoftver 10%-a esetében volt szükség manuális validáció elvégzésére [Fes99, Bur00, Süt00, Beh98].



28. ábra. Az MTI cégnél alkalmazott formális fejlesztési folyamat [Süt00]

5.2.4.2. A GRACE a Siemens AG Közlekedéstechnika Ágazata által kifejlesztett fejlesztőrendszer, amellyel a vasúti biztosítóberendezések felhasználóspecifikus részének feldolgozási logikája egyértelműen, ellentmondásmentesen és teljességben bemutatható, ábrázolható és olyan könnyen értelmezhető, mint egy jelfogós kapcsolás [Red99]. A középpontban a felhasználó által igényelt feldolgozási logika grafikus, formális megjelenítése áll. Az áramutas leíráshoz hasonló leíróeszközzel definiált funkciók szimulálhatók, és így tesztelhetők. Amennyiben a tesztelés, a megrendelővel történő egyeztetés eredménye pozitív, akkor a leírás automatikusan a biztosítóberendezés szoftverének cél-kódjává fordítható.

Cél	Biztosítóberendezési szoftver formális fejlesztése
Eljárás	Az informális követelmények formalizálása (grafikus funkcióleírás). A leírt funkciók szimulációja validáció céljából. A grafikus funkcióleírásból automatikus kódgenerálás verifikált eszköz segítségével.
Eszköz	GRACE (saját fejlesztésű eszköz)



29. ábra. A Siemens GRACE fejlesztőrendszere [Red99]

5.3. Összefoglaló értékelés

Az előzőekben bemutatott alkalmazási példákat két rendszer szerint, a 3. fejezetben kidolgozott Alkalmazási szempontrendszer, illetve a 4. fejezetben bemutatott és kiegészített Követelménykatalógus szerint értékeljük.

A részletes értékelések alkalmazásonként két-két táblázatban (az Alkalmazási szempontrendszer, illetve a Követelménykatalógus szerint), az 1. függelékben találhatók. Az összefoglaló értékeléseket a 7., illetve a 8. táblázat tartalmazza.

Az *Alkalmazási szempontrendszer* szempontjai közül meglévő alkalmazások értékelésére a következő szempontokat érdemes figyelembe venni:

- szigorúság;
- terjedelem
  - az életciklus szerint,
  - funkcionalitás szerint,
  - komponensek szerint,
  - az érintettek köre szerint;
- műszaki szempontok:
  - méret,
  - jelleg,
  - eszköztámogatottság.

A szempontrendszer további szempontjai új alkalmazások esetén útmutatóak, meglévő alkalmazások értékelésére nem kifejezetten alkalmasak.

Az értékelés során a *Követelménykatalógusban* szereplő követelmények közül azoknak a követelményeknek a teljesítését vizsgáltuk, amelyek kifejezetten az alkalmazott formális módszerre, illetve annak alkalmazására vonatkoznak, a rendszerfejlesztés módjára vonatkozó követelmények teljesülését nem vizsgáltuk.

A két értékelési rendszert vizsgálva megállapítható, hogy a Követelménykatalógus „Átjárhatóság” pontja, és az alkalmazási szempontrendszer „Terjedelem az életciklus szerint” pontja tulajdonképpen azonos tartalmú. A további szempontok a két rendszernél eltérő tartalmúak, bár találhatók közöttük összefüggések. Így például ha a Követelménykatalógus értékelése szerint formális verifikációt végeznek egy adott alkalmazásban, akkor ugyanannál az alkalmazásnál az Alkalmazási szempontrendszer „Terjedelem a funkcionalitás szerint” pontjánál „Helyességbizonyítás” (H) bejegyzést találunk.

5.3.1. Az alkalmazási szempontrendszer szerinti értékelés

Szigorúság: az elemzett alkalmazási példák *2-es,* illetve *3-as szigorúsági szintű* formális módszereket alkalmaznak.

Az életciklus szerinti terjedelmet vizsgálva azt látjuk, hogy a specifikációt célzó alkalmazások szinte mindegyike a *vasúti feltétfüzet formalizálásával* foglalkozik. Látható továbbá, hogy a gyártó cégek számára az automatikus kódgenerálásnak van kiemelt jelentősége.

Az alkalmazások túlnyomó többsége (beleértve a helyességbizonyítással foglalkozókat is) a biztosítóberendezési rendszerek alapfunkcionalitásával, azaz a *biztosítóberendezési logikával* foglalkoznak.

Az is jól látszik, hogy a formális módszereket túlnyomórészt a rendszer *szoftverkomponenseinek* fejlesztése során alkalmazzák. A hardver leírását célzó formális módszer alkalmazások esetében mindig az implementáció vizsgálatát végzik el.

Az *érintettek köre*: a vasúti feltétfüzet formalizálásával foglalkozó alkalmazások elvileg ugyan mind alkalmasak a vasút, a fejlesztő és a hatóság közötti kommunikáció elősegítésére, a bemutatott alkalmazások többségénél azonban a projektek során nem volt cél ilyen egyeztetések végrehajtása. Így valójában nem értékelhető, hogy az adott eljárás mennyire alkalmas a résztvevők közötti párbeszéd megkönnyítésére.

A formális módszerek ismert vasútbiztosítási alkalmazásainak többségére jellemző, hogy a modellezett feladat egy valódi biztosítóberendezési rendszer funkcionalitásához képest kicsi, terjedelmében és bonyolultságában is gyakran redukált. Megjegyezzük ugyanakkor, hogy még ilyen leegyszerűsített feladatok esetén is időnként hatalmas modellméretekkel, állapotterekkel találkozhatunk (*lásd még* 7.2.2. pont).

Az *alkalmazás jellege*: természetesen az összegyűjtött példák mindegyike a biztosítóberendezési rendszerek területéről származik.

Az alkalmazások *eszköztámogatottságát* tekintve azt mondhatjuk, hogy szinte minden alkalmazás igénybe vett valamilyen eszköztámogatást. Az alkalmazások közül ki kell emelni a GRACE rendszert [Red99], ahol a támogatóeszköz nem kereskedelmi szoftver, hanem a gyártó cég által kifejlesztett saját eszköz.

5.3.2. A Követelménykatalógus szerinti értékelés

Szemléletek: jól látható, hogy az alkalmazások elsődlegesen a biztosítóberendezési funkcionalitást célozzák meg. A teljesítményjellemzőkkel (beleértve a megbízhatóságot is) csak nagyon kevés alkalmazás foglalkozik.

A specifikáció formalizálását kitűző alkalmazások legtöbbje törekszik arra, hogy a formalizmus jól érthető, követhető legyen, vagy valamilyen módon (például szimulátor segítségével) támogatja az érthetőséget. Ugyanakkor a formális analízissel, illetve verifikációval foglalkozók nem tartják szem előtt az érthetőség szempontját. Ennek oka talán

az lehet, hogy a formális verifikációt célzó projektek többnyire kutatási projektek, ahol az érthetőség kisebb jelentőségű.

Ugyanez lehet az oka annak is, hogy a szabványoknak való megfelelés kérdése, továbbá a projektmenedzsment részfeladatai számára szolgáló interfész lehetősége csak a megvalósított biztosítóberendezési rendszerek fejlesztésével foglalkozó alkalmazások esetén merül fel.

Átjárhatóság: tartalmában azonos az Alkalmazási szempontrendszer szerinti értékelés „Terjedelem az életciklus szerint" pontjával.

Végrehajthatóság, *szimuláció*: az eddig ismert alkalmazások közül viszonylag kevés rendelkezik a végrehajthatóság, illetve a szimulálhatóság lehetőségével. Ugyanakkor például a GRACE rendszer (5.2.4.2.) esetében a szimuláció központi szerepet tölt be.

Verifikáció: a vizsgált alkalmazási példák többségénél a formális verifikáció nem volt kitűzött cél. Az alkalmazások kisebb hányadánál, a megvalósított biztosítóberendezési rendszerek fejlesztésénél (5.2.4.1, 5.2.4.2) azonban a formális verifikációnak nagy szerepe van, akár tényleges formális verifikáció formájában, akár egy verifikált eszköz alkalmazásával.

Validáció: a vasúti feltétfüzet formalizálását kitűző alkalmazások többnyire alkalmasak a validáció támogatására. A többi projekt esetében a célkitűzések között nem is szerepelt a validáció támogatása.

Teszt: érdekes megfigyelni, hogy formális verifikáció végrehajtása esetén az alkalmazások nem támogatják a tesztelést. Ennek oka az lehet, hogy a formális verifikáció csökkentheti a szükséges elvégzendő tesztek mennyiségét. A nem formális verifikációval foglalkozó alkalmazások többsége esetében támogatják a tesztelést.

A *kockázat- és veszélyelemzés* a formális specifikációt és formális analízist célzó alkalmazások körében támogatott.

A hagyományos specifikációs technikákkal való *kompatibilitásra* való törekvés elsősorban a formális specifikációt célzó alkalmazások körében figyelhető meg. Ugyanakkor például a GRACE fejlesztőrendszer (5.2.4.2) esetében e kompatibilitásnak az érthetőség miatt van nagy jelentősége.

7. táblázat. Vasúti alkalmazások értékelése az alkalmazási szempontrendszer szerint

	5.2.1. Formális specifikáció					5.2.2. Formális analízis					5.2.3. Formális verifikáció				5.2.4. Formális fejlesztés		
	5.2.1.1	5.2.1.2	5.2.1.3	5.2.1.4	5.2.1.5	5.2.2.1	5.2.2.2.	5.2.2.3	5.2.2.4	5.2.2.5	5.2.3.1	5.2.3.2	5.2.3.3	5.2.3.4	5.2.4.1	5.2.4.2	
Szigorúság	3	3	2	2	2	3	3	3	2	3	3	3	3	3	3	3	A számok a 3.1. fejezet szerinti szigorúsági szintet jelentik
Terjedelem az életciklus szerint	G	V	V	V	V	I	V	V	E	E	G	I	I	I	A	A	G: gyári feltétfüzet, V: vasúti feltétfüzet, I: implementáció, A: automatikus kódgenerálás E: egyéb
Terjedelem a funkcionalitás szerint	A	A	A	A	A	A, N	A	A, N	A	A	A, H	A, H	A, H	A, H	A, H	A	A: alapfunkcionalitás N: negatív rendszertulajdonságok vizsg., H: helyességbizonyítás
Terjedelem a komponensek szerint	SW	NÉ	NÉ	NÉ	NÉ	HW	NÉ	NÉ	NÉ	NÉ	SW	SW	SW	SW	SW	SW	SW: szoftver HW: hardver NÉ: nem értelmezhető
Terjedelem az érintettek szerint	F	V,F,H	V,F,H	V,F,H	V,F,H	F	V,F,H	NÉ	NÉ	V	NÉ	NÉ	NÉ	V,F,H	V,F,H	V,F,H	V: vasút/megrendelő, F: fejlesztő, H: hatóság NÉ: nem értelmezhető
Az alkalmazás mérete	1	2	1	1	1	1-2	2	1	1	1-2	2	1	1	2-3	2-3	3	1: kicsi, 2: közepes, 3: nagy
Az alkalmazás jellege	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B	B: biztosítóberendezési jellegű
Eszköztámogatottság	+	+	?	+	+	+	+	?	+	?	?	+	+	+	+	+	+: van –: nincs ?: nincs adat

8. táblázat. Vasúti alkalmazások értékelése a Követelménykatalógus szerint

	5.2.1. Formális specifikáció					5.2.2. Formális analízis					5.2.3. Formális verifikáció				5.2.4. Formális fejlesztés		
	5.2.1.1	5.2.1.2	5.2.1.3	5.2.1.4	5.2.1.5	5.2.2.1	5.2.2.2.	5.2.2.3	5.2.2.4	5.2.2.5	5.2.3.1	5.2.3.2	5.2.3.3	5.2.3.4	5.2.4.1	5.2.4.2	
Szemléletek	F	F	F	F	F	F+H	F	F+H	F	F	F	F	F	F	F+?	F	F: funkcionalitás, H: hibaviselkedés
Teljesítmény	–	–	–	–	–	+	–	+	+	–	–	–	–	–	?	–	+: támogatja, –: nem támogatja ?: nincs adat
Követhetőség	–	+	+	+	+	–	–	–	+	–	–	–	–	–	–	+	+: követhető, támogatja a megértést –: nehezen érthető
Átjárhatóság	G	V	V	V	V	I	V	V	E	E	G	I	I	I	A	A	G: gyári feltétfüzet, V: vasúti feltétfüzet, I: implementáció, A: automatikus kódgenerálás E: egyéb
Szabványok	–	–	–	–	–	+	–	–	–	–	–	–	–	–	–	+	+: támogatja –: nem támogatja
Interfészek	–	–	–	–	–	–	–	–	–	–	–	–	–	–	?	+	+: támogatja –: nem támogatja ?: nincs adat
Végrehajthatóság/ szimuláció	–	+	–	–	+	+	+	–	–	–	–	–	–	+	–	+	+: támogatja –: nem támogatja
Verifikáció	NÉ	NÉ	NÉ	NÉ	NÉ	NÉ	NÉ	NÉ	NÉ	NÉ	+	+	+	+	+	VE	+: formális verifikáció VE: verifikált eszköz NÉ: nem értelmezhető
Validáció	–	+	–	+	+	+	+	–	–	–	–	–	–	+	–	+	+: támogatja –: nem támogatja
Teszt	–	+	–	+	+	+	+	–	–	+	–	–	–	–	–	+	+: támogatja –: nem támogatja
Kockázat- és veszélyelemzés	–	+	+	+	+	–	+	+	+	–	–	–	–	–	–	–	+: támogatja –: nem támogatja
Kompatibilitás a hagyom. specifikációs. technikákkal	–	–	+	+	+	–	–	–	+	–	–	–	–	–	–	+	+: kompatíbilis a hagy. spec. techn. –: nem kompatíbilis

6. Jelfogókkal realizált logikai hálózat modellezése Petri-hálóval

A formális módszerek széleskörű elterjedésének egyik jelenlegi gátja a formális módszerek alkalmazásához, különösen a formális modellekhez használt matematikai jelölésrendszer bonyolultsága, nehéz érthetősége és követhetősége (*lásd* 3.6.3., [Bow93a, Tho95]). További problémát jelent, hogy a modellezéshez és a modellek analíziséhez szükséges módszerek alkalmazásához olyan magas szintű – elsősorban matematikai – felkészültségre van szükség, amely a gyakorló mérnökök számára jelenleg nem elérhető [Pat01]. Fontosnak tűnik ezért egy olyan kommunikációs lehetőség megkeresése, amelynek segítségével a formális specifikáció és az analízis eredményei a formális módszerek alkalmazásában nem jártas szakemberekkel is megvitathatók.

6.1. Mérnöki modell, matematikai modell

Az iparban viszonylag széles körben alkalmazott fél-formális specifikációs és rendszermodellezési technikák alapvető hátránya, hogy az általuk készült modellek a nem teljesen formális szemantika miatt kevéssé alkalmasak formális analízisek, formális bizonyítások végrehajtására. A megfelelő szemantikájú, így formális analízisek elvégzésére alkalmas modellek bonyolult matematikai jelölésmódja viszont alkalmatlanná teszi ezeket a modelleket a gyakorlati mérnöki munkában való alkalmazásra.

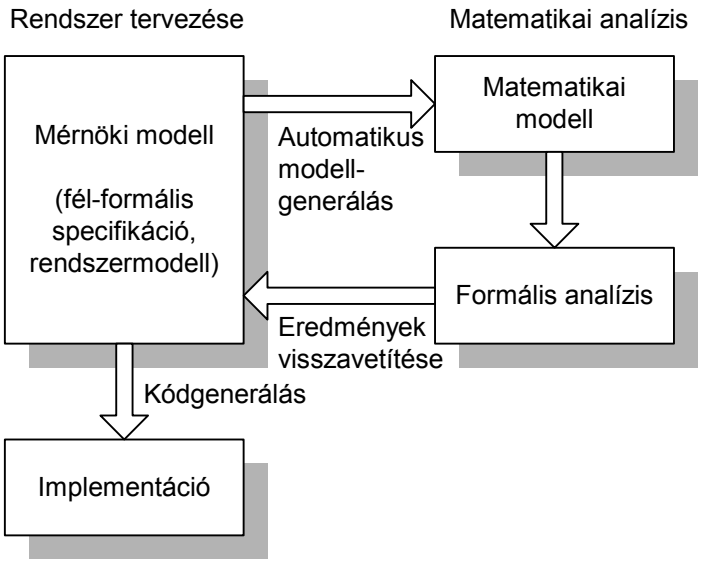
A fenti ellentmondás kiküszöbölésének egyik lehetséges módja a fél-formális *mérnöki modell* és a formális *matematikai modell* közötti transzformáció kifejlesztése. A transzformáció azonban több problémát is felvet [Pat99]:

- kérdés, hogy a mérnöki és a matematikai modell közötti konzisztencia megfelelő-e;
- problémát jelent az újramodellezés kérdése;
- kérdés, hogyan vetíthetők vissza a matematikai modellen elvégzett elemzések eredményei a mérnöki modellre.

E problémák kiküszöbölése érdekében a mérnöki és a matematikai modell közötti transzformáció automatikus végrehajtására van szükség (30. ábra). Ez irányban folytat kutatást az ún. HIDE (High-level Integrated Design Environment for dependability) projekt [Bon00, Bon01, MIT02, Var02]. Egyszerűen fogalmazva, a kutatás célja egy olyan fejlesztőkörnyezet létrehozása, amely a felhasználó elől elrejti a bonyolult matematikát.

A projektben az UML-t *(Unified Modelling Language)* alkalmazták mint fél-formális modellezési eszközt. Az UML az informatikai iparban széles körben alkalmazott, szabványosított, objektum-orientált, rugalmas modellezési eszköz, amely

- támogatja a funkcionális tervezés teljes folyamatát;
- többféle formalizmust foglal magában, amelyek segítségével a rendszer különféle tulajdonságai, viselkedése leírható;
- közel áll a mérnöki gondolkodásmódhoz;
- támogatja a hierarchikus modellezési, tervezési eljárást;
- lehetővé teszi modellek és tervek újrafelhasználását.



30. ábra. A mérnöki modell és a matematikai modell közötti transzformáció [Pat99]

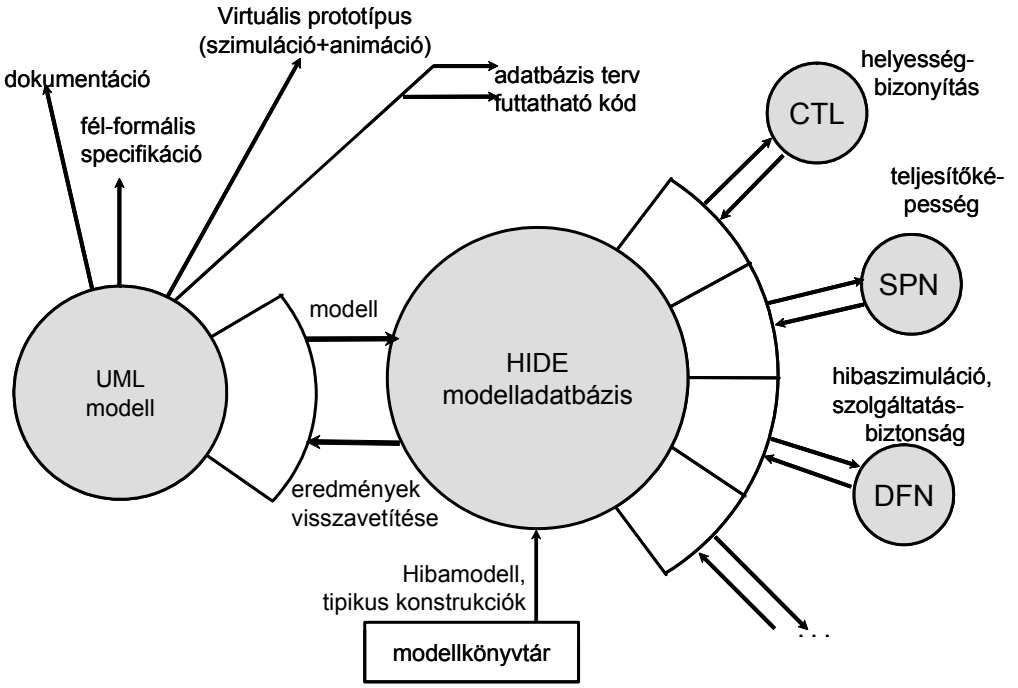
A fenti előnyök mellett az UML-nek komoly hátránya, hogy szemantikája nem teljesen formálisan definiált, ezért matematikai alapú analízisek nem végezhetők el az UML modelleken. Az UML modellezésnél a következő problémák fellépésével is számolni kell [Bon01]:

- a szokásos szimuláció alapú validáció (a rendszermodell és az eredeti követelmények konformitásának vizsgálata) által csak a helyesség nagy valószínűsége állapítható meg; nem *bizonyítható* a helyesség;
- az UML nem tartalmaz támogatást a megbízhatóság kvantitatív validációjának elvégzésére;
- a tisztán funkcionális specifikáció nem teszi lehetővé a rendszer hibaviselkedésének validációját.

A fenti hátrányok kiküszöbölésére a HIDE projekt keretében kialakított fejlesztőrendszerben az UML modellből (a különféle UML-formalizmusokkal leírt rendszertulajdonságok összességéből) egy központi modelladatbázist származtatnak. A központi modelladatbázis adatai alapján a rendszer különféle, teljesen formális matematikai modelljei (például időzített Petri-hálók) generálhatók, a különböző célú formális vizsgálatok elvégzéséhez. Ilyen vizsgálatok:

- formális verifikáció,
- megbízhatósági vizsgálatok,
- teljesítményelemzés és
- egyéb elemzések.

A formálisan végrehajtható vizsgálatok eredményei természetesen visszavetíthetők az eredeti, UML modellbe is. A teljes HIDE struktúráját a 31. ábra mutatja.



31. ábra. A HIDE fejlesztőkörnyezet struktúrája ([Bon01] alapján)

6.2. Mérnöki modellek a vasútbiztosítás területén

A *mérnöki és a matematikai modellek problematikája* a *vasútbiztosítás* területén is érvényes. A e területen tapasztalható erősen konzervatív szemlélet miatt a vasútbiztosítás szakterületének jellemző fél-formális leíróeszköze a jelfogós hálózatok leírási módjából származik. A jelfogós vasúti biztosítóberendezések leírására kialakított jelöléstechnikát így nemcsak a valóban jelfogókkal megépített biztosítóberendezések, illetve azok funkcióinak leírására alkalmazzák, hanem ugyanilyen jelöléstechnikát alkalmaznak a *rendszerek terveinek különböző fázisaiban* is (például specifikációk, alapkapcsolások, kiviteli tervek). De van arra is példa, hogy egy *PLC-vel megvalósított alrendszer* funkcióit is a jelfogós biztosítóberendezési jelöléstechnikával írják le, megkönnyítve ezzel a fejlesztési folyamatban résztvevők közötti kommunikációt [Ság00b, Gör98].

A következő fejezetekben megvizsgáljuk, hogy a *Petri-háló* mint elterjedt modellezési leíróeszköz, mennyire alkalmas jelfogós technikával megvalósított vasúti biztosítóberendezési rendszerek leírására. Ehhez először röviden bemutatjuk a vasúti *jelfogós kapcsolástechnikát*, majd a definiáljuk az alkalmazott *Petri-hálót*. Ezután bemutatjuk a vasúti biztosítóberendezési logikához hasonló logikai rendszerek leírására szolgáló *szokásos Petri-hálós modellezési* eljárást, majd bemutatjuk, hogy egy példaként vett jelfogós *sorompó illesztő kapcsolás* hogyan modellezhető ezzel a technikával, és megmutatjuk, hogy hogyan elemezhetők ennek a modellnek bizonyos tulajdonságai.

Ezt követően javaslatot teszünk egy új, szintén Petri-hálón alapuló, jelfogós hálózatok modellezésére szolgáló technika alkalmazására. Bemutatjuk, hogy az iménti sorompó illesztő kapcsolás hogyan modellezhető és elemezhető a *javasolt eljárás* alkalmazásával. Végezetül *összehasonlítjuk* a két eljárást.

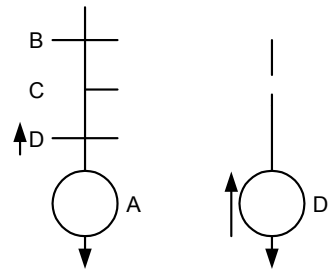
6.3. A jelfogós biztosítóberendezések és jelöléstechnikájuk

A ma is üzemelő biztosítóberendezések nagy része jelfogós technikával valósítja meg a vasúti biztosítóberendezésektől elvárt funkcionális és biztonsági követelményeket.

A biztonsági elvek a vasúti jelfogós berendezések esetében a valódi fail-safe biztonsági stratégián alapulnak. Ezt oly módon valósítják meg, hogy a berendezés kialakítása során olyan, ún. biztonsági jelfogókat használnak fel, amelyek aszimmetrikus meghibásodási tulajdonságúak. Ez azt jelenti, hogy van egy kitüntetett, a többi meghibásodási módnál nagyobb valószínűséggel bekövetkező meghibásodási mód, ez pedig a jelfogó ejtési jellegű meghibásodása[1].

A rendszerek biztonsági kialakítása során az aszimmetrikus meghibásodási hajlamot úgy használják ki, hogy a veszélyesebb üzemállapotokat a jelfogó fegyverzetének húzott állapotában záró érintkezők engedik meg, a biztonságos hibaállapotot (akadályozó állapot) pedig a jelfogó fegyverzetének ejtett helyzetében záró érintkezőkhöz rendelik. Fontos továbbá megjegyezni, hogy a jelfogó érintkezőinek kényszervezetése révén a jelfogó fegyverzetének állapota ellenőrizhető. A fenti biztonsági alapelvek a vasúti biztosítóberendezési technikában régre visszanyúló hagyományokkal bírnak, alkalmazásuk során rengeteg konstrukciós és üzemi tapasztalat gyűlt már össze.

A vasúti biztosítóberendezések által megkövetelt funkcionalitást a biztonsági jelfogók, illetve azok érintkezőinek felhasználásával tulajdonképpen egy logikai hálózat valósítja meg. Az ilyen jelfogós áramkörök dokumentálására a vasútnál speciális jelöléstechnika alakult ki. A jelfogók tekercsét az áramkörökben körök szimbolizálják (32. ábra, A tekercs), az ún. munkaérintkezőket (a jelfogó fegyverzetének húzott állapotában záró érintkezőket) a „vezetéken" keresztül húzott vonással (32. ábra, B érintkező), az ún. nyugalmi érintkezőket a „vezetéktől" jobbra húzott vonással (32. ábra, C érintkező) ábrázolják. Amennyiben egy jelfogó tekercsének áramköre a biztosítóberendezés alapállapotában zárt, akkor az adott jelfogó ún. alapállapotban húzott jelfogó; az ilyen jelfogókat tekercsük és érintkezőik neve mellett egy felfelé mutató nyíllal jelöljük (32. ábra, D jelfogó és érintkező). Az ilyen jelfogóknál a munka és a nyugalmi érintkezők jelölése fordított.



32. ábra A jelfogós áramkörök „vasúti" jelöléstechnikája

Bizonyos speciális célokra a jelfogós vasúti biztosítóberendezésekre szokás ún. *támasz-jelfogópárokat* alkalmazni. Az ilyen jelfogópárok egy alaphelyzetben húzott és egy alaphelyzetben ejtett jelfogóból állnak. Működésük annyiban tér el a hagyományos jelfogókétól, hogy egy mechanikus alátámasztás révén a pár bármely tagja csak akkor kerül ejtett helyzetbe, ha a pár másik tagja húzott állapotban van; azaz a pár egyik tagja az alátámasztás által mindaddig megtartja húzott állapotát – a jelfogótekercs gerjesztésének

[1] Fizikailag természetesen a jelfogó *fegyverzete* ejtett, illetve húzott állapotú, azonban az adott szakterületen elfogadott szóhasználat szerint a továbbiakban a *jelfogó* ejtett, illetve húzott helyzetére hivatkozunk.

megszűnése esetén is! – amíg a pár másik tagja meg nem húz. Ez a működésmód alkalmassá teszi a támasz-jelfogópárokat arra, hogy az utolsó állapotukat a tápfeszültség kiesése esetén is megőrizzék.

A jelfogós biztosítóberendezések funkcionális és biztonsági vizsgálata során a fent ismertetett jelöléstechnikával kialakított kapcsolási rajzok központi szerepet töltenek be. A berendezés életciklusa során a különböző biztonsági vizsgálatok, elemzések a különböző absztrakciós szintű, de azonos jelöléstechnikával készült kapcsolási rajzokon alapulnak.

A következő fejezetben bemutatjuk a modellezés alapjául szolgáló Petri-hálókat.

6.4. Az alkalmazott leíró eszköz: Petri-hálók

A modellezéshez leíró eszköznek a széles körben alkalmazott Petri-hálókat [Pet62] választottam. [Pat01] alapján a Petri-hálót a következőképpen definiáljuk: a *Petri-háló* strukturálisan egy olyan irányított súlyozott, páros gráf, amelynek két típusú csomópontja van: *hely* és *tranzíció*. Egy gráfban a helyek halmaza: P, a tranzíciók halmaza pedig T. A gráfbeli $e \in (P \times T) \cup (T \times P)$ élek helyeket tranzíciókkal vagy tranzíciókat helyekkel kötnek össze. Grafikusan a $p \in P$ helyeket körök, a $t \in T$ tranzíciókat vonalkák reprezentálják. Az élekhez *súlyokat* lehet rendelni; a súlyok nemnegatív egész számok lehetnek.

A Petri-hálók *állapota tokenek* segítségével írható le. A hálózatot a π komponensű *token eloszlás vektorral* írhatjuk le, ahol $\pi = |P|$ a hálózatban lévő helyek száma.

$$M = \begin{bmatrix} m_1 \\ \vdots \\ m_\pi \end{bmatrix}$$

E vektor *i*-edik m_i komponense az *i* helyen található tokenek számának felel meg. A Petri-háló kezdőállapotát a kezdő tokeneloszlás, M_0 definiálja. Grafikusan a tokeneket a helyeket reprezentáló körökbe rajzolt pöttyök ábrázolják.

A fentieknek megfelelően, a Petri-hálók formális definíciója a következőképpen foglalható össze:

Petri - háló :	$PN = (P, T, E, W, M_0)$
Helyek halmaza :	$P = \{p_1, p_2, \ldots, p_\pi\}$
Tranzíciók halmaza :	$T = \{t_1, t_2, \ldots, t_\tau\}$
	$P \cap T = \varnothing$ *és* $T \cap P = \varnothing$
Élek halmaza :	$E \subseteq (P \times T) \cup (T \times P)$
Súlyfüggvény :	$w^* : E \to N$
Kezdeti állapot :	$M_0 : P \to N$

Egy $n \in (P \cup T)$ csomópont $\bullet n$ *ősei* és $n\bullet$ *utódai* a következőképpen definiálhatók:

1. egy $t \in T$ tranzíció ősei a bemeneti helyei: $\bullet t = \{p \mid (p,t) \in E\}$
2. egy $t \in T$ tranzíció utódai a kimeneti helyei: $t\bullet = \{p \mid (t,p) \in E\}$
3. egy $p \in P$ hely ősei a bemeneti tranzíciói: $\bullet p = \{t \mid (t,p) \in E\}$
4. egy $p \in P$ hely utódai a kimeneti tranzíciói: $p\bullet = \{t \mid (p,t) \in E\}$

A Petri-háló dinamikus viselkedésében az állapotváltozások a tranzíciók *tüzelése* hatására jönnek létre. A tüzelés szabályai az alábbiak:

1. Egy $t \in T$ tranzíciót *engedélyezettnek* nevezünk, ha *t* minden egyes $p \in \bullet t$ bemenő helyén legalább $w^-(p,t)$ token van, ahol $w^-(p,t)$ a *p*-ből *t*-be vezető $e = (p,t)$ él $w^*(e)$ súlya, azaz:

$$\forall p \in \bullet t : m_p \geq w^-(p,t)$$

2. Egy engedélyezett tranzíció tetszése szerint tüzelhet, vagy nem tüzelhet, azaz működése *nem-determinisztikus*.
3. Egy engedélyezett $t \in T$ tranzíció tüzelése $w^-(p,t)$ darab tokent vesz el minden egyes $p \in \bullet t$ bemenő helyről és $w^+(t,p)$ tokent helyez el a tranzíció minden egyes $p \in t \bullet$ kimenő helyére, ahol $w^+(t,p)$ a *t*-ből *p*-be vezető él súlya.

Az élsúlyokat az ún. súlyozott szomszédossági mátrixban foglalhatjuk össze: $W = \|w(t,p)\|$. Ez a $\tau \times \pi$ dimenziójú mátrix minden egyes eleme azt fejezi ki, hogy *t* egyszeri tüzelésére mennyit változik a *p*-beli tokenszám:

$$w(t,p) = \begin{cases} w^+(t,p) - w^-(p,t) & \text{ha } (t,p) \in E \\ 0 & \text{ha } (t,p) \notin E \end{cases}$$

A fentiek szerint a *t* tranzíció egy tüzelésének hatására a kiinduló *M* állapotból a Petri-háló az $M' = M + W^T e_t$ állapotba megy át, ahol e_t a *t* tranzíciónak megfelelő egységvektor.

Az egyes tüzelések sorozatosan hajtódnak végre, azaz az állapotátmenetek egymást követő tüzelések útján valósulnak meg. A $\vec{\sigma} = \langle t_{i_1} \ldots t_{i_n} \rangle$ sorozatot *tüzelési szekvenciának* nevezzük, ha az abban szereplő összes tranzíció tüzelése kielégíti a tüzelési szabályt. Ebben az esetben az M_{i_n} állapotot M_{i_0} állapotból a $\vec{\sigma}$ tüzelési szekvencia által *elérhetőnek* mondjuk.

A Petri-hálók működésének nem-determinizmusát korlátozni lehet a *prioritás* fogalmának bevezetésével. A tranzíciókhoz rendelt prioritás azt jelenti, hogy az engedélyezett tranzíciók közül egy alacsonyabb prioritásszintű mindaddig nem tüzelhet, amíg engedélyezve van magasabb prioritású szintű tranzíció tüzelése.

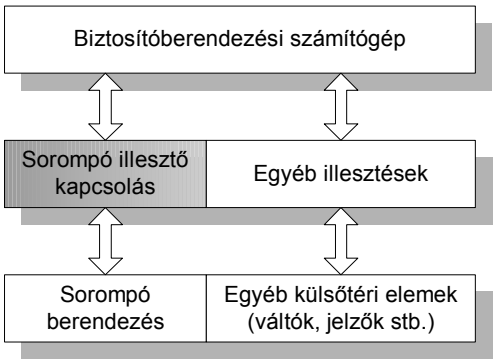
Bevezethető továbbá az egyes helyek *kapacitáskorlátja* is. Ekkor a tüzelési szabály azzal a feltétellel egészül ki, hogy a tranzíció egyetlen kimenő helyre sem tölthet több tokent, mint amennyi az adott hely kapacitása.

A továbbiak szempontjából fontos még a *tiltó élek* bevezetése. A tiltó élek arra szolgálnak, hogy egy-egy feltétel meg nem létét lehessen vizsgálni, vagy hogy egyes feltételek esetén egy működés *ne* hajtódjék végre. A tiltó élek esetén a tüzelési szabály úgy egészül ki, hogy egy *t* tranzíció tüzelése csak akkor engedélyezett, ha a *t* tranzícióhoz kapcsolódó bármely (*p*,*t*) tiltó él w(p,t) súlyánál kevesebb számú token van a bemenő helyén. A tiltó élek alkalmazásának fő hátránya, hogy számos analízis módszer a tiltó élekkel bővített Petri-hálókra már nem használható. A tiltó éleket a Petri-háló grafikus reprezentációjában az él végén lévő karikával jelölik: ——○ .

6.5. A modellezendő jelfogós illesztő kapcsolás

A modellezési technikák kialakításához és vizsgálatához egy jellemző jelfogós kapcsolást, egy elektronikus vasúti állomási biztosítóberendezéshez kapcsolódó sorompó berendezés jelfogós interfész kapcsolását választottam ki [Sie99].

A modellezendő sorompó illesztő kapcsolás parancsokat kap a biztosítóberendezési számítógéptől, ezek alapján, a külsőtéri elemek állapotának figyelembevételével és különböző funkcionális és biztonsági függések létrehozásával vezérli a sorompó-berendezés külsőtéri elemeit (sorompó fények, sorompó hajtóművek). Ezenfelül, a külsőtéri elemek fizikai és logikai állapotáról visszajelentéseket ad a biztosítóberendezési számítógépnek (33. ábra).

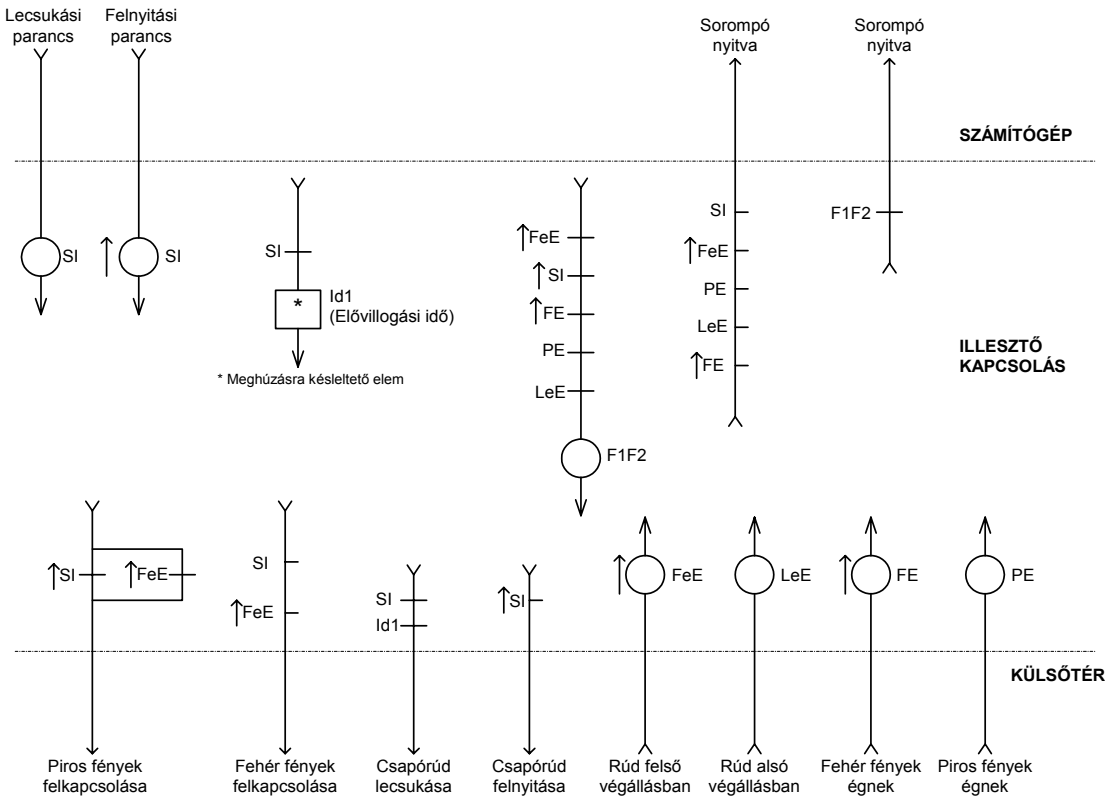


33. ábra. A sorompó illesztő kapcsolás [Sie99]

A modellezendő illesztő kapcsoláshoz a kiindulás az elvi kapcsolási rajz volt. Az eredeti elvi kapcsolást a modellezés számára egyszerűsítettem: csak az alapvető függőségek, visszajelentések és vezérlések kerültek modellezésre. Az egyszerűsített, azaz a modellezett kapcsolás rajza a 34. ábrán látható. A kapcsolásban alkalmazott jelfogók nevei a 9. táblázat szerint értelmezhetők.

9. táblázat. Jelmagyarázat a sorompó illesztő kapcsolásához

Név	**Elnevezés**	**Magyarázat**
SI, ↑SI	Sorompó indító	A sorompó vezérlését végző támasz-jelfogópár
Id1	Időzítő	A piros fények elővillogási ideje (meghúzásra késleltető jelfogó; a késleltetés jelenleg nem kerül modellezésre)
FeE	Fent ellenőrző	A csapórúd felső végállását ellenőrző jelfogó
LeE	Lent ellenőrző	A csapórúd alsó végállását ellenőrző jelfogó
FE	Fehér ellenőrző	A fehér fények meglétét ellenőrző jelfogó
PE	Piros ellenőrző	A piros fények működését ellenőrző jelfogó
F1F2	Függőség	A sorompó lezárt állapotának függősége teljesül

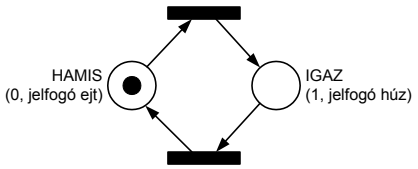


34. ábra. Az egyszerűsített sorompó illesztő kapcsolás áramkörei

6.6. Logikai hálózatok klasszikus modellezése

A fentiekhez hasonló logikai rendszerek leírása szokásosan a Petri-háló következő értelmezésével lehetséges (például [Yak98]): minden egyes logikai változót egy két helyből és két tranzícióból álló egyszerű hálóval modellezünk (35. ábra).

Esetünkben minden jelfogót egy-egy logikai változónak tekinthetünk. A két hely egyike felel meg a logikai változó *hamis* (0) értékének (a jelfogó ejtett helyzetének), a másik hely pedig a logikai változó *igaz* (1) értékének (a jelfogó húzott helyzetének). Ebben az egyszerű hálóban az egyetlen token holléte határozza meg a logikai változó aktuális értékét. Ezt a modellezési eljárást *állapotmodellezés*nek nevezzük.



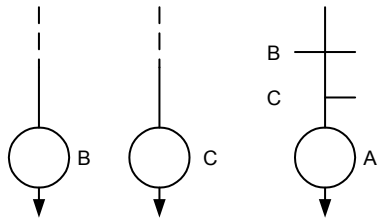
35. ábra. Logikai változók modellezése Petri-hálóval

A két állapotot jelképező helyek közötti tranzíciók különböző típusú megválasztása esetén különböző rendszertulajdonságok is modellezhetők:

- ha a tranzíciók determinisztikus, késleltetés nélküli tranzíciók, akkor a modell a jelfogós hálózat ideális (késleltetés- és hibamentes) működését ábrázolja;

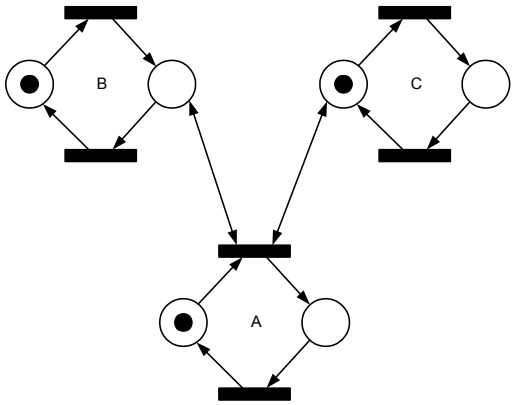
- amennyiben a tranzíciók valamilyen adott idejű, vagy sztochasztikusan változó késleltetéssel bírnak, akkor a modell a jelfogós hálózat tranziens viselkedését is reprezentálja;
- ha pedig a tranzíciók sztochasztikus jellegűek, akkor az adott jelfogó meghibásodási tulajdonsága is figyelembe vehető.

Természetesen a Petri-hálók ilyen értelmezésével a logikai változók közötti szokásos logikai műveletek ábrázolása is lehetséges. Tekintsük például az $A = B \cdot \overline{C}$ logikai *ÉS* műveletet. Ezt a logikai kapcsolatot a fenti jelfogós jelöléstechnikával a következőképpen ábrázolhatjuk (36. ábra).



36. ábra. Logikai műveletek ábrázolása jelfogós jelöléstechnikával

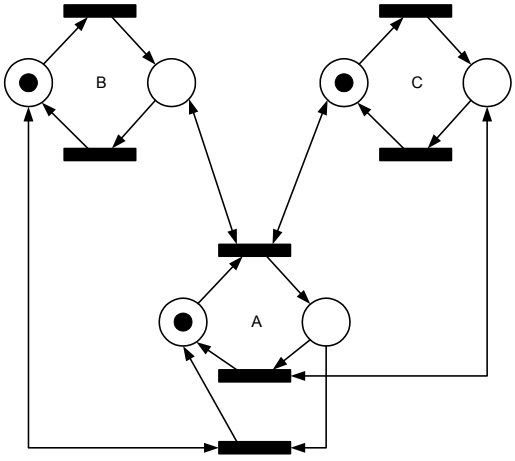
A Petri-hálós, állapotmodellezési eljárás szerint ekkor mindhárom logikai változónak (*A, B, C*) megfelel egy-egy egyszerű, 35. ábra szerinti háló (37. ábra). Az ábrán látható $\longleftrightarrow$ jelölésű élek ún. *lekérdező* vagy *tesztélek*. Valójában egy rajztechnikai egyszerűsítésről van szó: amennyiben egy p_i hely egy t_j tranzíciónak bemenő és kimenő helye is, azaz $p_i \in {}^\bullet t_j, p_i \in t_j {}^\bullet$, akkor a két él külön-külön jelölése helyett a fenti, mindkét végén nyíllal ellátott vonal jelölést alkalmazzuk. Az ilyen p_i helyeken lévő tokenek számát a t_j tranzíció tüzelése nem változtatja meg: $w^+(t_j, p_i) - w^-(p_i, t_j) = 0$



37. ábra. Logikai műveletek modellezése 1.

Látható, hogy az *A* logikai változó csak akkor veheti fel az igaz értéket, ha a *B* változó értéke *igaz*, a *C* változó értéke pedig *hamis*. A fentieknek megfelelően az *A* logikai változó értékének megváltozása nem változtatja meg a *B*, illetve a *C* változók értékét.

Akár az algebrai, akár a jelfogós jelölést tekintjük, egyértelmű, hogy ha a $B \cdot \overline{C}$ feltétel a továbbiakban nem teljesül, úgy az *A* változónak hamis értéket kell felvennie. A 33. ábrán látható háló azonban csak a következő kiegészítéssel modellezi ezt a működést (38. ábra).



38. ábra, Logikai műveletek modellezése 2.

A modellbe tehát be kell építeni az *igaz*-ból a *hamis* értékre történő változásnak (a jelfogó ejtésének) a feltételét:

$$\overline{A} = \overline{B \cdot \overline{C}} = \overline{B} + C$$

A kiegészítésben látható, hogy milyen módon lehet két változó logikai *VAGY* kapcsolatát modellezni. Az állapotváltozást ilyenkor több, egymástól független feltétel is kiválthatja, ezért az állapotváltozás annyi tranzíció tüzelésével mehet végbe (azok bármelyikén), ahány változó *VAGY* kapcsolatáról van szó (jelen esetben két független tranzíció).

6.6.1. A jelfogós sorompó illesztő kapcsolás állapotmodellezése

A fenti technikával az 6.5 szakaszban leírt kapcsolási rajz (amely tulajdonképpen egy logikai rendszert ír le) modellezése elvégezhető. A modellezés során a logikai kapcsolatok, műveletek az előző szakaszban részletezett módon írhatók le. A teljes rendszer modellezéséhez két további kiegészítésre van szükség:

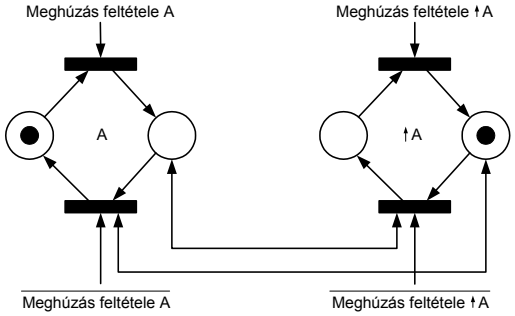
1. a kapcsolásban szereplő támasz-jelfogópár modellezése és
2. az illesztőkapcsolás külső kapcsolatainak modellezése.

A *támasz-jelfogópár* működésére utalva (ld. 6.3.) azt mondhatjuk, hogy a támasz-jelfogópár működése abban különbözik egy hagyományos jelfogóétól, hogy az ejtés csak akkor következhet be, ha a pár másik tagja húzott állapotban van. Ez a feltétel a jelfogó ejtésének egyéb feltételével (a húzás feltételének negáltjával) logikai *ÉS* kapcsolatban van. Ennek megfelelően egy támasz-jelfogópárt a következőképpen modellezhetünk (39. ábra).

A jelfogó-hálózat működésének vizsgálatához modellezni kell a hálózat *külső kapcsolatait* is, így a kapcsolás bemenő vezérlését, visszajelentését, valamint az illesztőkapcsolás által vezérelt külsőtéri elemek működését. A vezérlési állapotok modellezése egy-egy jelfogó modellezésével azonos módon képzelhető el, ugyanez vonatkozik a kapcsolás által a számítógépnek visszajelentett információra is.

A *külsőtéri elemeket* is hasonló módon lehet modellezni. A sorompó csapórúdjának egyszerű modellje szintén megfelel egy jelfogó modelljének (két hely, két tranzíció). A csapórúd akkor csukódik le, ha ilyen irányú vezérlést kap, és akkor nyílik fel, ha felnyitásra

utaló parancsot kap. Hasonlóképpen működnek a sorompó piros és fehér fényei; ezeknek be- és kikapcsolt állapota van.



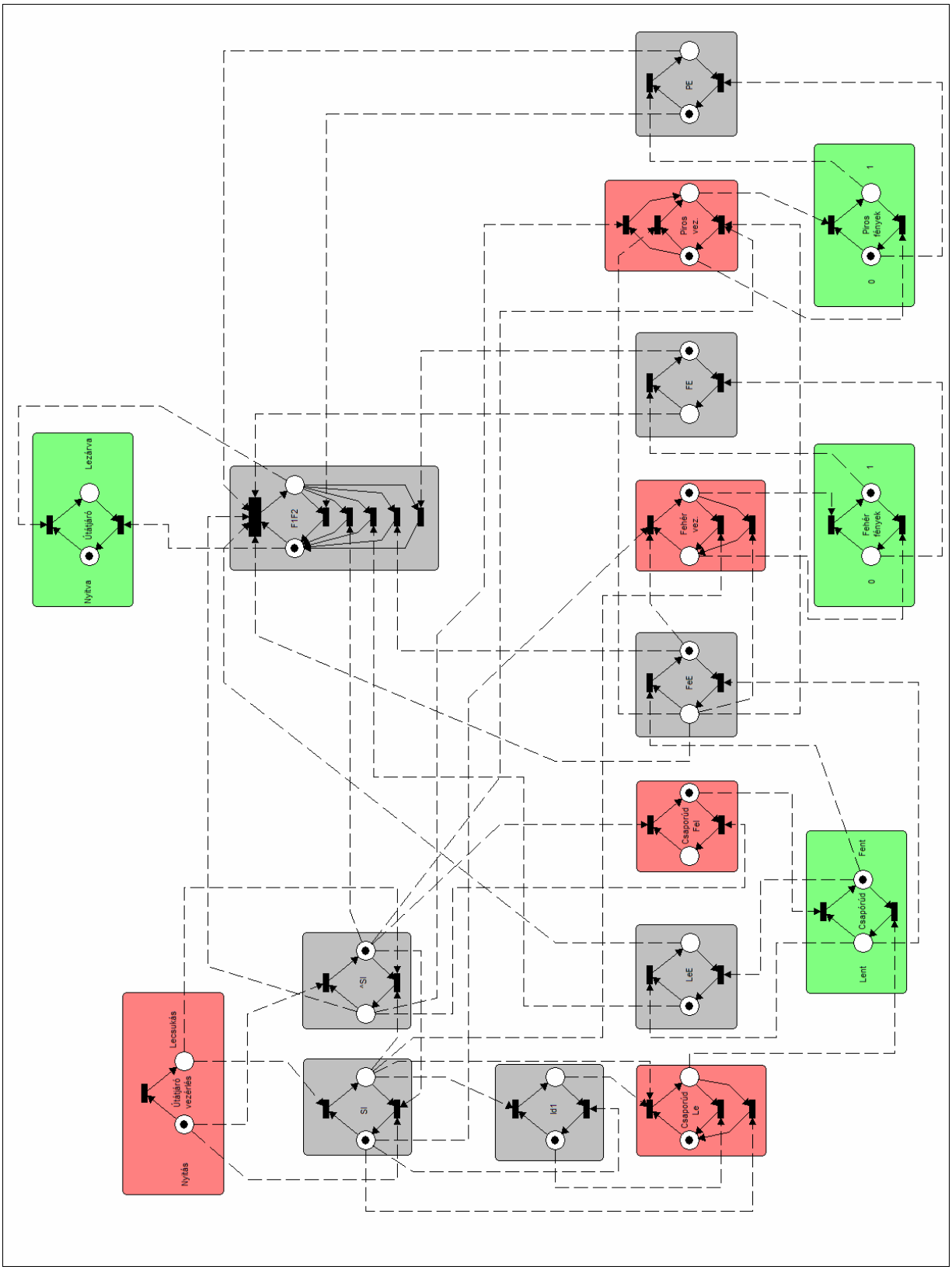
39. ábra. Támasz-jelfogópár állapotmodellezése

A külsőtéri elemek ilyen egyszerű modellezésével csak a normál, hibamentes működés modellezhető. Természetesen az egyszerű külsőtéri-elem modellek helyettesíthetők komplikáltabb, *hibaviselkedést* is tartalmazó modellekkel. Ekkor az is vizsgálhatóvá válik, hogy a jelfogós kapcsolás hogyan reagál a külsőtéri elemek hibás működésére.

Az 6.5. fejezetben bemutatott kapcsolás állapotmodellezés szerinti leírása a 40. ábrán látható. A modellben piros színnel vannak ábrázolva a vezérlések, szürkével az egyes jelfogók és zölddel a külsőtéri elemek, illetve a visszajelentések. Az ábrán a már említett lekérdező vagy tesztéleket szaggatott vonal jelöli. A modell összefoglaló adatai a következők:

Helyek száma:	34
Tranzíciók száma:	40
Élek száma:	176

A modellezéshez a HPSim (v. 1.1) Petri-háló editort és szimulációs programot alkalmaztam [HPSim].



40. ábra. A jelfogós illesztő kapcsolás állapotmodellje

6.6.2. A jelfogós kapcsolás állapotmodelljének analízise

A modellanalízis célja jelen esetben az, hogy a jelfogós hálózat funkcionális helyességét ellenőrizzük.

Tulajdonképpen azt vizsgáljuk, hogy előfordulhat-e olyan helyzet, amikor az illesztő kapcsolás azt jelzi az elektronikus biztosítóberendezésnek, hogy az útátjáró lezárt állapotban van, ugyanakkor a lezártságnak valamelyik feltétele nem teljesül (pl. a csapórudak nincsenek alsó végállásban, nem égnek a piros fények). Az ilyen *veszélyes állapotok* a Petri-hálóban egy-egy token-eloszlással írhatók le. A feladat tehát az, hogy megvizsgáljuk, hogy a kitüntetett M_0 kezdőállapotból elérhetők-e a veszélyes állapotok, azaz létezik-e olyan $\vec{\sigma}^*$ tüzelési szekvencia, amelynek hatására a háló az M_0 kezdőállapotból az M^*, általunk veszélyesnek minősített állapotba kerül.

A fenti vizsgálatot szimbolikus modell-ellenőrzéssel lehet végrehajtani. Az állapotmodellezési technikával előálló modell *korlátos*, sőt 1-*korlátos*, azaz *biztonságos* Petri-háló. Ez azt jelenti, hogy a tokenek száma a háló „működése” során egyetlen helyen sem haladja meg az egyet. Az ilyen tulajdonságú Petri-hálók állapotainak elemzésére mutat be eljárást [Pas01]. Az eljárás alapelve, hogy a biztonságos Petri-hálót egy Boole-algebrának fogja fel, amelyben minden egyes hely megfelel egy logikai változónak; a változók *igaz*, illetve *hamis* értékét pedig az adott helyen lévő, illetve nem lévő token jelzi. Ezzel a módszerrel vizsgálható a biztonságos Petri-háló teljes állapottere.

A [Pas01] által javasolt Petri-háló→Boole-algebra transzformációt felhasználó elérhetőségi analízis algoritmus [Ube02]-ben került implementálásra. A sorompó illesztő kapcsolás modellezésére is ezt az algoritmust alkalmaztam. (Az [Ube02]-ben implementált algoritmus bemenő adatként a DNANet nevű Petri-háló szerkesztő program [DNANet] formátumát igényli. Ezért a Petri-háló szerkesztésére használt HPSim és a DNANet programok formátumai közötti konverzió elvégzésére egy Pascal programot fejlesztettem ki.)

Példaként megvizsgáltuk azt az esetet, hogy az illesztő kapcsolás jelezheti-e a számítógépnek azt, hogy az útátjáró le van zárva, miközben a fehér fények égnek. (Ennek az állapotnak a fellépése természetesen nem kívánatos.) A hálózat M_0 kezdeti állapota megfelel a 40. ábrán jelölt hálóállapotnak. (A Petri-háló mátrixos ábrázolásmódja a 2. függelékben látható.)

$$M_0=[1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0]^T$$

A *keresett állapothalmaz* úgy írható le, hogy a fehér fényeket reprezentáló hálórészen a „0” jelű helyen nincs token, az „1” jelű helyen pedig van token, az útátjáró állapotát jelző hálórészen pedig a „Nyitva” jelű helyen nincs token, a „Lezárva” jelű helyen pedig van token, a többi hely tokenszáma pedig bármi lehet (ezeket az állapotvektorban X jelöli). A vizsgált tokeneloszlás vektor a következőképpen írható le:

$$M^*=[X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,X\,0\ 1\ X\,X\,X\,X\,X\,X\,X\,X\,0\ 1\ X\,X]^T$$

Az algoritmust lefuttatva megállapítható, hogy a fenti modellnek összesen *1178 állapota* lehetséges, amelyek között az M^* nem szerepel, azaz ez a *veszélyes állapot nem érhető* el. Természetesen egy kapcsolás tényleges vizsgálatához egynél több veszélyes állapot vizsgálata is szükséges lehet.

6.7. Áramutas modellezési eljárás

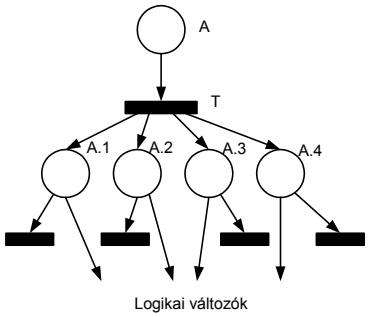
A klasszikus állapotmodellezési technikának megfigyelhetők bizonyos hátrányai. Ezek nagyrészt arra vezethetők vissza, hogy minden egyes logikai változó *hamis* → *igaz* értékváltozásának feltételén túl, a modellbe be kell építeni az *igaz* → *hamis* változás feltételét is. A logikai rendszerek hagyományos leírási módjaihoz képest (*például* algebrai alak vagy jelfogós jelöléstechnika) ez *redundanciának* tünik, ugyanis az ilyen rendszerekben az *igaz* → *hamis* átmenet feltétele *mindig* a *hamis* → *igaz* átmenet feltételének negáltja. (Ilyen módon természetesen a hagyományos leírások implicit módon tartalmazzák ezt a feltételt.)

Ezeknek a *ponált* feltételeken túli, ún. *negált* feltételeknek a modellezése egy jelfogós kapcsolás Petri-hálóvá való alakítása során azt jelenti, hogy olyan feltételeket is modellezni kell, amelyek az eredeti kapcsolásban explicit módon nem szerepelnek. Ez – látszólag feleslegesen – növeli a modell méretét, továbbá a modellezés során hibalehetőségeket okoz.

A *negált* feltételek beépítése a modellbe azzal a hátránnyal jár, hogy nehéz szétválasztani a ténylegesen modellezni kívánt kapcsolatokat és a modellezés *technikája* miatt szükséges kapcsolatokat.

Előnyös lenne tehát egy olyan modellezési technika alkalmazása, amely mentes a fent részletezett hátrányoktól, és további járulékos előnyökkel is jár, úgymint a könnyebb modellelkészítés és a működés valósághűbb modellezés. A következőkben egy ilyen, *áramutas modellezési technikára* teszünk javaslatot [Ság99a].

Reprezentálja egy jelfogó tekercsét és minden egyes érintkezőjét egy-egy *hely* a Petri-hálóban. Ilyen módon egy 4 érintkezős jelfogó modellje a következőképpen néz ki (41. ábra).



41. ábra. Jelfogó áramutas Petri-háló modellje

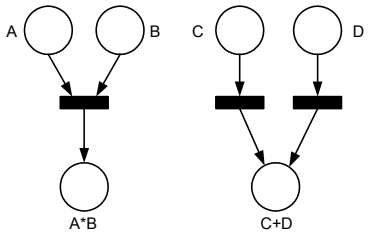
Az *A* hely jelöli az A jelfogó tekercsét, az *A.1–A.4* helyek pedig a jelfogó érintkezőit. Az adott jelfogó *húzott* állapotát az jelenti, ha az *A* helyen token van, az érintkezők pedig akkor zárnak (illetve szakítanak, ha nyugalmi érintkezőről van szó), ha az azokat reprezentáló helyeken token van.

A *T* tranzíció különböző típusú (determinisztikus, időzített vagy sztochasztikus) megválasztása esetén – az állapotmodellezési eljáráshoz hasonlóan – különböző rendszertulajdonságok is modellezhetők (*lásd* 6.6.).

Az érintkezőket reprezentáló helyek melletti *nyelő tranzíciók* szerepe a jelfogó ejtésének modellezéséhez szükséges: amennyiben a meghúzás feltételei nem teljesülnek, a jelfogónak el kell ejtenie; a meghúzott állapotot jelentő tokenek kiürülése az érintkezők, illetve a tekercs helyeiből ezeken a nyelő tranzíciókon keresztül történik. A nyelő tranzícióknak *alacsonyabb prioritással* kell rendelkezniük, mint az adott érintkezőt mint logikai változót felhasználó tranzícióknak.

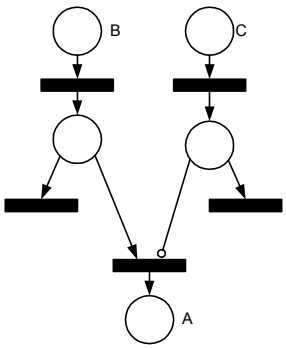
Ez a modellezési technika nem teszi szükségessé a *negált feltételek* beépítését a modellbe, ugyanis ha a meghúzás feltételei nem teljesülnek, akkor a jelfogó tekercsét szimbolizáló hely token-utánpótlása elapad, így a tokenek a jelfogó „tekercséből" és „érintkezőiből" is kiürülnek.

A fenti eljárással elkészített jelfogó-érintkező modellekből *tetszőleges logikai hálózat* építhető fel az érintkezőket reprezentáló egyes helyeknek mint logikai változóknak a felhasználásával. A logikai *ÉS* kapcsolatok az egyes változók közös tranzícióval való összefogásával, a *VAGY* kapcsolatok pedig a bemenő változók egy-egy tranzíció – hely kapcsolatával alakíthatók ki (42. ábra).



42. ábra. Logikai változók ÉS, illetve VAGY kapcsolatának áramutas modellezése

A negált logikai változók (azaz a nyugalmi érintkezők) tiltó élek felhasználásával vehetők figyelembe. Az állapotmodellezés során is bemutatott $A = B \cdot \overline{C}$ művelet a következőképpen mod ellezhető áramutas módon (43. ábra, az ábrán nem jelöltük a B és C jelfogók „működtetését", sem az A jelfogó érintkezőit).



43. ábra. Logikai kapcsolatok áramutas modellezése

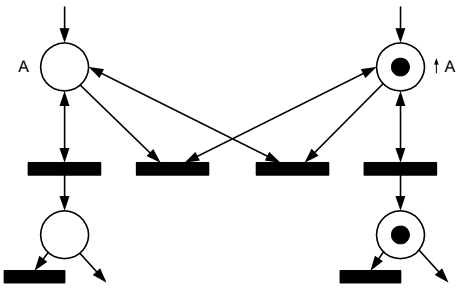
Az *eljárás előnye* – azon felül, hogy nem szükséges a *negált feltételek* beépítése a modellbe – az, hogy az egyes jelfogók működése pontosabban, a valósághoz közelibb módon modellezhető azáltal, hogy *minden egyes érintkezőjét külön reprezentáljuk*. Ez a későbbiekben lehetőséget ad arra, hogy egy-egy jelfogó egyes érintkezőinek *hibáját is szimuláljuk*, és ennek hatását a teljes hálón vizsgáljuk.

Az áramutas modellezési eljárásnak *két hátránya* van. Az egyik a *tiltó élek* alkalmazása, a másik pedig az, hogy a modell *nem korlátos*, azaz egy-egy helyen a tokenek számának a háló egyes állapotaiban nincs felső határa. Mindkét hátrány a háló analízisét nehezíti meg; az áramutas modellek analíziséhez sokkal *bonyolultabb algoritmusokra* van szükség (*lásd* 6.7.2.).

6.7.1. A jelfogós sorompó illesztő kapcsolás áramutas modellezése

A 6.5.-ben bemutatott jelfogós illesztő kapcsolás áramutas modellje a 45. ábrán látható.

Az állapotmodellezéssel elkészített modellhez hasonlóan itt is figyelmet érdemel a támasz-jelfogópár modellezése. Áramutas modellezés esetében ez a 44. ábrán látható.



44. ábra. Támasz-jelfogópár modellezése áramutas módon

Megfigyelhető, hogy például az A helyen, az onnan eredő – a normál jelfogók modelljétől eltérő – lekérdező élnek köszönhetően, a „tokenutántöltés” megszűnése esetén is mindig marad token. A token csak akkor kerül ki az A helyről, ha az ↑A helyen lévő token által az A-hoz tartozó nyelő tranzíció engedélyezve van. Ezeknek nyelő tranzíciónak itt értelemszerűen magasabb prioritásúnak kell lennie, mint a jelfogó érintkezőit „működtető” tranzíciónak.

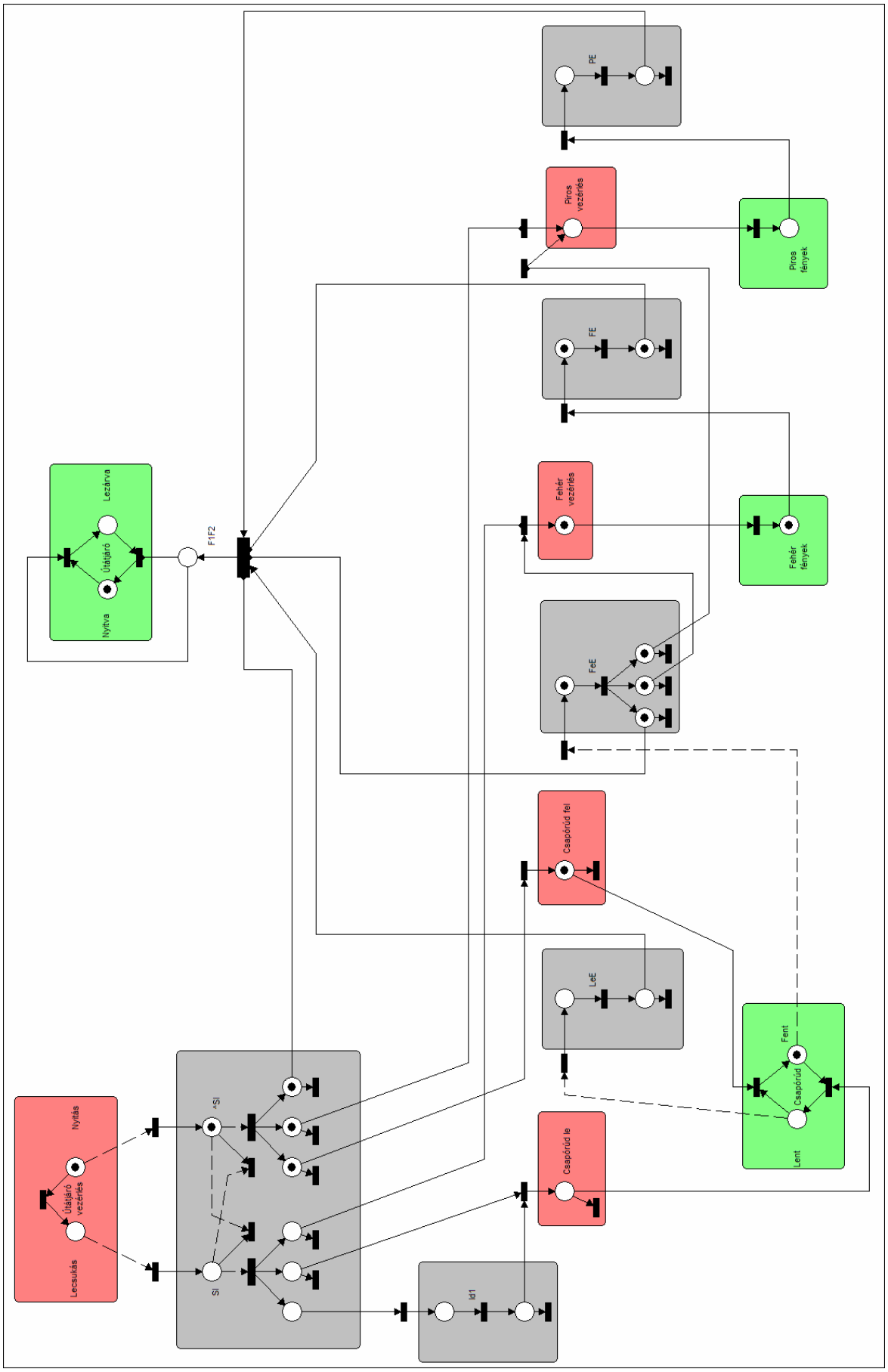
A külsőtéri elemek, illetve a hálózat külső kapcsolatai részben az állapotmodellezési technikához hasonló módon, részben ennél egyszerűbb módon kerültek modellezésre: a kétállapotú vezérlések, például, egyetlen hellyel reprezentálhatók; a bennük lévő token jelzi a vezérlés aktív állapotát.

A modell szerkesztéséhez itt is a HPSim program került alkalmazásra [HPSim]. A modell számszerű jellemzői, összehasonlítva az állapotmodellezési eljárással készült modell adataival, a 10. táblázatban találhatók.

10. táblázat. Az áramutas modell és az állapotmodell számszerű jellemzői

	Áramutas modell	**Állapotmodell**
Helyek száma:	33	34
Tranzíciók száma:	40	40
Élek száma:	96	176

A számszerű adatokból látható, hogy az áramutas modell körülbelül ugyanannyi hellyel és ugyanannyi tranzícióval, de mintegy feleannyi éllel modellezi – az állapotmodellnél valósághűbb módon – ugyanazt a jelfogós kapcsolást.



45. ábra. A sorompó illesztő kapcsolás áramutas modellje

6.7.2. Az áramutas modell analízise

Az előzőekből látható, hogy az áramutas modellezési technika könnyebb modellkészítést, kisebb modellméretet, áttekinthetőbb modellt eredményez, továbbá a jelfogók működése valósághűbb módon modellezhető segítségével.

Az áramutas modellezési technika hátránya a modell nehezebb analizálhatósága. Az áramutas technikával előállított modellek analízisét alapvetően két tényező teszi bonyolulttá:

1. az áramutas modellek megalkotása során nem lehet elkerülni a tiltó élek alkalmazását. Ez azért probléma, mert ahogyan már korábban is utaltunk rá, számos analízis módszer a tiltó élekkel bővített Petri-hálókra már nem használható.
2. Az áramutas Petri-háló modellek nem korlátosak, azaz állapotterük nem feltétlenül véges. Ennek folyományaként az állapotmodellezéssel készült Petri-háló elemzésére alkalmas, 6.6.2-ben bemutatott elemzési technika sem alkalmazható.

E problémák megoldása érdekében, az áramutas modellek analíziséhez továbbfejlesztett technikák szükségesek. A továbbfejlesztésnek két iránya képzelhető el:

- az egyik lehetőség az, hogy a nem korlátos Petri-hálót vissza kell vezetni biztonságos hálóvá. Ez esetünkben azért lehetséges, mert a tokenek száma egy-egy helyen nem hordoz számunkra lényeges információt; a fontos az, hogy van-e token az adott helyen vagy nincs. Ezzel – az elérhetőségi vizsgálat algoritmusába beépíthető – redukcióval az áramutas modellt is az 6.6.2-ben bemutatott módon lehetne vizsgálni. Ez a módszer a háló nem korlátosságának problémáját megoldja, de a tiltó élek alkalmazásával járó nehézség csak további elemzések útján oldható meg.
- A másik lehetőség az áramutas modellek vizsgálatára a szimulációs módszerek alkalmazása. Ez az eljárás mind a korlátosság, mind a tiltó élek alkalmazásának problémáját kezelni tudja.

6.8. Összegzés

Ebben a szakaszban összehasonlítjuk a hagyományos állapotmodellezési eljárást és a javasolt áramutas modellezési technikát.

Az állapotmodellezési eljárás jellemzői a következőkben foglalhatók össze.

- Az állapotmodellezési eljárás esemény-orientált technika. Az eseményeket az egyes jelfogók meghúzása, illetve elejtése adja.
- A negált információk beépítése miatt a modell mérete nagyobb, áttekinthetősége rosszabb, az áramutas modellhez képest.
- Az állapotmodellezés előnye, hogy nem szükséges tiltó élek alkalmazása; ami megkönnyíti a háló elemzését.
- Szintén az elemezhetőségre van pozitív hatással az állapotmodellnek az a tulajdonsága, hogy a Petri-háló korlátos, sőt biztonságos lesz.

Az áramutas modellezés a következőkkel jellemezhető:

- Nem szükséges a negált információk beépítése, ezért a modell mérete kisebb, a modell áttekinthetőbb, a kapcsolási rajznak való megfelelősége könnyebben vizsgálható.

- Az áramutas eljárás dinamikus modellt eredményez: a Petri-háló a jelfogós hálózat stabil állapotában is változtatja az állapotát.
- Az áramutas technika lehetővé teszi, hogy a jelfogós hálózatok működését a valósághoz közelibb módon modellezzük, azáltal, hogy minden egyes érintkezőnek megfelel egy-egy modell-elem.
- Hátránya, hogy nem kerülhető el a tiltó élek használata, ez pedig nehezíti a modell analízisét.
- Ugyanilyen hatással van az analízisre, hogy az ilyen módon kialakított Petri-háló nem korlátos.

A jellemzőket a 11. táblázatban is összefoglaltuk.

11. táblázat. Az állapotmodellezés és az áramutas modellezés összehasonlítása

Állapotmodell	**Áramutas modell**
Eseményorientált	Dinamikus működésű
Nagyobb modellméret	Kisebb modellméret
Nehezebben értelmezhető	Könnyebben értelmezhető
Nincs tiltó él	Van tiltó él
Korlátos, 1-korlátos	Nem korlátos
Könnyebb analízis	Bonyolultabb analízis

6.9. Új tudományos eredmények

Az áramutas modellezési technikával kapcsolatos új tudományos eredményeket a következőképpen foglalhatjuk össze.

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 valósághűbb módon modellezhető.*

A hagyományos és a javasolt modellezési eljárást egy jellegzetes jelfogós kapcsolás modellezése során hasonlítottam össze.

A tézis a [Ság99a] publikáción alapul. A tézisben kidolgozott áramutas modellezési eljárás, egy további kutatás tárgyát képező elemző módszerrel kiegészítve, előnyösen alkalmazható jelfogós kapcsolások, biztosítóberendezések, illetve azok egyes részeinek vizsgálatára.

7. Irányelvek a formális módszerek biztosítóberendezési alkalmazásához

E fejezet célja olyan irányelvek meghatározása, amelyek a formális módszereknek a vasúti biztosítóberendezések életciklusában való alkalmazásához útmutatóak lehetnek. Az irányelvek meghatározásához a 3. fejezetben kidolgozott, általános érvényű alkalmazási szempontrendszer szolgál alapul. Ennek egyes szempontjaihoz

- a vasúti biztosítóberendezési életciklus jellegzetességei (*lásd* 1. fejezet),
- a Követelménykatalógus értékelése (*lásd* 4. fejezet) során megfogalmazott vasúti biztosítóberendezési sajátosságok, továbbá
- az alkalmazási példák elemzéséből levonható tanulságok (*lásd* 5. fejezet)

figyelembevételével határozzuk meg az irányelveket.

Mivel az alkalmazási szempontrendszer egyes szempontjai között szoros összefüggések figyelhetők meg (elsősorban a szigorúság, valamint az alkalmazás különböző szempontok szerinti terjedelmei között), célszerű a tárgyalás során ezek közül valamelyik szempontot, mint *osztályozási alapot* kiemelni. Mivel a formális módszerek alkalmazásának módját elsősorban az határozza meg, hogy a rendszerek életciklusának mely fázisában, illetve fázisaiban törekszünk a formális módszerek alkalmazására, mi a formális módszerek *életciklus-fázisok* szerinti terjedelmét emeljük ki. A többi szempont tárgyalását e köré csoportosítva végezzük el.

A vasúti biztosítóberendezések fejlesztését vizsgálva azt mondhatjuk, hogy a formális módszerek alkalmazása alapvetően két életciklus-fázis köré csoportosítható. Ez a két életciklus fázis a *vasúti feltétfüzet* és a *gyári feltétfüzet* (7.1., illetve 7.2. fejezetek).

Ezután a vasúti és a gyári feltétfüzet közötti *átjárhatóság* kérdését elemezzük a formális módszerek vonatkozásában (7.3. fejezet), majd megvizsgáljuk, hogy milyen módon képzelhető el a formális módszerek alkalmazása a vasúti biztosítóberendezések életciklusának *további fázisaiban* (7.4. fejezet). Végezetül a 7.5. fejezetben a formális módszereknek a vasútbiztosítás területére történő *bevezetésének folyamatával* foglalkozunk.

A fejezetben ismertetett irányelvek és a bevezetési modell a [Ság02a] és a [Ság02b] publikáción alapul.

7.1. Formális módszerek alkalmazása a vasúti feltétfüzetek szintjén

Ebben a fejezetben azt vizsgáljuk meg, hogy milyen irányelvek határozhatók meg a formális módszerek vasúti feltétfüzetek előállítása során történő alkalmazása számára. A tárgyalás vázát a disszertáció 3. fejezetében bemutatott alkalmazási szempontrendszer adja. Az ott szereplő szempontok a következők:

- szigorúság;
- terjedelem
  - funkcionalitás szerint,
  - komponensek szerint,
  - érintettek köre szerint,
- műszaki szempontok;
- adminisztratív szempontok;

7.1.1. Szigorúság és terjedelem

A vasúti feltétfüzet célja a vasút által elvárt követelmények meghatározása. A vasúti feltétfüzetet a megrendelő vasút készíti el. Az ebben megfogalmazott a követelményrendszert a felügyeleti hatóság vizsgálja, a szállító cégek pedig ez alapján készítik el a követelményeket teljesítő rendszerüket. A specifikáció készítője tehát a vasút, a specifikáció olvasóiként a felügyeleti hatóság, a gyártó cégek és a független szakértők vehetők figyelembe. A vasúti feltétfüzet szintjén a formális módszerek alkalmazása tehát a biztonsági folyamat valamennyi szereplőjét érinti. Ez meghatározza a formális módszerek alkalmazásának *terjedelmét az érintettek köre szerint*.

A fentiek alapvető jelentőségűek az alkalmazandó formális módszer szigorúsági szintjének meghatározásához. Ezek alapján a vasúti feltétfüzetek szintjén elkészített formális specifikációnak viszonylag könnyen olvashatónak kell lennie. Ebből következően a 3.1. fejezetben bemutatott *szigorúsági szintek* közül legfeljebb a 2. szint (formális specifikációs nyelv, egyszerű, például szintaktikai ellenőrzés lehetőségével) alkalmazása javasolható. Már egy 2. szigorúsági szintű formális specifikáció is egyértelműbb, precízebb vasúti feltétfüzetet eredményezhet a jelenlegi gyakorlathoz képest. Az egyértelműség javulása a vasúti feltétfüzet szintjén pozitívan hat a vasúti feltétfüzetből kiinduló fejlesztési folyamatra is, hiszen számos implementációs hiba oka vezethető vissza a vasúti feltétfüzet hiányosságaira.

Egy 3. szigorúsági szintű formális módszer alkalmazása ellen több érv szól:

- egy 3. szintű formális módszer kezelése olyan matematikai felkészültséget igényelne, amely jelenleg nincs meg a vasúti feltétfüzetet előállítók és alkalmazók körében;
- a 3. szint alkalmazása jelentősen megnehezíti a formális specifikáció érthetőségét;
- a 3. szint által nyújtott lehetőségek (például formális bizonyítás) nem használhatók ki a vasúti feltétfüzetek szintjén. A további életciklus-fázisokban a vasúti feltétfüzet 3. szigorúsági szintje elvileg ugyan kihasználható lenne, de a vasúti feltétfüzetből a gyári feltétfüzet előállítása olyan cégspecifikus módon történik (*lásd* 7.3. pont), hogy az szinte lehetetlenné teszi egy univerzális, több gyártó cég által is alkalmazható transzformáció végrehajthatóságát.

A vasúti feltétfüzeteket túlnyomórészt funkcionális követelmények alkotják. A további, elsősorban teljesítményjellemzőkre (strukturális biztonsági követelmények, alkalmazási körülmények stb.) vonatkozó követelmények értelmezése, azok számszerűsíthető volta miatt nem ütközik különösebb nehézségekbe. A funkcionális követelmények, azaz a tulajdonképpeni biztosítóberendezési logika értelmezése azonban a megfogalmazott funkciók viszonylag nagy száma, és az azok közti komplex kapcsolatrendszer miatt meglehetősen bonyolult. Az értelmezést tovább nehezíti a nemzetközi projektek esetén fellépő, a különböző vasutak eltérő filozófiájából is adódó fordítási problémák. Ezek alapján azt mondhatjuk, hogy a vasúti feltétfüzetek szintjén a legnagyobb jelentősége a funkcionális követelmények formalizálásának van (*terjedelem a rendszerfunkcionalitás szerint*).

A vasúti feltétfüzetek esetében az, hogy az adott formális módszer alkalmazása mely *rendszerkomponensekre* terjed ki, nem vizsgálható, hiszen a leírt funkciók elosztása hardver-, illetve szoftverelemekre ebben a fejlesztési fázisban még nem történik meg. Az azonban kijelenthető, hogy a korszerű vasúti biztosítóberendezések esetében a feltétfüzetben megfogalmazott funkcionalitást, legalábbis annak jelentős hányadát rendszerint szoftver segítségével valósítják meg. Ilyen módon a vasúti feltétfüzetben alkalmazott formalizálás – figyelembe véve az életciklus további fázisait is – elsősorban a leendő szoftverkomponenseket érinti.

7.1.2. Műszaki szempontok

A 3.1. fejezetben három műszaki alkalmazási szempont figyelembevételét javasoltuk a formális módszerek alkalmazásához. Ezek a következők:

- az alkalmazás jellege,
- az alkalmazás mérete,
- az eszköztámogatottság.

7.1.2.1. A vasúti feltétfüzet funkcionális követelményeit az ún. biztosítóberendezési logika valósítja meg. A vasúti feltétfüzetek szintjén ez a logika absztrakt. A biztosítóberendezési logika *jellegét* mint formalizálandó, modellezendő feladatot vizsgálva azt mondhatjuk, hogy a biztosítóberendezési logika összetett, elsősorban logikai, diszkrét matematikai alapú rendszer. Felfigyelhetünk arra is, hogy a biztosítóberendezési logika erős strukturális rendezettséget foglal magába, a funkciók hagyományosan a biztosítóberendezések külsőtéri objektumaira, illetve azok kapcsolataira vannak leképezve. Ugyanakkor a különböző funkciók közti kapcsolatok a hagyományos specifikációs technikákat alkalmazva nehezen deríthetők fel. Meg kell jegyezni, hogy a biztosítóberendezési logika jellemzően tartalmaz néhány időzítési kritériumot is. Az időzítési jellemzők aránya azonban a biztosítóberendezési logikában elég alacsony. Az időzítési problémák modellezésére a logikai rendszerek leírására szolgáló formális módszerek többsége nem kifejezetten alkalmas, azonban megfelelő kiterjesztésükkel az időzítés modellezése megoldható. A fentiek alapján azt mondhatjuk, hogy a biztosítóberendezési logika jól modellezhető, a formális módszerek alkalmazása számára adekvát feladat, és a formális módszerek alkalmazásával a belső összefüggések könnyebben felismerhetők.

7.1.2.2. A biztosítóberendezési logika modellezési feladatát tekintve az *alkalmazás mérete* az egyik legkritikusabb szempont. Számos kutatási projekt esetében [például Mal99, Cim98] tapasztalható, hogy szigorú formális módszerek alkalmazásával egy méretében és funkcionalitásában is gyakran erősen redukált biztosítóberendezési logika modellezése is már olyan nagyméretű modelleket generál, amelyek kezelése a jelenlegi támogatóeszközökkel nehézkes lehet. E kutatási modellek esetében a nagy modellméret sokszor nem közvetlenül a modellezendő feladatból adódik, hanem a szükséges környezet modellezéséből. Az ilyen ún. *globális* információk modellezése sok esetben nagyobb ráfordítást és nagyobb modellméretet eredményez, mint magának a *lokális* feladatnak a modellezése. Az ilyen globális információk, alapdefiníciók, szabályok a biztosítóberendezések szakterületén dolgozók számára egyértelműek, modellezésük azonban bonyolult.

A vasúti feltétfüzet funkcionális követelményeinek modellezésekor nem célszerű ezeknek az alapinformációknak a modellezése, hiszen ezek tárgyalása eddig sem volt a vasúti feltétfüzet célja. A globális információk formális leírása rendkívül terjedelmessé teheti a formális vasúti feltétfüzetet, ez pedig rontja a ténylegesen modellezendő funkcionalitás áttekinthetőségét, illetve érthetőségét.

A fentiek fényében joggal merül fel az a kérdés, hogy mi a vasúti biztosítóberendezések formális modellezésének a mérethatára a jelenlegi modellezési eszközök által megengedett modellméret szempontjából. Egyszerűen fogalmazva: mekkora bonyolultságú funkcionalitás, illetve mekkora állomásméret modellezhető?

Ennek megállapítása a formális módszerek ismert vasúti alkalmazásai alapján nem egyszerű feladat, aminek alapvetően két oka van:

1. Az egyik fontos tényező, amely megnehezíti a méretkorlátok megállapítását az, hogy sikertelen kísérletekről, próbálkozásokról általában nem számolnak be tudományos fórumokon. Ez természetesen nem jelenti azt, hogy nem lennének ilyenek.

2. A másik ok az, hogy a formális módszerek eddigi vasútbiztosítási alkalmazásai elsősorban a tudományos kutatások sorába tartoznak. E kutatási projekteknek rendszerint nem célja egy teljes biztosítóberendezési funkcionalitás, de még egy adott funkciócsoport teljes feltérképezése sem. Ezek tehát a modellezendő probléma oldaláról nézve nem is feszegetik a korlátokat, így az ottani tapasztalatok sem utalnak feltétlenül a modellméret-korlátokra.

Ez utóbbinak ellenére néhány projektnél egy biztosítóberendezés teljes funkcionalitását meg sem közelítő problémaméret esetén is hatalmas modellméretekkel találkozhatunk.

- Így például a [Mey98a, Mey98b, Jan99]-ben bemutatott ETCS modell, amely a teljes működést nem, csak bizonyos szcenáriók lefolyását modellezi, egy olyan színezett Petri-háló, amely összesen több mint 2500 helyből és tranzícióból áll (*lásd* 5.2.2.2.).
- A [Mal99]-ben bemutatott biztosítóberendezési Petri-hálós modell, amely egy 4-vágányú, 14 váltóból álló állomást modellez (annak csak funkcionális viselkedését szimulálva), összesen kb. 1500 csomópontból és 3100 kapcsolatból áll (*lásd* 5.2.2.5.).
- A [Har00]-ben bemutatott projekt egy megvalósított biztosítóberendezés teljes logikáját modellezi, de a választott konfiguráció rendkívül egyszerű: egy sorompó és egy tolatómenet. E modell állapottere kb. 10^{27} állapot (*lásd* 5.2.3.2.).

A modellek méretét a modellezendő probléma tényleges méretén túl több tényező is befolyásolja, így

- az alkalmazott leíróeszköztől,
- a modellezés módjától, technikájától, és
- a modellezendő funkciócsoport jellegétől is.

A számadatok értékelésénél nehézséget okoz az is, hogy bár viszonylag sok vasútbizotsítási alkalmazás lelhető fel az irodalomban, de *számadatokról kevés* esetben számolnak be. Az egyelőre nem egységes modellezési technikák miatt pedig az értékek *nehezen vethetők össze* egymással.

Ezek fenntartásával, a fenti értékek alapján és azokat összevetve azzal az adattal, hogy a jelenleg vizsgálható állapotterek mérete kb. 10^{120}, azt mondhatjuk, hogy egy teljes biztosítóberendezési logika valósághű mélységű modellezése a jelenlegi korlátok miatt nem lehetséges. A méretkorlát problémájának megoldására két megoldási irány kínálkozik.

- Az egyik lehetőség a biztosítóberendezési logika funkcionalitásának particionálása önállóan vizsgálható funkciócsoportokká. Természetesen ennek során fontos, hogy ne vesszen el a formalizálás egyik fontos lehetősége e területen: a funkciók közötti kapcsolatok feltárása.
- A másik lehetőség a modell megfelelő absztrakciója. A gyakorlati alkalmazások szempontjából ez természetesen nem valósítható meg a funkciók egyszerűsítésével, bizonyos funkciók elhanyagolásával. Ehelyett a megoldás egyfajta hierarchikus modellezési eljárás formájában képzelhető el.

Mindkét esetben a határokat a modellméret kezelhetősége szabja meg: akkora funkciócsoportokat kell kiválasztani a modellezésre, amekkorák még kezelhetők, illetve addig lehet egy absztrakciós szintű modellel dolgozni, amíg annak kezelése nem okoz problémát.

Természetesen a két irány kombinációja is elképzelhető: a funkciócsoportok felbontása, és azokon belül egy hierarchikus modellezési technika.

7.1.2.3. A harmadik figyelembe veendő műszaki alkalmazási szempont az *eszköztámogatottság*. Az előző pontban láthattuk, hogy a biztosítóberendezési logika

modellezése terjedelmes feladat. A modellezéshez ezért elengedhetetlen valamilyen támogatóeszköz rendelkezésre állása. E kérdésben utalunk a 3.4.3. fejezetben megfogalmazottakra.

7.1.3. Adminisztratív jellegű szempontok

A 3.5. fejezetben a következő adminisztratív jellegű alkalmazási szempontokat mutattuk be:

- szakmai összetétel;
- képzés, képzettség;
- bevezető esettanulmány;
- fejlesztési folyamatba való integráció;
- projekt irányelvek figyelembe vétele.

A következőkben megvizsgáljuk ezek értelmezését a formális módszerek vasúti feltétfüzetek szintjén történő alkalmazása esetén.

7.1.3.1. Vasúti feltétfüzetek esetében, illetve általában a formális módszerek vasúti biztosítóberendezési területen történő alkalmazásához csakúgy, mint bármilyen más alkalmazás esetén, lényeges szempont a szükséges *személyi kör összetétele*. Ugyanúgy, mint más alkalmazások esetén, itt is szükséges olyan szakemberek részvétele, akik a formális módszerek alkalmazásában járatosak; a vasúti biztosítóberendezésekhez értő szakemberek jelenléte vasúti feltétfüzet készítése esetén magától értetődő.

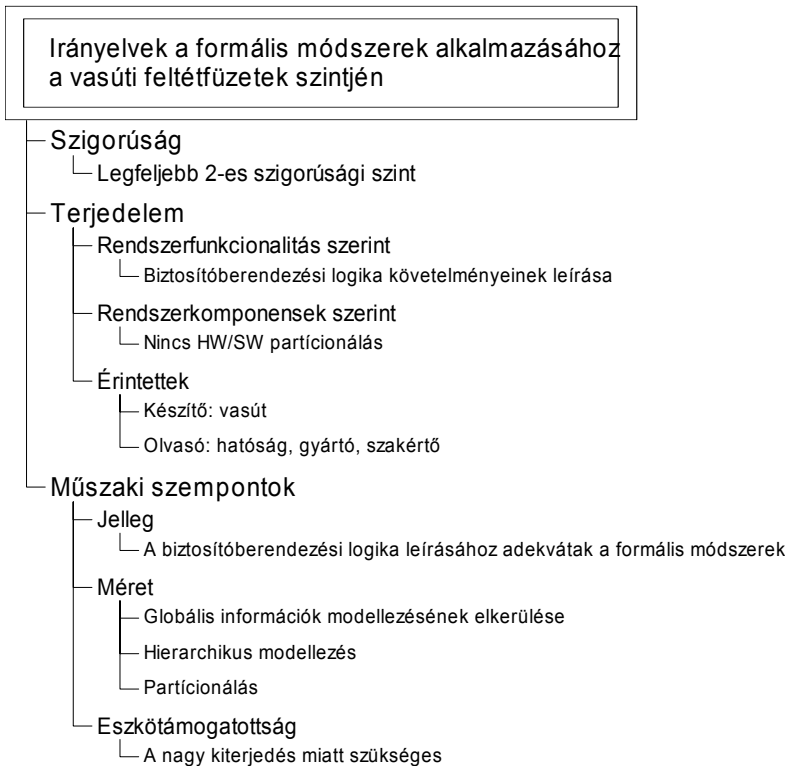
7.1.3.2. A vasúti feltétfüzetek formalizálása során ugyanazok a megfontolások érvényesek a résztvevők *képzését, képzettségét* tekintve, mint bármilyen más típusú alkalmazás esetén (*lásd* 3.5.2. fejezet).

7.1.3.3. *Bevezető esettanulmányként* a vasúti feltétfüzetek esetében egy-egy részfeladat formális specifikációja szolgálhat.

7.1.3.4. Általában fontos szempont a formális módszerek *integrálhatósága a* meglévő *fejlesztési folyamatba*. Mivel a vasúti biztosítóberendezések fejlesztésének folyamata megfelelő módon szabályozott, a formális tevékenységek, így a formalizált feltétfüzet létrehozásának, a meglévő fejlesztési folyamatba való beillesztése nem jár különösebb nehézséggel.

7.1.3.5. A különböző *projekt irányelvek* figyelembevételénél, néhány korábbi ponthoz hasonlóan, vasúti feltétfüzetek elkészítése során ugyanazok a megfontolások érvényesek, mint bármilyen más alkalmazás esetén (*lásd* 3.5.5. fejezet).

A formális módszereknek a vasúti feltétfüzetek szintjén történő alkalmazására vonatkozó irányelveket a szigorúságra, a terjedelemre és a műszaki szempontokra vonatkozóan a 46. ábra foglalja össze.



46. ábra. Irányelvek a formális módszerek a vasúti feltétfüzetek szintjén történő alkalmazásához (szigorúság, terjedelem, műszaki szempontok)

7.2. Formális módszerek alkalmazása a gyári feltétfüzetek szintjén

A következőkben a formális módszerek gyári feltétfüzetek szintjén való alkalmazásához határozunk meg irányelveket, az előző fejezetben is alkalmazott módszer szerint.

A gyári feltétfüzet a vasúti feltétfüzetben megfogalmazott követelményeknek az adott cég általi megoldási módját írja le. Ilyen módon a gyári feltétfüzet vasút- és cégspecifikus. A gyári feltétfüzetet a biztosítóberendezési rendszert fejlesztő cég készíti el. A gyári feltétfüzet olvasói: a vasút és a független szakértő.

7.2.1. Szigorúság és terjedelem

A gyári feltétfüzet a gyártó cégen belüli fejlesztés kiindulási dokumentuma. Ezért nagyon fontos, hogy e dokumentum megfelelően precíz, egyértelmű legyen. A gyártó cég alapvető érdeke, hogy a rendszert minél kevesebb ráfordítással, lehetőleg hibamentesen fejlessze ki. Egy formalizált, legalább részben automatizált fejlesztési folyamat megfelel ennek az elvárásnak. Egy ilyen folyamathoz azonban olyan kiindulási dokumentumra, formális specifikációra (gyári feltétfüzet) van szükség, amelynek szintaktikája és szemantikája lehetővé teszi az automatikus feldolgozást. E követelménynek egy olyan formális módszer felel meg, amelynek *szigorúsági szintje* eléri a 3.1. fejezetben bemutatott 3. szintet (formális szintakszis és szemantika). A formális, automatikus fejlesztési folyamat akkor igazán hatékony, ha rendelkezésre áll az azt támogató, verifikált eszköz is. Ez esetben a bizonyítottan helyesen működő eszköz segítségével készült termékek is helyesnek tekinthetők (*lásd még* 7.2.2.2 pont).

A gyári feltétfüzet követelményei alapján készített részletes rendszerterv vagy az implementáció helyességének formális bizonyításához szintén a gyári feltétfüzet 3. szintű szigorúságára van szükség. Ilyenfajta formális bizonyításra abban az esetben van szükség, ha verifikált eszköz nem áll rendelkezésre.

Amint azt már említettük, a gyári feltétfüzet a vasúti feltétfüzetben leírt követelményeknek egy adott cég által történő értelmezését mutatja be. Annak ellenőrzésére, hogy a vasúti követelmények értelmezése helyes volt-e, feltétlenül szükséges a gyári feltétfüzet validációja. A gyári feltétfüzet validációja célszerűen *szimuláció* segítségével mehet végbe, amelynek segítségével a vasút és a gyártó cég egyeztetheti, hogy a megkívánt funkciók teljesülnek-e. Szimulátor alkalmazására azért van szükség, mert a 3. szigorúsági szinten megfogalmazott formális specifikáció rendszerint a gyári feltétfüzetet jóváhagyó vasúti szakemberek számára nehezen értelmezhető, a jelölésmód komplikáltsága miatt.

Az általános célú formális specifikációs nyelvek nehezen követhető jelölésmódja indokolja azokat a törekvéseket, amelyek arra irányulnak, hogy a vasút számára *speciális leíróeszközöket* alkalmazzanak (például [Red99]). Ezek a leíróeszközök önmagukban nem feltétlenül érik el a 3. szigorúsági szintet. Formális fejlesztésre azonban így is alkalmasak, mert a leíróeszközt is magába foglaló fejlesztőrendszer tükrözi az alaprendszer azon jellemzőit, amelyek figyelembe vételével a leírás szemantikája egyértelmű lesz. Az ilyen jellegű feladatmegosztás magát a funkcionális leírást tömörebbé teheti.

Ahogyan azt a 4.1.1. pontban részleteztük, a gyártó cégek egy-egy vasúti feltétfüzet követelményeinek kielégítésére gyakran nem teljesen új rendszereket fejlesztenek, hanem a követelményeket meglévő rendszereik továbbfejlesztésével vagy adaptálásával igyekeznek kielégíteni. A gyakorlatban ez azt jelenti, hogy a gyártó cégek egyetlen alaprendszerükre több, különböző vasutak funkcionális követelményeit kielégítő felhasználói rendszert is fejlesztenek. Ebből az adódik, hogy a gyártó cég számára megtakarítás akkor jelentkezhet, ha a viszonylag gyakran változó rész fejlesztése során lehet automatizált eszközöket alkalmazni. A vasúti biztosítóberendezések esetében – a gyártó cégek szempontjából – a gyakran változó rész a felhasználói rendszer, azaz tulajdonképpen a biztosítóberendezési logika. Ebből az következik, hogy a formális módszerek alkalmazása a gyári feltétfüzet szintjén is célszerűen a funkcionális követelményekre, azaz a biztosítóberendezési logikára terjed ki (*funkcionalitás szerinti kiterjedés*).

A formális módszerek alkalmazásának *rendszerkomponensek szerinti kiterjedését* vizsgálva részben megismételhetjük a vasúti feltétfüzetek esetében megfogalmazottakat: a formalizálásba bevont biztosítóberendezési logika legnagyobb részét szoftver segítségével valósítják meg a korszerű biztosítóberendezésekben. A formális módszerek hardverösszetevőkre való alkalmazásának szintén van létjogosultsága, ez azonban elsődlegesen nem a biztosítóberendezések funkcionalitásával kapcsolatos (*lásd* 7.4. fejezet).

7.2.2. Műszaki alkalmazási szempontok

7.2.2.1. A formális módszerek műszaki alkalmazási szempontjait a gyári feltétfüzetekkel kapcsolatosan vizsgálva azt mondhatjuk, hogy az *alkalmazás jellegéről* és *méretéről* a vasúti feltétfüzettel kapcsolatban leírtak a gyári feltétfüzetre is érvényesek.

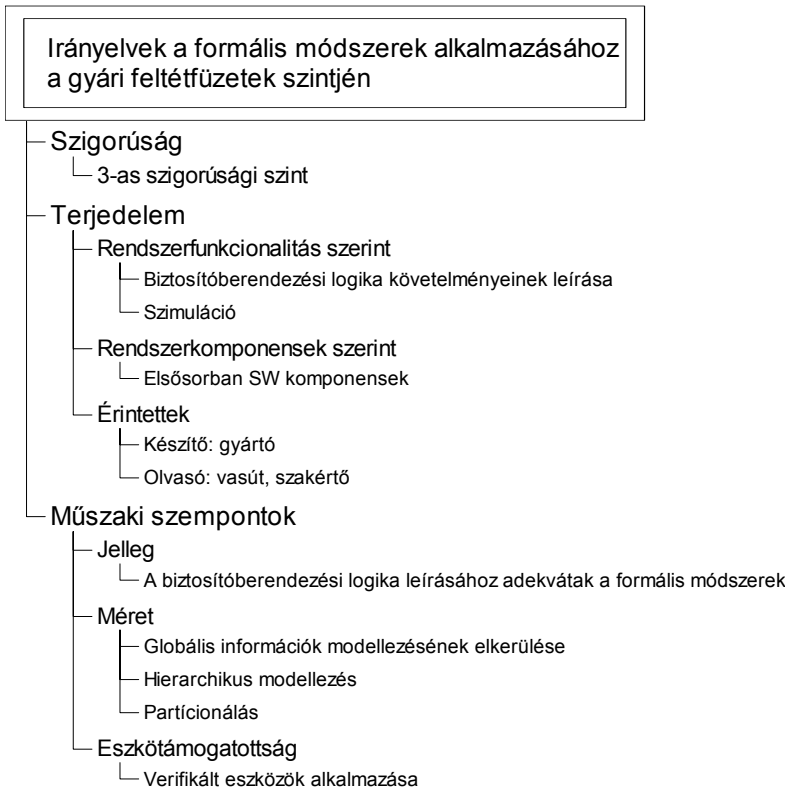
7.2.2.2. Az *eszköztámogatottságot* tekintve megállapítható, hogy a gyártó cégek érdeke az, hogy a formális (automatizált) fejlesztési folyamat során felhasznált támogatóeszközök helyes működését igazolják (verifikálják). A támogatóeszköz helyességének bizonyítása azzal az előnnyel jár, hogy az eszköz segítségével készült termékek egyenkénti vizsgálatának szükségessége jelentősen csökkenhet. Tehát például ha egy automatizált kódgeneráló szoftver

helyes működése igazolást nyert, akkor az ezzel a rendszerrel generált szoftverek helyességének vizsgálatától el lehet tekinteni.

7.2.3. Adminisztratív jellegű szempontok

A vasúti feltétfüzettel kapcsolatban tett, az adminisztratív jellegű alkalmazási szempontokra vonatkozó megfontolások a gyári feltétfüzet esetén változatlanul érvényesek.

A formális módszereknek a gyári feltétfüzetek szintjén történő alkalmazására vonatkozó a szigorúsághoz, a terjedelemhez és a műszaki szempontokhoz kapcsolódó irányelveket a 47. ábra foglalja össze.



47. ábra. Irányelvek a formális módszereknek a gyári feltétfüzetek szintjén történő alkalmazásához (szigorúság, terjedelem, műszaki szempontok)

7.3. A vasúti és a gyári feltétfüzet közötti átjárhatóság kérdései

A 7.1 és 7.2 szakaszok alapján látható, hogy mind a vasút, mind pedig a gyártó szempontjából a biztosítóberendezési logika funkcionalitása a legnagyobb jelentőségű. A formalizálás funkcionalitás szerinti kiterjedését tekintve, ez az a terület, ahol a vasúti feltétfüzetek és a gyári feltétfüzetek közötti átjárhatóság elképzelhető.

A formális módszerek alkalmazásával, illetve kifejezetten a vasútbiztosítási alkalmazással foglalkozó irodalmak többsége megfogalmazza azt az igényt, hogy a formális módszerek a rendszerek *életciklusának minél több fázisában* kerüljenek alkalmazásra. Többen fogalmazzák meg azt az elvárást (például [Anf99]), hogy az életciklus egyes fázisait egy egységes formális módszer alkalmazása kösse össze. A vasúti biztosítóberendezések

fejlesztése sok-résztvevős, összetett folyamat (*lásd* 1. fejezet). A résztvevők eltérő érdekei és a formális módszerek alkalmazásának eltérő céljai miatt nem várható, hogy a vasúti biztosítóberendezések fejlesztését egy egységes formális módszer támogassa, a fejlesztés valamennyi fázisában. Ezért felmerül a különböző életciklus fázisokban alkalmazott formális módszerek közötti átjárhatóság kérdése.

A vasúti és a gyári feltétfüzet közötti átjárhatóságot a következő tényezők korlátozzák:

- A gyári feltétfüzetek elkészítése során a gyártó cégek rendszerint figyelembe veszik egy már meglévő alaprendszerük tulajdonságait. Emiatt az egyes gyártók által elkészített gyári feltétfüzetek nagyon eltérőek lehetnek.
- A gyártó cégek nagy valószínűséggel nem „osztják meg egymással" a formális módszerek alkalmazásának eljárásait, ennek ugyanis az egyes cégek eltérő alaprendszerei miatt nincs értelme. Természetesen a gyártó cégek piaci megfontolásokból sem adnák át egymásnak a megtakarításokat eredményező, viszonylag nagy költséggel kialakított hatékony fejlesztési rendszerüket.

A jelenlegi állapot szerint a formális módszerek alkalmazása leginkább a gyári feltétfüzetek szintjén történik (például [Red99, Bur00]). A jövőben várható, hogy az egyes vasutak vasúti feltétfüzeteiket félformálisan, majd formálisan fogalmazzák meg. Ennek kapcsán elképzelhető, hogy az egyes cégek olyan, saját alaprendszerüket figyelembe vevő transzformáló rendszereket fejlesztenek ki, amelyek segítségével a formális vasúti feltétfüzet funkcionális követelményei legalább részben automatikusan transzformálhatók az adott cég gyári feltétfüzetévé.

Elképzelhető az is, hogy az egyes gyártó cégek továbbra is manuálisan állítják elő az immár formális vasúti feltétfüzetből a formális gyári feltétfüzetet, és az automatikus transzformáló rendszerek helyett olyan formális bizonyítási rendszereket fejlesztenek ki, amelyek segítségével igazolható lenne, hogy a gyári feltétfüzetben leírt funkciók tartalmazzák a vasúti feltétfüzet által megkövetelt funkciókat. Mivel a két összevetendő dokumentum formálisan van megfogalmazva, ezért az összehasonlítás is elvégezhető lenne formálisan, legalább részben automatizálva.

Meg kell jegyezni, hogy míg a formális gyári feltétfüzet és az azt követő formális fejlesztés kialakítása a gyártó cég érdeke, addig a vasúti feltétfüzet formalizálása nem várható a vasút kezdeményezéséből. A vasútnak, mint megrendelőnek ugyanis nem közvetlen érdeke, hogy a követelmények megfogalmazása során nagyobb ráfordításokat eszközöljön, mint a jelenlegi gyakorlat, még akkor sem, ha ez a vasúti feltétfüzet minőségi javulását eredményezné.

7.4. Formális módszerek az életciklus többi fázisában

A formális módszerek természetesen nemcsak a vasúti feltétfüzet és a gyári feltétfüzet előállításának szintjein, valamint az ezt követő, cégen belüli fejlesztési fázisok esetén alkalmazhatók. A formális módszerek fontos szerepet játszhatnak a vasúti feltétfüzet megfogalmazását megelőző fázisokban, elsősorban a veszély- és a kockázatelemzés fázisaiban, valamint a termék előállításához, gyártásához kapcsolódó fázisokban, például a terméktesztelésben is.

A vasúti feltétfüzetben megfogalmazott követelményeket a vasutak jelenleg leginkább tapasztalati alapon határozzák meg. E követelmények meghatározása során jelenleg egy ún. minőségi szemlélet figyelhető meg. Így például az egyes veszélyforrások figyelembe vétele szisztematizált módon, de elsősorban intuitív, tapasztalati alapon történik.

Az utóbbi években több olyan törekvés figyelhető meg, amelyek célja – többek között – a biztonsági irányítórendszerekre fordított költségek ésszerű mérséklése. Ebbe a sorba tartozik a biztosítóberendezések területén az ún. *low-cost signalling* (kis költségű vasútbiztosítás) irányzat, illetve ide tartoznak az új CENELEC szabványok is. Ezek az új európai szabványok szakítanak a korábbi minőségi szemlélettel. Ehelyett egy mennyiségi szemléletet követve, kockázati osztályokat, biztonsági integritási szinteket alakítottak ki, hogy a biztonsági rendszerek kialakítására fordított költségeket olyan alacsonyan lehessen tartani, ahogyan azt a feladat ténylegesen indokolja. A vasutak többsége a biztosítóberendezésekkel szemben támasztott követelmények meghatározása során az eddigiekben nem alkalmazta ezt a mennyiségi szemléletet, kutatások azonban folynak ebben az irányban (*lásd például* [Zah98]).

A veszély- és kockázati elemzések elvégzésére a formális módszerek igen megfelelőek, számos alkalmazás célja ilyen biztonsági elemzések formális végrehajtása (*lásd például* [Zah99]).

A formális módszerek alkalmazásának elsődleges célja az lehet az említett korai életciklus-fázisokban, hogy támogassa a veszély- és kockázatelemzés mennyiségi szemléletű végrehajtását. Ennek eredményeként határozható meg a biztosítóberendezésektől ésszerűen elvárható funkcionalitás. A biztosítóberendezések hagyományos, tapasztalati alapon kialakult funkciórendszere helyett egyszerűbb, következésképp olcsóbban realizálható funkciórendszer alakítható ki. Abból az elvből kiindulva, hogy a biztonsági rendszerektől elvárt biztonsági integritási szint a rendszerek funkciói által végbevitt kockázatcsökkentés mértékével arányos, a kívánt integritási szint elérésével kapcsolatos költségek is mérsékelhetők lennének.

Természetesen a veszély- és kockázatelemzés során alkalmazott formális módszerek modelljei nem alkalmasak arra, hogy belőlük a kockázatcsökkentést végrehajtó funkciók modelljei közvetlenül levezethetők legyenek. Ezért a veszély- és kockázatelemzés formalizálása a funkcionalitás formalizálásától teljesen elkülönülve képzelhető el.

A formális módszerek a rendszerek életciklusának későbbi fázisaiban is sikeresen alkalmazhatók. Így például a termékek tesztelése során előnyös lehet a formális módszerek alkalmazása automatikus tesztgenerálás céljára (*lásd például* [Tar82a, Tar82b, Tar98]).

Megfigyelhetők a formális módszereknek olyan alkalmazásai is, amelyek nem illeszkednek be a rendszerek szokásos életciklusába. Ide tartoznak az olyan projektek, amelyek során egy már meglévő rendszer vizsgálatát végzik el utólag, formális módszereket alkalmazva (*lásd például* [Ság99, Eri96, Eri98]).

7.5. A formális módszerek bevezetésének javasolt lépései

Az előzőekből látható, hogy a vasúti biztosítóberendezési rendszerek fejlesztési folyamatában részt vevők céljai, és így érdekei is különbözőek a formális módszerek alkalmazásával kapcsolatban. Az egyelőre hiányzó szakismeretek mellett ez a tényező nehezíti meg leginkább a formális módszerek bevezetését, illetve széleskörű elterjedését a vasútbiztosító technikában.

Egy új technológia bevezetése egy olyan szakterületre, amelyben sok résztvevő érintett, nem egyszerű feladat. A formális módszereknek a szabványosítás területére történő bevezetésének problematikájával, illetve lehetséges folyamatával például részletesen foglalkozik a Nemzetközi Szabványosítási Szervezet (*International Standards Organization*, ISO). Ez a szervezet a formális módszerek bevezetésére a szabványosítás területén egy háromfázisú tervet javasolt [ISO87]:

- Az első fázisban, amíg a formális módszerek alkalmazhatóságát korlátozza a szükséges szaktudás megléte, addig a formális módszerek alkalmazását párhuzamos tevékenységként javasolják a hagyományos eljárással. Ebben a fázisban azonban a szabvány kizárólag hagyományos módon jelenik meg. A szabványok formális

fejlesztése során végzett tevékenységek természetesen hathatnak a hagyományos szabványfejlesztési folyamatra is. A terv javasolja minden, a párhuzamos tevékenység eredményeképpen létrejött formalizált munka publikálását annak érdekében, hogy a tapasztalatok minél szélesebb körben alkalmazhatók legyenek.

- A második fázisban a megszerzett tapasztalatokra és tudásra építve, a formálisan megfogalmazott szabványt a hagyományos nyelven megírt szabvány informatív függelékeként javasolják megjelentetni. A szabványok formális és hagyományos fejlesztése ebben a fázisban is párhuzamosan halad.
- Amikor a formális módszerek alkalmazása és az ehhez szükséges ismeretek megfelelően széles körben elterjedtek, a szabványok alapvető megjelenési formája a formális leírás lehet.

A bevezetési folyamat hatékonyabbá tétele érdekében a vasútbiztosító berendezések szakterületén is célszerű egy többlépcsős bevezetési modell kialakítása. E területen azonban meg kell különböztetni a fejlesztési életciklusban központi szerepet betöltő vasúti, illetve gyári feltétfüzetet, és a bevezetési folyamat egyes fázisait e dokumentumok formalizáltsági szintjével érdemes meghatározni:

1. Informális vasúti és gyári feltétfüzet
2. Informális vasúti, formális gyári feltétfüzet
3. Formális vasúti és gyári feltétfüzet

A következő pontokban a bevezetési folyamat fenti lépcsőit tekintjük át részletesen.

7.5.1. Informális vasúti és gyári feltétfüzet

Hagyományosan a vasúti és a gyári feltétfüzetet is informálisan fogalmazzák meg. A vasúti és a gyári feltétfüzet közötti transzformáció ekkor, a két feltétfüzet nem formális volta miatt csak manuálisan történhet.

Meg kell jegyezni, hogy a gyári feltétfüzetekkel kapcsolatban a gyártó cégek már korábban felismerték az egyértelműség fontosságát. Ezért a hagyományos gyári feltétfüzetek is gyakran tartalmaznak formalizmusokat, fél-formális jelölésmódokat, például folyamatábrákat, matematikai logikai összefüggéseket. E leíróeszközök szigorúsága rendszerint nem haladja meg az 1. szintet. Az előbbieknek megfelelően, ezt a lépcsőt két további al-fázisra lehet bontani aszerint, hogy a gyári feltétfüzet teljesen informális, vagy fél-formális módon van-e megfogalmazva.

7.5.2. Informális vasúti, formális gyári feltétfüzet

A formális módszerek bevezetésének következő lépéseként, a formális gyári feltétfüzet kialakításához 2., illetve 3. szintű szigorúságot alkalmaznak a gyártó cégek. Ez lehetővé teszi a gyári feltétfüzetből kiindulva a célrendszer egy részének, legalább részben automatizált implementációját. A 7.2.1. pontban leírtak miatt, a gyártó cégek a formalizálást várhatóan a szűkebb értelemben vett biztosítóberendezési funkcionalitásra, azaz a biztosítóberendezési logikára terjesztik ki. Ez természetesen nem zárja ki azt, hogy az egyes gyártó cégek a biztosítóberendezési logikával nem kapcsolatos funkciók, rendszerkomponensek fejlesztése során (például bizonyos hardverösszetevők, kommunikációs rendszerek) is alkalmazzanak formális technikákat.

A vasúti feltétfüzet nem formális volta miatt a vasúti és a gyári feltétfüzet közötti transzformáció ebben az esetben is csak manuálisan mehet végbe.

A gyári feltétfüzetek formalizálásához, illetve a formális gyári feltétfüzeten alapuló fejlesztőrendszerek kidolgozásához feltétlenül szükséges olyan szakemberek alkalmazása, akik a formális módszerek alapos ismerői. Emellett a cégek természetesen nem nélkülözhetik a vasúti folyamatokat ismerő szakembereket sem (*lásd* 3.5.1. szakasz).

7.5.3. Formális vasúti és gyári feltétfüzet

A bevezetés végső lépcsőjeként várható, hogy a vasutak formálisan fogalmazzák meg a biztosítóberendezésekkel kapcsolatos elvárásaikat. Mint azt már korábban említettük, a formalizálásnak a vasúti feltétfüzetek szintjén is a biztosítóberendezési logikára célszerű kiterjednie. Mivel egy-egy vasúti feltétfüzetet többen olvasnak, mint egy gyári feltétfüzetet, szélesebb az érintettek köre, a vasúti feltétfüzet formalizálását finomabb lépcsőkben érdemes kidolgozni. Egy javasolható módszer a következő:

1. Az első fázisban, amíg a formális módszerek alkalmazhatóságát korlátozza a szükséges szaktudás megléte, addig a formális módszerek alkalmazása párhuzamos tevékenységként javasolható a hagyományos eljárással. A formális vasúti feltétfüzetet a hagyományosan, szövegesen megfogalmazott vasúti feltétfüzet informatív függelékeként javasolt megjelentetni.
2. Amikor a formális módszerek alkalmazása és az ahhoz szükséges ismeretek megfelelően széles körben elterjedtek, a vasúti feltétfüzet alapvető megjelenési formája a formális leírás lehet, kiegészítve egy természetes nyelvű leírással.

A vasúti és a gyári feltétfüzet közötti transzformáció, amennyiben a vasúti feltétfüzet formálisan van megfogalmazva, elvileg automatikus módon is történhet. Az 1. pontban leírt bevezetési lépés esetén a gyártó cégek alkalmazhatnak ugyan automatikus transzformáló rendszereket, a vasúti feltétfüzet formális mellékletén alapulva, azonban e melléklet informatív jellege miatt természetesen szükséges egy manuális felülvizsgálat is. A 2. pontban leírt esetben, amikor a vasúti feltétfüzet elsődleges megjelenési formája a formális megfogalmazás, a vasúti és a gyári feltétfüzet közötti transzformáció teljesen automatikusan is lehetséges. A 12. táblázatban a javasolt bevezetési folyamat összefoglalása látható.

12. táblázat. A formális módszerek bevezetésének folyamata [Ság02b]

A bevezetés lépcsői		**Vasúti feltétfüzet**	**Transzformáció**	**Gyári feltétfüzet**
1. lépcső	**1.1**	informális	manuális	informális
	1.2			félformális
2. lépcső		informális	manuális	formális
3. lépcső	**3.1.**	informális, formális függelék	manuális/automatikus	formális
	3.2	formális, informális függelék	automatikus	

A vasútbiztosítás szakterülete az utóbbi egy-két évben érte el a fent ismertetett folyamat 2. lépcsőjét, igaz csak részlegesen: a cégek egy része (*lásd például* [GRACE, Meteor]) már alkalmaz formális módszereket a bizotsítóberendezési rendszerek fejlesztése során, a vasúti feltétfüzetek azonban továbbra is természetes nyelven vannak megfogalmazva.

A biztosítóberendezési rendszereket megrendelő és üzemeltető vasúttársaságok egy része már felismerte a vasúti feltétfüzetek természetes nyelven való megfogalmazásával járó hátrányokat, ezért érdeklődést mutatnak az új technikák, így a formális módszerek iránt is. Így például mind az 1998-99-ben megrendezett FMERail (Formal Methods Europe - Railway) workshopokon, mind az 1998 és 2000 között megrendezett FORMS (Formal Specification Techniques of Railway Control Systems) fórumokon aktívan képviselték magukat az üzemeltető vasutak.

És bár az üzemeltető vasutaknak nem fűződik közvetlen érdeke a vasúti feltétfüzetek formalizálásához (ellentétben a gyártó cégekkel a gyári feltétfüzetek vonatkozásában), mégis minden fontos, a formális módszerek alkalmazását elősegítő fórumon aktívan jelen vannak és támogatják a formális módszerek elterjedését. A vasutakat pedig a gyártó cégek szintén támogathatják a vasúti feltétfüzet formalizálásában, hiszen a vasúti és a gyári feltétfüzet közötti automatikus transzformáció lehetősége miatt előnyös lenne számukra a formális vasúti feltétfüzet.

7.6. Új tudományos eredmények

A 7. fejezet alapján a következő új tudományos eredményeket fogalmazhatjuk meg.

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 előbbiekben említett értékelő elemzés eredményeinek figyelembevételével határoztam meg.

Az 5. tézis a disszertáció 7.1.-7.4. fejezetein, valamint a [Ság02a, Ság02b] publikációkon alapul.

6. tézis. *Olyan többlépcsős 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 és a [Ság02a, Ság02b] publikációkon alapul.

Az 5. tézis alkalmazási irányelveit mind a további kutatásokban, mind a jövőbeni gyakorlati alkalmazások esetén fel lehet használni. A 6. tézis bevezetési modellje alapot teremthet a formális módszerek vasútbiztosítás területén történő bevezetéséhez; többek között alkalmas lehet egy személyi és tárgyi feltételeket meghatározó bevezetési stratégia kialakítására.

8. Kitekintés

Napjainkra a formális módszerek alkalmazásához gazdag módszer- és eszközrendszer alakult ki. A vasúti biztosítóberendezési alkalmazásnak azonban mindezidáig több gátja is volt. Így 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 következőkben röviden áttekintjük a tématerület aktuális, illetve várható jövőbeni kutatási irányait.

A formális módszereknek a széles *mérnöki gyakorlatban való elterjesztése* az egyik fontos irány. E célt szolgálják azok a kutatások, amelyek a formális módszerekhez kapcsolódó bonyolult matematikát próbálják elrejteni a felhasználók elől (*lásd* 6.1. fejezet, [Pat02a, Pat02b]).

Speciálisan a vasútbiztosítás területén ez a célkitűzés egy olyan formális nyelv, illetve az ahhoz kapcsolódó eszközrendszer kifejlesztésében nyilvánulhat meg, amely a vasútbiztosító berendezések szakterületének alapfogalmait is magába foglalja. Így nem csak a komplikált matematikai jelölésmód tűnhet el a felhasználó szeme elől, hanem az alapfogalmak meglehetősen nehézkes matematikai definícióival sem kell a felhasználónak foglalkoznia. Ebbe a kutatási irányba tartozhat a disszertáció 6. fejezetében bemutatott Petri-hálós modellezési eljáráshoz megfelelő analízis eljárás kifejlesztése is. Az eljárás hosszú távon alkalmassá tehető az általánosan elterjedt jelfogós jelölésmóddal leírt valamennyi rendszer vagy rendszermodell vizsgálatára, nemcsak a valóban jelfogós technikával megvalósított rendszerek vizsgálatára.

A formális módszerek bevezetéséhez szükséges további tevékenység egy részletes bevezetési stratégia kialakítása, amely a 7.5. fejezetben bemutatott modellen alapulhat. E stratégia kialakítása során feltétlenül szükséges a folyamatban érintett résztvevőkkel való szoros együttműködés.

Egy másik aktuális kutatási irány a formális módszerek alkalmazása területén a formális leírásoknak a *fejlesztési folyamatok leírásra* történő alkalmazása. Ilyen például a SPEM (*Software Process Engineering Metamodel*), amelyik egy olyan objektumorientált megközelítésű metamodell, amely konkrét szoftverfejlesztési folyamatok vagy ahhoz kapcsolódó eljárások leírására alkalmas [Dob02]. A fejlesztési folyamat formális leírása alkalmas lehet a fejlesztési folyamatok értékelésére, optimalizálására, illetve adott esetben a hozzájuk kapcsolódó költségek becslésére is.

9. Irodalomjegyzék

[Anf99] Formale Techniken für die Eisenbahnsicherungstechnik. Anforderungskatalog – Zusammenfassung der Arbeitsunterlagen. *Signal+Draht* (91) 10/1999, pp. 38-42.

[Ans95] Anselmi, A., C. Bernardeschi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi, and F. Torielli: An experience in formal verification of safety properties of a railway signalling control system. *SAFECOMP'95 14th International Conference on Computer Safety, Reliability and Security*, Belgirate, Italy, 1995. Springer-Verlag. pp. 474-488.

[Ara00] Arabestani, S, J.-T. Gayen: Objektorientierte Analyse zur Modellierung im Eisenbahnwesen. *Signal+Draht* (**92**) 1+2/2000, pp. 20-27.

[Bas94] Basten, T., R.N. Bol, and M. Voorhoeve: Simulating and Analyzing Railway Interlocking in ExSpect. Technical Report 94-37, *Department of Computing Science, Eindhoven University of Technology*, September 1994.

[Bas95] Basten, T., R.N. Bol, and M. Voorhoeve: Simulating and analyzing railway interlockings in ExSpect. *IEEE Parallel & Distributed Technology: Systems & Applications*, 3 (3), Fall 1995. pp. 50-62.

[Bec96] Bechina, A., J. Hermle, and M. Siormanolakis: Using Prolog for a railway control system. *Fourth International Conference on the Practical Application of Prolog*; London, UK, Practical Application Co., Blackpool, UK, 1996. pp. 19-30.

[Beh98] P. Behm and J.-M. Meynadier. Météor: an Industrial Success in Formal Development. In: [FMERail98/1].

[Ber00] Berglehner, R.: Anforderungsspezifikation für die Hp-Schnittstelle. In: [FORMS00]

[Ber96] Bernardeschi, C., A. Fantechi, S. Gnesi, and G. Mongardi: Proving safety properties for embedded control systems. *Dependable Computing - EDCC-2. Second European Dependable Computing Conference Proceedings*; Taormina, Italy, Springer-Verlag; Berlin, Germany, 1996. pp. 321-32.

[Bjo00] Bjørner, D.: Formal Software Techniques for Railway Systems. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 129-136.

[Bly90] Blyth, D., C. Boldyreff, C. Ruggles, N. Tetteh-Lartey: The Case for Formal Methods in Standards. *IEEE Software*, September 1990. pp. 65-67.

[Bol94] Bol, R.N., J.W.C. Koorn, L.H. Oei, and S.F.M. van Vlijmen: Syntax and Static Semantics of the Interlocking Design and Application Language. Technical Report P9422, *Programming Research Group, University of Amsterdam*, November 1994.

[Bon00] Bondavalli, A., M. Dal Cin, D. Latella, Pataricza A.: High-level integrated Design Environment for Dependability (HIDE). In: *Proc IEEE WORDS'99 5th Int Workshop on Object-oriented Real-time Depenable Systems, Monterey*, 1999. pp. 87-92. *IEEE Computer Society Press*, 2000.

[Bon01] Bondavalli, A., M. Dal Cin, D. Latella, Majzik I., Pataricza A., G. Savoia: Dependability Analysis in the Early Phases of UML Based System Design. *International Journal of Computer Systems – Science & Engineering*, Vol. 16 (5), Sep 2001, pp. 265-275.

[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.

[Boy88] Boyer, R.S., J.S. Moore: A computational logic handbook. *Academic Press,* Boston, 1988.

[Bur00] Burdy, L., J.-M. Meynadier: Experience on the use of a Formal Method in a Railway Company. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 224-228.

[Can97] Canver, E., J.T. Gayen, and A. Moik: Formal specification of the controller software on railway switch example. *Automatiserungs Praxis*, 1997.

[Cas99] Casaza, A, D. Comini, A. Morzenti, M. Pradella, P. San Pietro. F. Schreiber: Interlocking: Specification and Test Case Generation for the Safety Kernel of the Naples Subway. In: [FMERail99/1].

[Cic99] Cichocki, T., J. Górski: Safety assessment of computerized railway signaling equipment supported by formal techniques. In: [FMERail99/3]

[Cim98] Cimatti, A, F. Giunchiglia, G. Mongardi, D. Romano, F. Torielli, P. Traverso: Model Checking Safety Critical Software with SPIN: an Application to a Railway Interlocking System. In: *Proceedings of the Seventeenth International Conference on Computer Safety, Reliability and Security (SAFECOMP'98)*. Heidelberg, Germany. 1998.

[Cla96] Clarke, E.M., J.M. Wing: Formal Methods: State of the Art and Future Directions. Technical Report CMU-CS-96-178. August 1996. p. 22.

[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.

[DIN19250] DIN V 19250 Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen. DIN Standard, May 1994.

[DNANet] DNANet leírás. http://people.cs.uct.ac.za/~william/DNAnet.html

[Dob02] Dobán O., Pataricza A.: Szoftverfejlesztési folyamatok metamodell specifikációja. *BME Méréstechnika és Információs Rendszerek Tanszék*. 2002.

[Ehr98] Ehrig, H.: Relevanz, Integration und Vergleich formaler Spezifikationstechniken. In: [FORMS98]

[Ehr99] Ehrig, H., F. Orejas, J. Padberg: Relevance, Integration and Classification of Specification Formalisms and Formal Specification Techniques. In: [FORMS99]

[EN50126] Railway Applications: The Specification and Demonstration of Dependability – Reliability, Availability, Maintainability and Safety (RAMS); CENELEC.

[EN50128] Software for Railway control and Protection Systems; CENELEC.

[EN50129] Railway Applications: Safety Related Electronic Systems for Signalling; CENELEC.

[Eri96] Erikson, L.-H.: Specifying railway interlocking requirements for practical use. In: E. Schoitsch (ed.): *Proceedings of the 15th International Conference on Computer Safety, Reliability and Security* (SAFECOMP'96). Springer-Verlag, 1996.

[Eri97a] Eriksson, L.H.: Formal verification of railway interlockings. Technical Report 1997:4, *Swedish National Rail Administration*, 1997.

[Eri97b] Eriksson, L.H.: Formalising railway interlocking requirements. Technical Report 1997:3, *Swedish National Rail Administration*, 1997.

[Eri98] Erikson, L.-H., K. Johansson: using formal methods for quality assurance of interlocking systems. In: [COMPRAIL98]

[Eri99] Eriksson, L.H.: Adtranz Signal's Formal Verification Process: The STERNOL Specification Tool (SST). In: [FMERail99/2].

[Fes99] Fessler, M, J. Schütte: Die Methode 'B' – Sichere Software für Bahnanwendungen. In: [FORMS99]

[FME97] FME: Choosing a Formal Method. Introductional Guide. http://www.fmeurope.org/choosing.htm

[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

[Fok96] Fokkink, W.J.: Safety criteria for the vital processor interlocking at Hoorn-- Kersenboogerd. *Proceedings of the 5th Conference on Computers in Railways, COMPRAIL'96*, Part I: Railway Systems and Management, pp. 101-110.

[Fok98] Fokkink, W.J., G.P. Kolk, and S.F.M. van Vlijmen: EURIS, a specification method for distributed interlockings. *SAFECOMP '98*, LNCS. Springer-Verlag, 1998.

[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] FORMS '99 – Formale Techniken für die Eisenbahnsicherung. *Fortschr.-Ber. VDI Reihe 12 Nr. 436 Düsseldorf: CDI Verlag* 2000 p.291

[Fuk00] Fukuda, M, Y. Hirao, T. Ogino: VDM Specification of an Interlocking System and a Simulator for its Validation. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 218-223.

[God95] Godber, A.M.: A European interlocking specification --- the work of the ERRI A201 Committee. *ASPECT--95, IRSE Intl. Conf. on Advanced Railway Control*, Vol. 10, September 1995. pp. 19-26.

[God99] Godziejewski, B.: On Formal Notation to Express Requirements Specifications --- Phase 1 of the Euro--Interlocking Project. In [FMERail99/2]

[Gor91] Gordon, M.J.C.: HOL: A proof generating system for Higher-Order Logic. In G. Birtwistle, P.A. Subramanyam (szerk.): VLSI Specification, Verification and Synthesis. *Kluwer,* 1998. pp. 73-128.

[Gör98] 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.

[Gro94] Groote, J.F., J.W.C. Koorn, and S.F.M. van Vlijmen: The Safety Guaranteeing System at Station Hooen-Kersenboogerd. Technical Report 121, *Utrecht University, Department of Philosophy*, October 1994.

[Gro95] Groote, J.F., S.F. van Vlijmen, and J.W.C. Koorn: The safety guaranteeing system at station Hoorn-Kersenboogerd. *COMPASS '95. Proceedings of the Tenth Annual Conference on Computer Assurance* Gaithersburg, MD, USA. IEEE, New York, N.Y., USA, 1995. pp. 57-68.

[Gro98] Groote, J.F.: A Language for Railway Interlocking Specification. In: [FMERail98/1].

[Gui84] Guiho, G. and L.-F. Mejia: Operational safety critical software methods in railways. *IFIP Transactions A (Computer Science and Technology), IFIP World Congress*, Hamburg, Germany, 1984. pp. 262-

[HaG95] Hartonas-Garmhausen, V., T. Kurfess, E.M. Clarke, D. Long: Automatic verification of industrial designs. *Workshop on Industrial-Strength Formal Specification Techniques*; Boca Raton, FL, USA. *IEEE Comput. Soc. Press*, Los Alamitos, CA, USA, 1995.

[Hal90] Hall, J.A.: Seven Myths of Formal Methods. *IEEE Software,* September 1990. 7 (5) pp.11-19.

[Han94a] Hansen, K.M.: Validation of a railway interlocking model. *Lecture Notes in Computer Science*, 1994. 873:582-

[Han94b] Hansen, K.M.: Validation of a railway interlocking model. *FME'94: Industrial Benefit of Formal Methods*, Springer-Verlag, October 1994. pp. 582-601.

[Han94c] Hansen, K.M.: Validation of a railway interlocking model. *FME '94: Industrial Benefit of Formal Methods. Second International Symposium of Formal Methods Europe*. Barcelona, Spain, Springer-Verlag, Berlin, Germany; Lecture Notes in Computer Science LNCS, 1994. pp. 582-601

[Han98] Hansen, K.M.: Modeling Railway Interlocking Systems. In: [FMERail98/2].

[Har00] Hartonas-Garmhausen, V., S. Campos, A. Cimatti, E. Clarke, F. Giunchiglia: Verification of a safety-critical railway interlocking system with real-time constraints. Science of Computer Programming 36 (2000), pp. 53-64.

[Har95] Harrison, A.J., I.D.R. Shannon: The application of formal methods to railway signalling systems specification and the Esprit III project CASCADE. *SAFECOMP 95. 14th International Conference on Computer Safety, Reliability and Security*, Springer-Verlag, 1995. pp. 101-112.

[Hei96] Heimdahl, M.P.E., N.G. Leveson: Completeness and consistency analysis of state-based requirements. *IEEE Transactions on Software Engineering*, 22(6):363-377, June 1996.

[Hir99] Hirao, Y., T. Ogino, M. Fukuda, I. Watanabe: Interest in Formal Methods from Japanese Perspective. In: [FMERail99/3]

[HPSim] HPetriSim leírás. http://home.t-online.de/home/henryk.a/petrinet/e/hpsim_e.htm

[IEC65A] IEC 65A (Sec) 123: Functional Safety of Electrical/Electronic/Programmable Electronic Systems; IEC

[IEEE81] Special Issue on Reliability. *IEEE Spectrum*, October 1981, **18**, (10)

[Inc92] Ince, D. C.: An Introduction to Discrete Mathematics, Formal System Specification, and Z. *Oxford University Press, Oxford.* 1992.

[Ing92] Ingleby, M., I. Mitchell: Proving safety of a railway signalling system incorporating geographic data. *SAFECOMP 1992: Safety of Computer Control Systems 1992*, 1992. pp. 129-134

[Ing95] Ingleby, M., D.J. Mee: A calculus of hazard for railway signalling. *Workshop on Industrial-Strength Formal Specification Techniques,* Boca Raton, FL, USA, IEEE Comput. Soc. Press, Los Alamitos, CA, USA, 1995. pp. 146-58.

[Ing98] Ingleby, M.: A predicate logic for harmonised interlocking functions. In [FMERail98/1].

[ISO87] *JTC1 Statement of Policy on Formal Description Techniques*. ISO/IEC JTC1 N145 and ISO/IEC JTC1/SC18 N1333, International Standards Organization, Geneva, 1987.

[Jaf91] Jaffe, M.S., N.G. Leveson, M.P.E. Heimdahl, B. Melhart: Software requirements analysis for real-time process-control systems. *IEEE Transactions on Software Engineering*, 17(3):241-258, March 1991

[Jan00] Referenzfallstudie Verkehrsleittechnik: funkbasierte Bahnübergangssteuerung. In: [FORMS00]

[Jan98] Janhsen, A.: Use of models to support communication and clarity in specifications. In: [FORMS98]

[Jan99] Jansen, L., H.-M. Schulz: Simulation of the ETCS model in Design/CPN. In: [FORMS98]

[Jan02] Janota, A., K. Raztocny, J. Zahradnik: UML-based Specification of a Railway Interlocking and Signalling System. *Workshop on Software specification of safety relevant transportation control tasks. 3rd Workshop of the DFG-Priority Program Integration of Software Specification Techniques for Application in Engineering*. Braunschweig, 2002. április 23-24.

[Jon90] Jones, C.B.: Systematic software development using VDM. 2nd edition. *Prentice Hall International* Series in Computer Science, 1990.

[Kam00] Anforderungsspezifikation für die Hp-Schnittstelle. In: [FORMS00]

[Kam99] Kammel, K.: „Formale Techniken“ Anwendung/Anforderungen. In: [FORMS99]

[Kem90] Kemmerer, R. A.: Integrating Formal Methods into the Development Process. *IEEE Computer.* September 1990. pp. 37-50.

[Klo00] Klose, J., A. Moik: Modellierung der Forms-Fallstudien mit Statemate. In: [FORMS00]

[Kol98] Kolk, G.: Interlocking logic: specification and validation form a users perspective. In: [FMERail98/1].

[Lap91] Laprie, J. C. (ed.): Dependability: Basic Concepts and Terminology. *IFIP WG 10.4 Dependable Computing and Fault Tolerance*. Springer-Verlag Wien New Your. 1991.

[Lar96] Larsen, P.G., J. Fitzgerald, T. Brookes: Applying Formal Specification in Industry. *IEEE Software*, May 1996. pp. 48-56.

[Len97] Lennartz, K.: Europäische Normen für neue Sicherungseinrichtungen. *Signal+Draht* (89) 11/1997 pp. 5-10.

[Lin00] Lindegaard, M. P., P. Viuf, A. E. Haxthausen: Modelling Railway Interlocking Systems. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 211-217.

[Mal99] Malavasi, G., S. Ricci: Petri nets theory in the railway signalling models. In: [FMERail99/3]

[Mey00] Meyer zu Hörste, M., S. Parthasarathy, E. Schnieder: Notation, Method, Tool: A Conceptual Framework for the Application of Formal Methods. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 141-146.

[Mey98a] Meyer zu Hörste, M.: Die formale Modellierung und Simulation von ERTMS/ETCS mit Petrinetzen. In: [FORMS98]

[Mey98b] Meyer zu Hörste, M.: Modelling and Simulation of Train Control Systems Using Petri Nets. In: [FMERail98/2]

[Mey99] Meyer zu Hörste, M.: Petrinetze für die durchgängige Entwicklung von Systemen der Eisenbahnsicherung. In: [FORMS99]

[Mon00] Montigel, M.: Special Session on Formal Methods in Transport – Notes of the Editor. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 138-140.

[Mon95] Montigel, M.: Modelling and enforcement of dependencies in railway safety systems. Technical Report 1995DI-th10776, *Swiss Federal Institute of Technology*, Zurich, August 21 1995.

[Mon99] Montigel, M.: Why it may be Difficult to introduce Formal Methods into an existing Development Process. In: [FMERail99/1]

[Mor91] Morley, M.J.: Modelling British Rail's Interlocking Logic: Geographic Data Correctness. Technical Report ECS-LFCS-91-186, *University of Edinburgh*, 1991.

[Mor93] Morley, M.J.: Safety in railway signalling data: A behavioural analysis. *Proc. 6th annual workshop on higher order logic and its applications*, Vancouver, 4-6 August, Springer-Verlag Lecture Notes in Computer Science, Vol.780, 1993-4. pp. 465-474.

[Mos91] Moser, L.E., P.M. Melliar-Smith: Formal Verification of Safety-Critical Systems. *In*: P.A. Bennett (ed.): *Safety Aspects of Computer Control.* Butterworth–Heinemann, 1991

[Mye86] Myers, W.: Can Software for the Strategic defense initiative ever be error-free? *IEEE Computer*, November 1986, 19, (11)

[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.

[Nel96] Nelli, M., A. Bondavalli, L. Simoncini: Dependability modeling and analysis of complex control systems: An application to railway interlocking. *Lecture Notes in Computer Science*, 1996. 1150:93-

[Nix88] Nix, C.J., B.P. Collins: The Use of Software Engineering, Including the Z Notatation, in the Development of CICS. *Quality Assurance*, September 1988, pp. 103-110.

[Ost92] Ostroff, J.S.: Formal Methods for the Specification and Design of Real-Time Safety Critical Systems. *Journal of Systems and Software*. Vol. 18, Nr. 1, pp. 33-60 April 1992.

[Par98] Park, D.Y.W, J.U. Skakebæk, M.P.E. Heimdahl, B.J. Czerny, D.L. Dill: Checking Properties of Safety Critical Specifications Using Efficient Decision Procedures. *Proceedings of the second workshop on formal methods in software practice*, March 4-5, 1998, Clearwater Beach, FL USA pp. 34-43.

[Par99] Parthasarathy, S., E. Schnieder: The explication problem: Achille's heel of formal methods. *6th Symposium on Development and Operation of Complex Automation Systems (EKA'99).* Braunschweig, 1999.

[Pas01] Pastro, E., J. Cortadella, O. Roig: Symbolic Analysis of Bounded Petri Nets. *IEEE Transactions on Computers* Vol. 50. No. 5. May 2001. pp. 432-448.

[Pat99] Pataricza A., Sziray J., Majzik I., Csertán Gy., Jávorszky J., Szász Cs., Huszerl G.: Biztonságkritikus rendszerek UML bázisú tervezése és verifikálása. In: *Biztonságkritikus számítógéprendszerek funkcionális verifikálása. 3. miniszimpózium*. Győr, Akadémiai Napok, Sécsenyi István Főiskola, 1999. szeptember

[Pat01] Pataricza A., Csertán Gy., Majzik I., Bartha T.: Formális módszerek az informatikában. Jegyzet kézirat. 2001. március.

[Pat02a] Pataricza A.: Dependability – a Byproduct of Model-Driven System Synthesis? In: Brinkschulte, U., Grosspietsch, K.E., Hochberger, C, Mayr, E.W. (eds.): *Workshop Proceedings of the International Conference on Architecture of Computing Systems ARCS 2002.* Karlsruhe, Germany, VDE Verlag GmbH, Berlin. pp. 13-15.

[Pat02b] Pataricza A.: From the General Resource Model to a General Fault Modeling Paradigm? *Workshop on Critical System Development with UML 2002*, Dresden, Germany.

[Pel00] Peleska, J., A. Baer, A. E. Haxthausen: Towards Domain-Specific Formal Specification Language for Railway Control Systems. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 147-152.

[Pet62] Petri, C.A.: Kommunikation mit Automaten. Dissertation, *TH Darmstadt*, 1962.

[Pet97] Petersen, J.L.: Formal Requirement Verification of a Swedish Railway Interlocking System. Technical Report IT-TR: 1997-005, *Technical University of Denmark, Department of Information Technology*, April 1997.

[Pet98] Petersen, J.L.: Automatic verification of railway interlocking systems: a case study. *Proceedings of the second workshop on Formal methods in software practice.* March 4-5, 1998. Clearwater Beach, FL USA, pp. 1-6.

[PM97] Petri Maker Overview. 1997. 01. 31. http://www.daimi.aau.dk/~petrinet/tools/ db/ petrimaker.html

[Red99] Reder, H.-J.: Entwicklungsmethodik und Werkzeuge GRACE. In [FORMS99]

[Rei00a] Reif, W., G, Schellhorn, A. Thums: Safety Analysis of a Radio Based Crossing Control System Using Formal Methods. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 289-294.

[Rei00b] Reif, W, G. Schellhorn, A. Thums: Formale Sicherheitsanalyse einer funkbasierten Bahnübergangsteuerung. In: [FORMS00]

[Roa98] Roanes-Lozano, E., L. M. Laita, and E. Roanes-Macias. An application of an AI methodology to railway interlocking systems using computer algebra. *Lecture Notes in Computer Science*, 1998. 1416:687-,

[Rus00] Rust, H.: Modelling the Generalized Railway Crossing with Hybrid Abstract State Machines. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 281-288.

[Ság98] 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.

[Ság99a] Sághi B.: Jelfogós sorompó illesztő kapcsolás modellezése Petri hálóval. *Féléves házi feladat a* Formális módszerek az informatikában *c. tárgyból.* 1999. november

[Ság99b] Tarnai G., Sághi B.: Erhöhung der Bahnsicherheit durch formale Methoden. *Periodica Polytechnica,* Transportation Engineering, Vol. 26, No 1, Budapest, 1999. pp. 175-186.

[Ság00a] 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.

[Ság00b] Tarnai, G, B. Sághi: Development Method of a Special Railway Interlocking Subsystem. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 495-500.

[Ság00c] Tarnai G., Sághi B.: Formális módszerek alkalmazása a vasútbiztosító technikában. *Vezetékek Világa. Vasúttechnikai szemle.* Budapest 3/2000 pp. 11-15.

[Ság00d] Tarnai G., Sághi B.: Követelményrendszerek formalizálása a vasútbiztosításban. *III. Országos Vasúti Távközlési és Biztosítóberendezési Konferencia* Miskolc-Lillafüred, 2000. október 9-11. pp. 86-98.

[Ság00e] Pataricza A. (szerk.): Formal Methods of Informatics – KHVM 96/2000 projekt beszámoló. Tarnai G., Sághi B.: Chapter *Safety-critical Systems*. p. 53.

[Ság01a] Tarnai G., Sághi B.: Zusätzliche Aspekte zur Anwendung von formalen Techniken in der Eisenbahnsicherungstechnik. *Signal+Draht* (Németország) (93) 7-8/2001. pp. 42-45.

[Ság01b] 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.

[Ság02a] 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 of the DFG-Priority Program Integration of Software Specification Techniques for Application in Engineering*. Braunschweig, 2002. április 23-24.

[Ság02b] Sághi B.: Irányelvek a formális módszereknek a vasútbiztosítás területén történő alkalmazásához. *Közlekedéstudományi szemle.* Budapest LII. (2002) 8. pp. 291-299

[Sie99] ESTW-MÁV. Állomási sorompó illesztésének specifikációja. *Siemens AG*. 1999.

[Sni98] Schnieder, E.: Zum Geleit. In: [FORMS98]

[Sni99] Schnieder, E.: Methoden der Automatisierung. *Vieweg* Braunschweig/ Wiesbaden 1999. p.362.

[Spi92] Spivey, J.M.: The Z notation: a reference manual. 2nd edition *Prentice Hall International* Series in Computer Science, 1992.

[Sul98] Schulz, H-M.: Komplexität des Test technischer Systeme mit Blick auf Leitsysteme im Schienenverkehr. In: [FORMS98]

[Süt00] Schütte, J.: Top Down Optimization of RAMS as Key to High Quality Public Transportation. *9th IFAC Symposium on Control in Transportation Systems*, Braunschweig, 2000, pp. 380.

[Suw99] Suwe, K.-H.: Begrüßung. In: [FORMS99]

[Tar82a] Tarnai G.: Automatic Testing of Functional Units of Railway Safety Appliances. *Quality and Reliability*, Special Issue Vol. 16. Budapest, 1982. pp. 123-126.

[Tar82b] Tarnai G.: Theoretical Bases for Final Checking of the Manufactured Relay Units. *Ganz Electric Review*, Budapest, 19 (1982) pp. 25-30.

[Tar84] Tarnai G.: Algebraisches Modell für Relaiseinheiten der Eisenbahnsicherungsanlagen. *Periodica Polytechnica Transportation Engineering*, Budapest, 1987. pp. 161-169.

[Tho95] Thomas, M.: IEE/BCS Workshop report 20/3/95. University of Glasgow, Dept. of Computing Science. 1995.

[Ube02] Übelhart I.: Application of semi-decision techniques. Diplomaterv. *BME Méréstechnika és Információs Rendszerek Tanszék*. 2002. pp. 41-50.

[Yak98] Yakovlev, A. V., A.M. Koelmans: Petri Nets and Digital Hardware Design. In: *Reisig, W., Rozenberg, G. (Eds.): Lectures on Petri Nets II: Applications. Advances in Petri Nets.* Springer Verlag Berlin. 1998.

[Var02] Varró D., Pataricza A.: Integration of UML and formal analysis methods for assuring dependability. http://www.inf.mit.bme.hu/FTSG/UML.htm

[Vli98] van Vlijmen, S.F.M.: Verification of the Vital Processor Interlocking. In: [FMERail98/1].

[Win90] Wing, J.: A Specifier's Introduction to Formal Methods. *IEEE Computer* September 1990. pp. 8-24.

[Zah98] Zahradník, J., K. Rástočný: Sicherheit des Verkehrs an Bahnübergängen der ŽSR.. Signal+Draht (90) 6/98, pp. 22-25.

[Zah99] Zahradník, J., N. Hanusová, H. Bariová: Analýza rizík v železničnej doprave (Risk analysis in railway transport) In: *Proc. of ŽEL'99*, Žilina, Slovak Republic, pp. 196-200.