Formális módszerekkel a jobb szabványokért

Az UML PSSM állapotgép-szemantika szabvány validációja

Szkupien Péter, Zavada Ármin

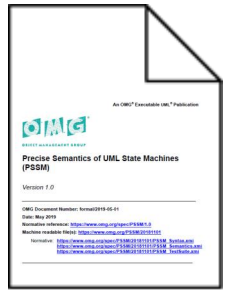
Konzulensek: Elekes Márton, Graics Bence, Dr. Molnár Vince

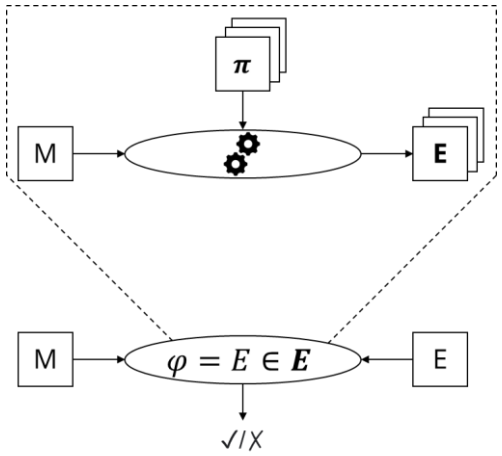
Critical Systems Research Group

Kontextus


OBJECT MANAGEMENT GROUP


UNIFIED
MODELING
LANGUAGE®


Precise Semantics of UML State Machines
(PSSM)
Version 1.0


π
M
E
M
φ = E ∈ E
E
√/X

Szabványok jelentősége

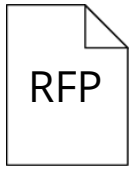
- Komplex rendszerek fejlesztése → **együttműködés**
  - Sok mérnök
  - Különböző szakterületek

- Modellalapú rendszertervezés (MBSE)

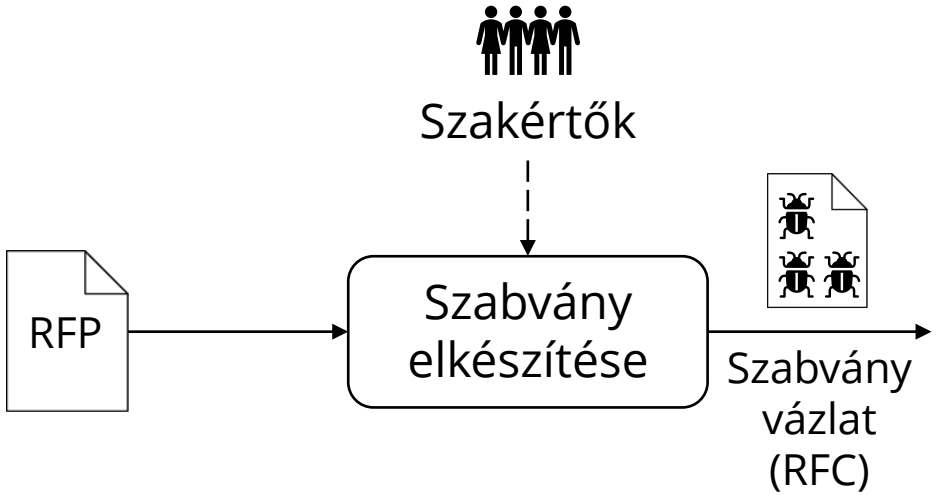
- Modellezési nyelvek
  - Közös nyelv a sok mérnöknek
  - **Közös értelmezés → szabvány**
  - Ma et al., SoSyM'22: igény a formális módszerekre

Validation and verification in domain-specific modeling method engineering: an integrated life-cycle view

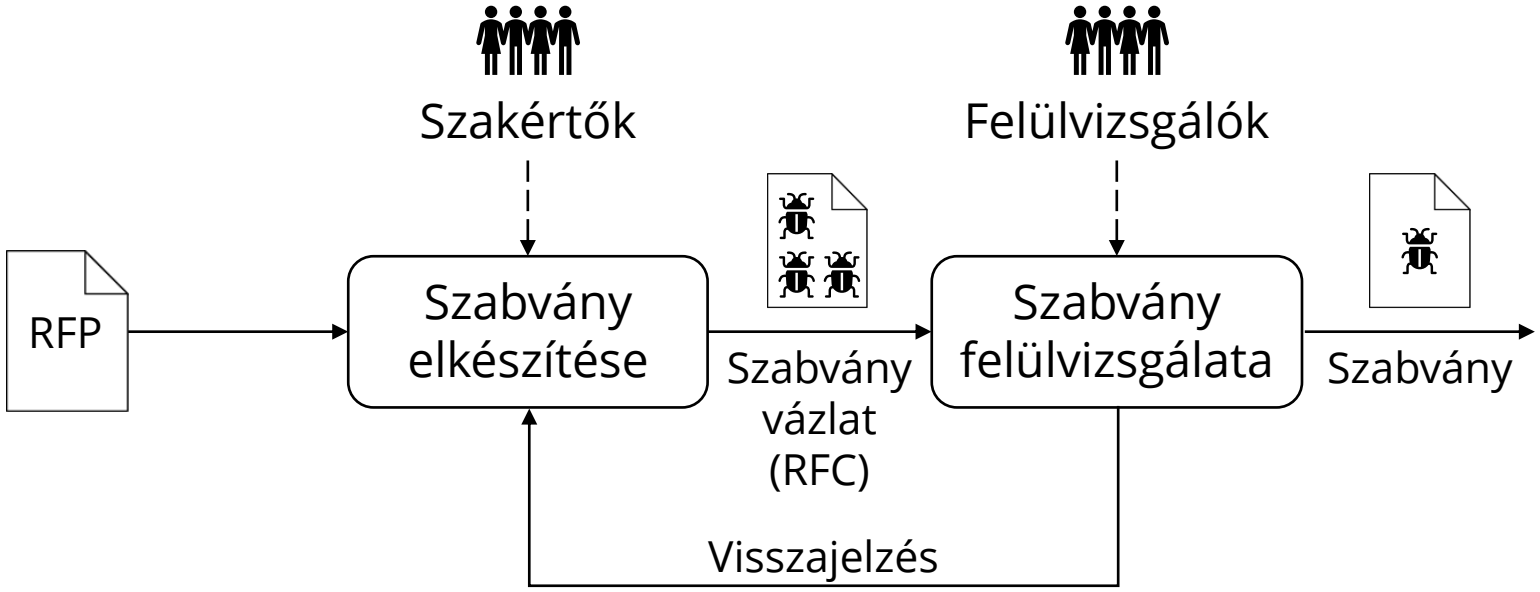
Szabvány életciklusa



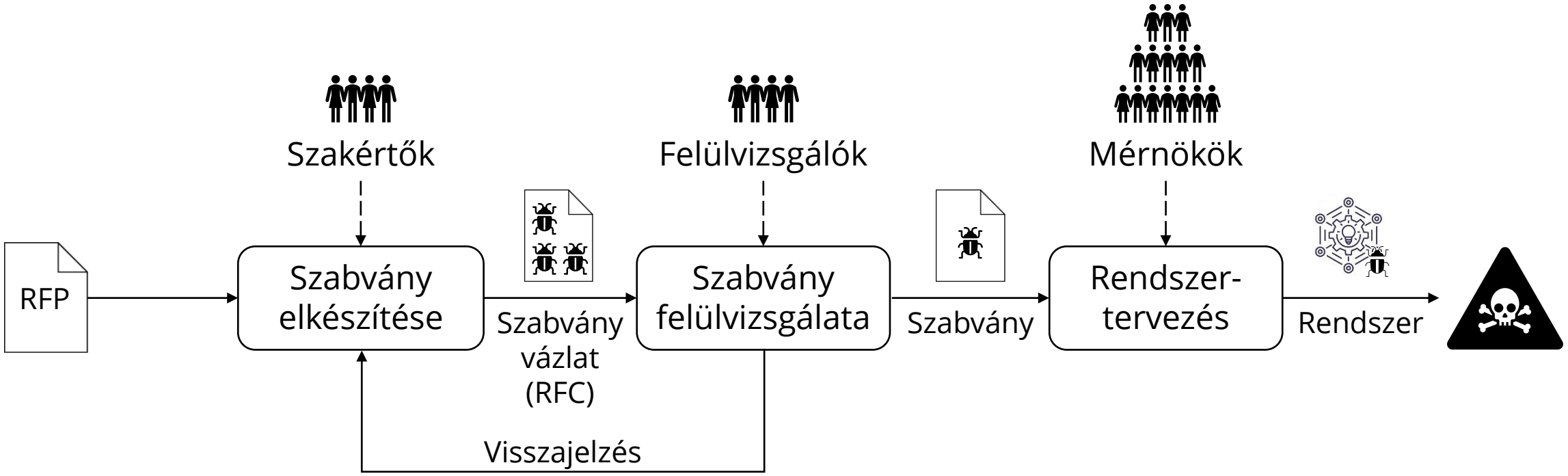
Szabvány életciklusa



Szabvány életciklusa



Szabvány életciklusa

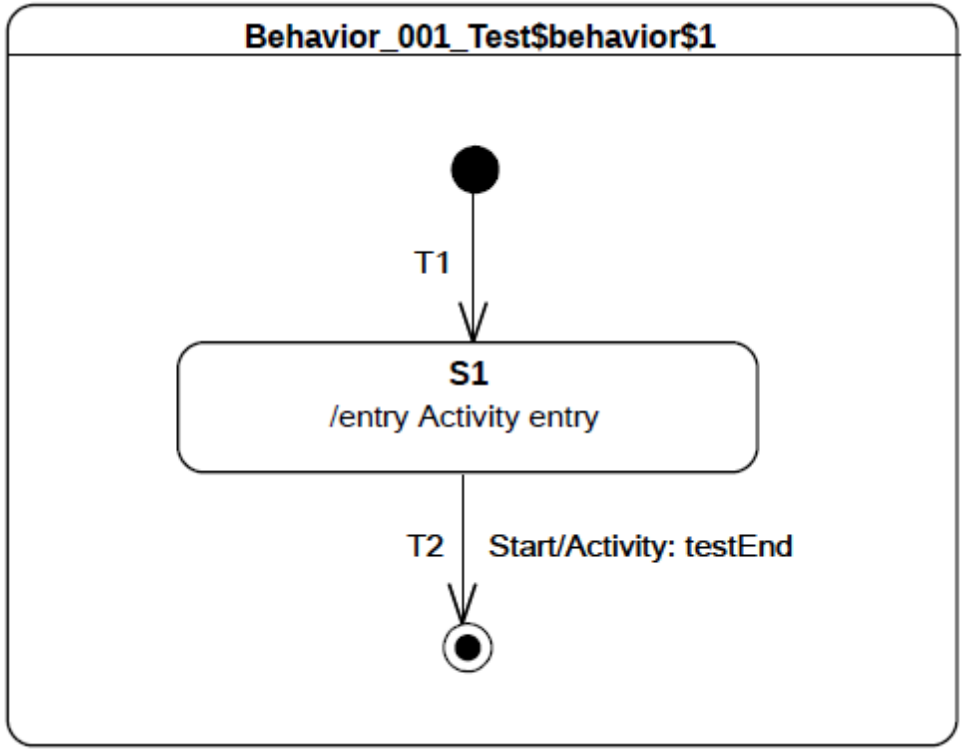


UML PSSM szabvány

- Modellezési nyelv: **UML**
- Formalizmus: **állapotgép** (state machine)**, aktivitás** (activity)
- Szemantika: **PSSM** (Precise Semantics of UML State Machines)
  - Mit jelent *pontosan* egy modell: hogyan viselkedhet

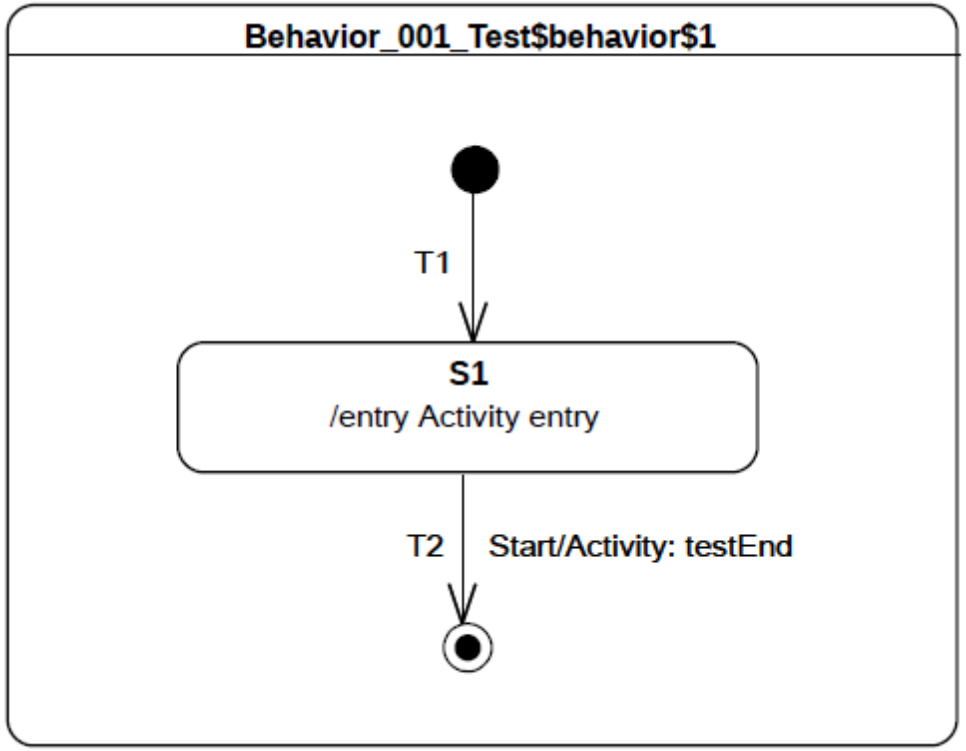
PSSM Test Suite

- Teszt modellek
  - Pl. `Behavior 001`



PSSM Test Suite

- Teszt modellek
- Lehetséges lefutások (trace)
  - Pl. `S1(entry)`



PSSM Test Suite

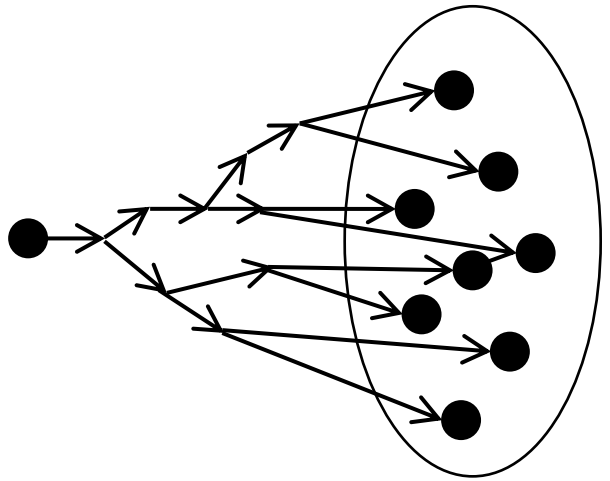
- Teszt modellek
- Lehetséges lefutások (trace)
- „State of the art”
  - Szabvány megértése (példák)
  - Eszközök konformancia ellenőrzése

PSSM Test Suite

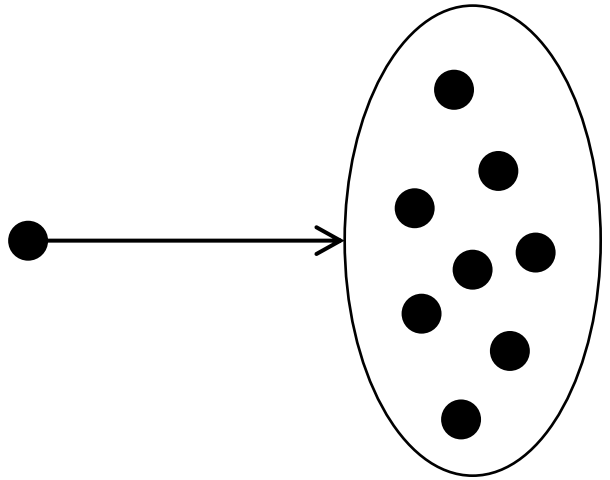
- Teszt modellek
- Lehetséges lefutások (trace)
- „State of the art”
  - Szabvány megértése (példák)
  - Eszközök konformancia ellenőrzése
- Mégis vannak benne hibák
  - Pontatlanságok
  - **Nem teljes → szabványos lefutások hiányoznak**

Szemantikák

- Operációs szemantika (imperatív)
  - *Hogyan* kell kiszámolni az eredményt (lépések)



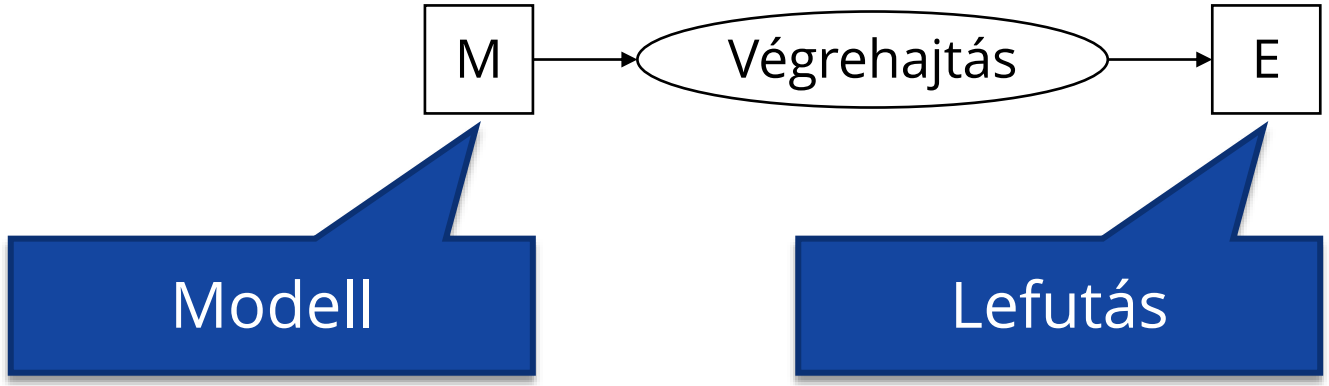
- Denotációs szemantika (deklaratív)
  - *Mi* lehet az eredmény



Modell Végrehajtások

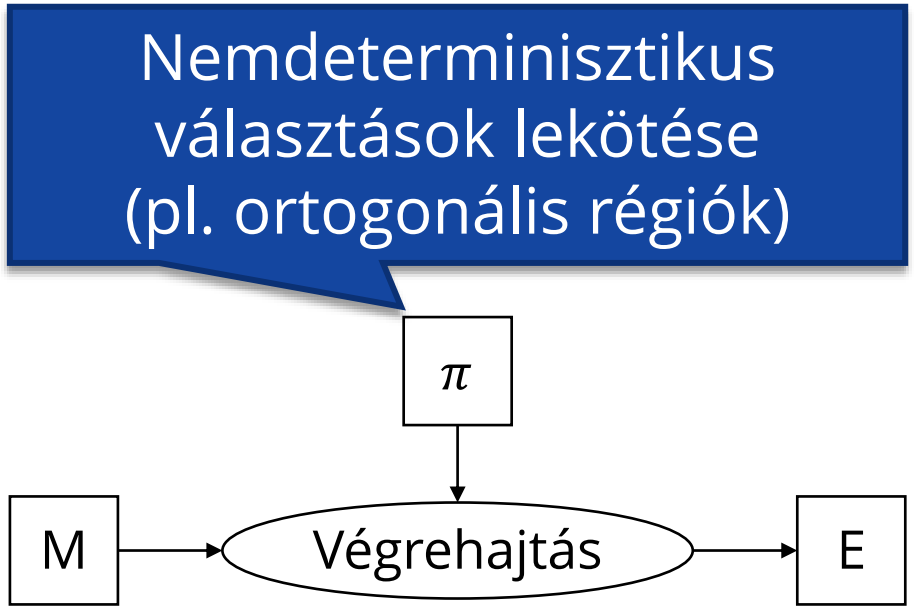
Szemantikák

- Operációs szemantika (imperatív)



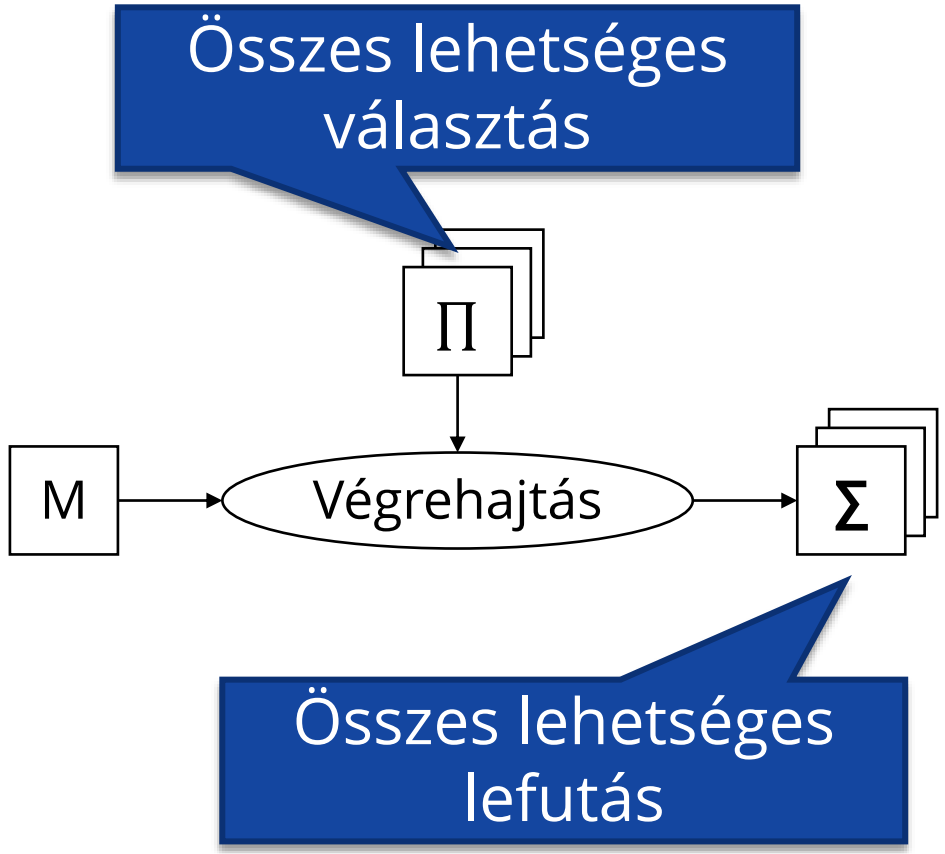
Szemantikák

- Operációs szemantika (imperatív)



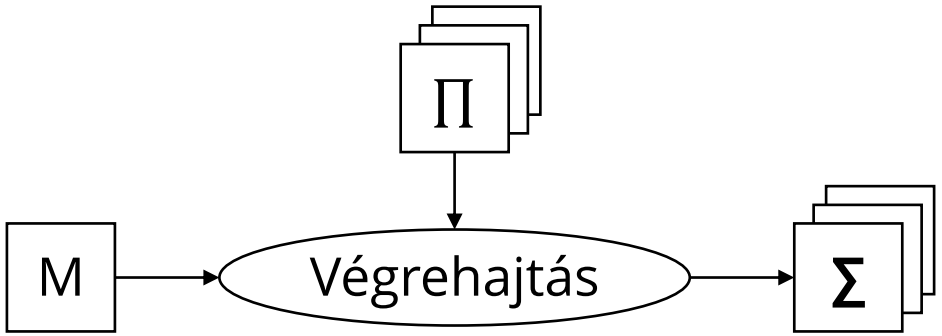
Szemantikák

- Operációs szemantika (imperatív)

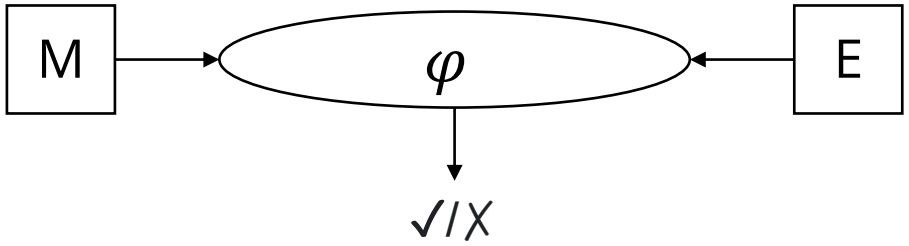


Szemantikák

- Operációs szemantika (imperatív)

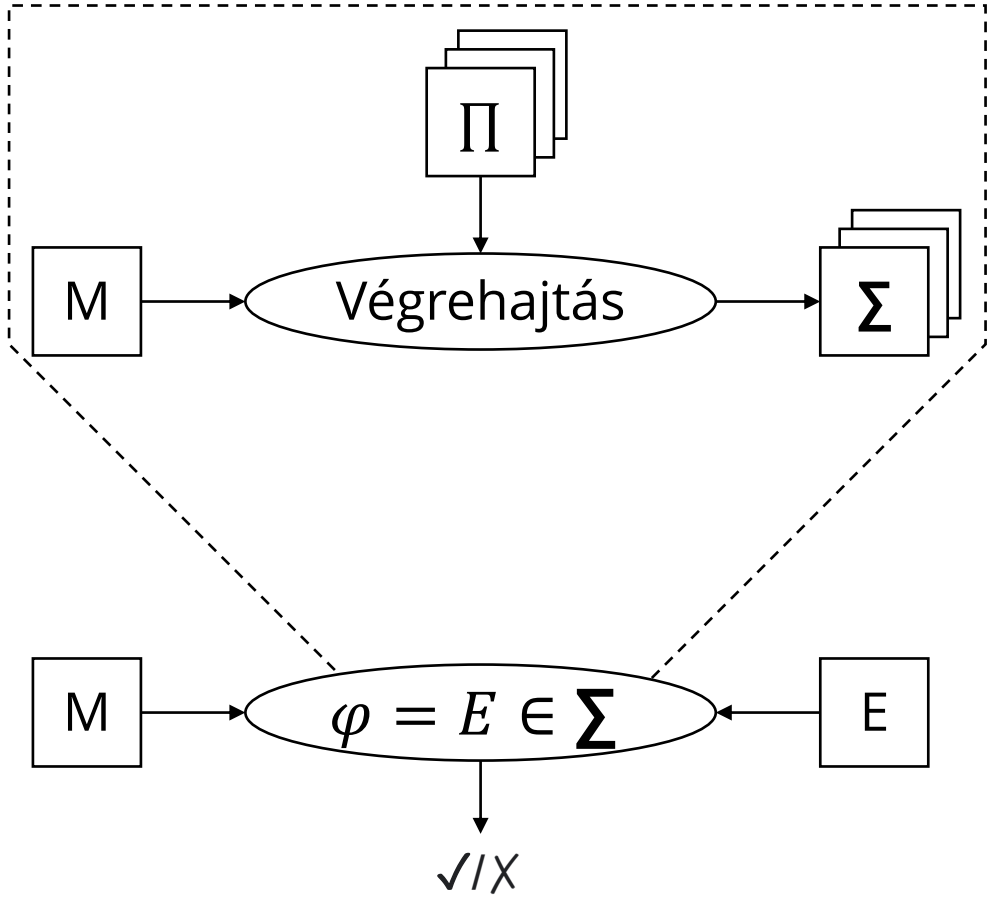


- Denotációs szemantika (deklaratív)



Szemantikák

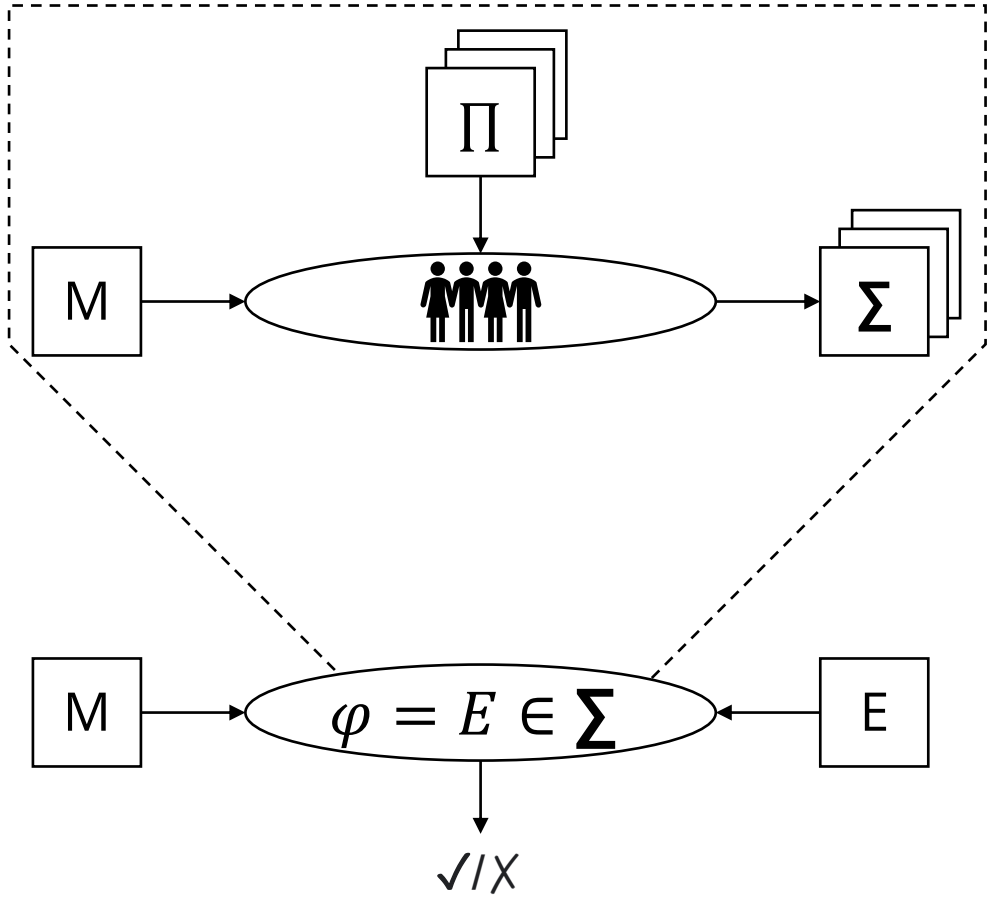
- Operációs szemantika (imperatív)



- Denotációs szemantika (deklaratív)

UML PSSM

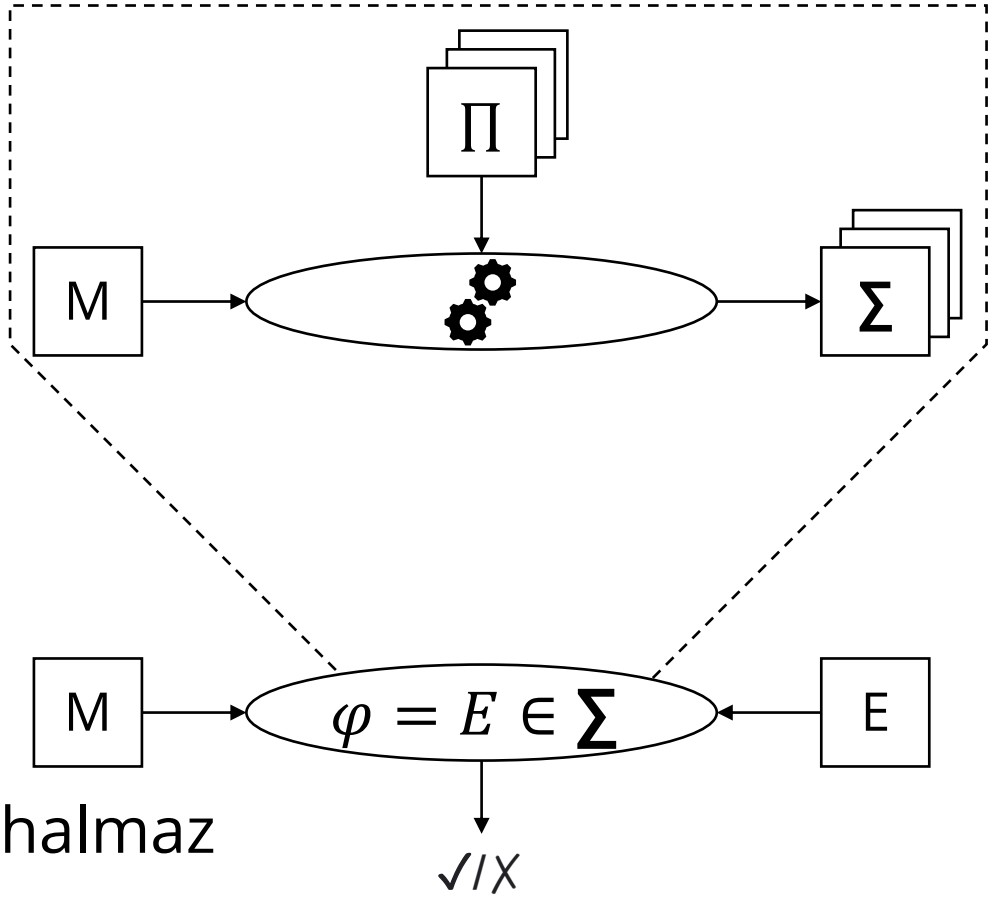
- Operációs szemantika (imperatív)
  - PSSM szemantika szövegesen



- „Denotációs szemantika” (deklaratív)
  - Konformancia ellenőrzés: *orákulum*
  - Operációs szemantika alapján
  - *Manuálisan* előállított lefutás halmaz

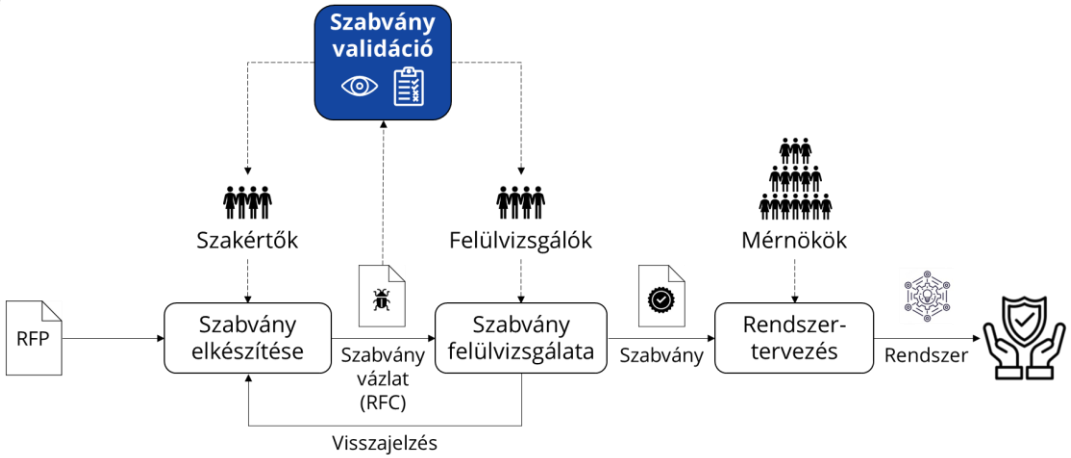
Formális módszerek használata

- Operációs szemantika (imperatív)
  - PSSM szemantika szövegesen

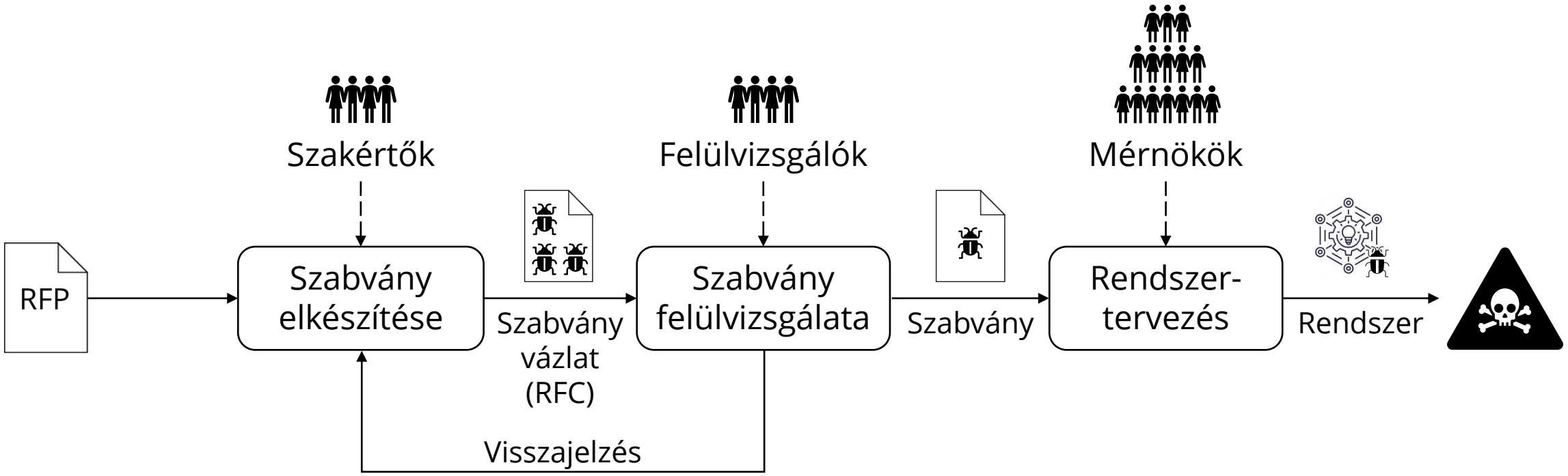


- „Denotációs szemantika” (deklaratív)
  - Konformancia ellenőrzés: *orákulum*
  - Operációs szemantika alapján
  - ***Formális módszerekkel*** előállított lefutás halmaz

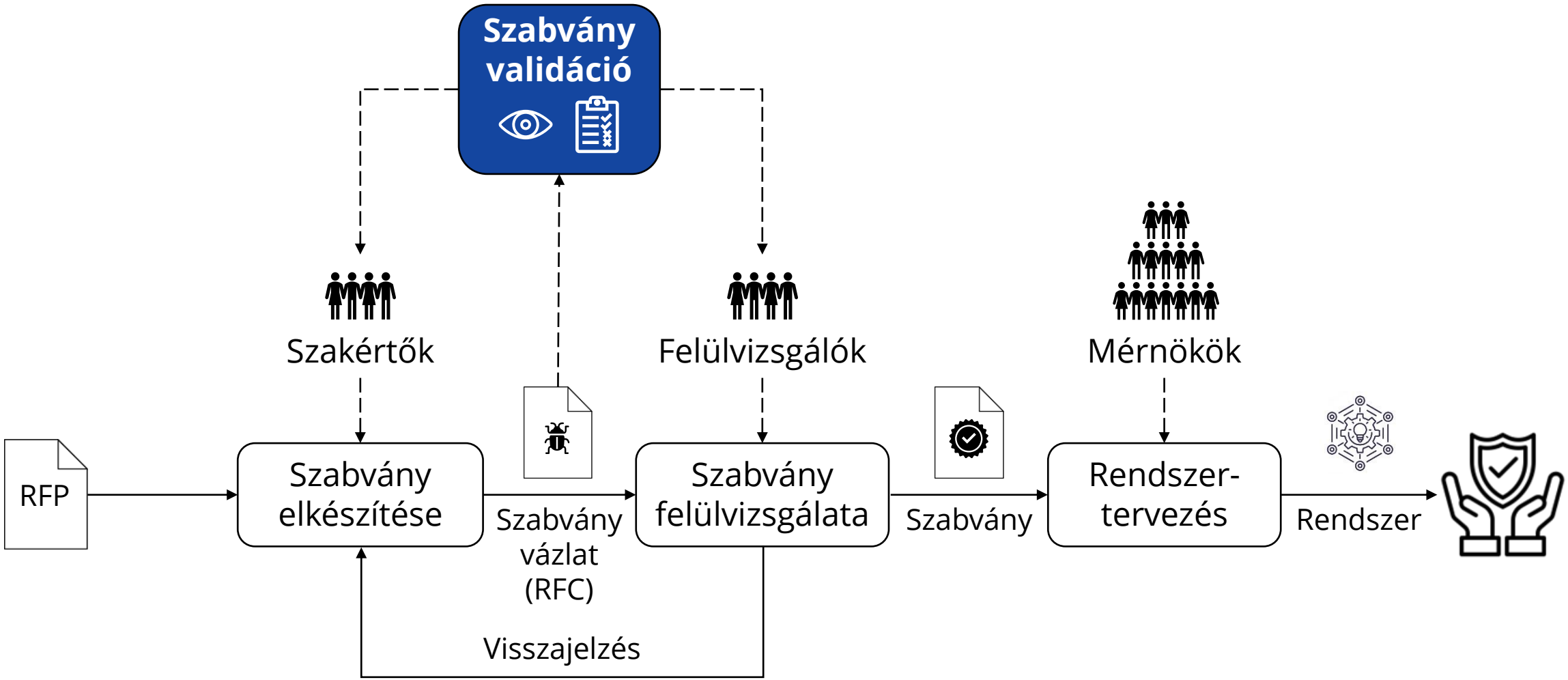
Szabvány validáció



Szabvány validáció



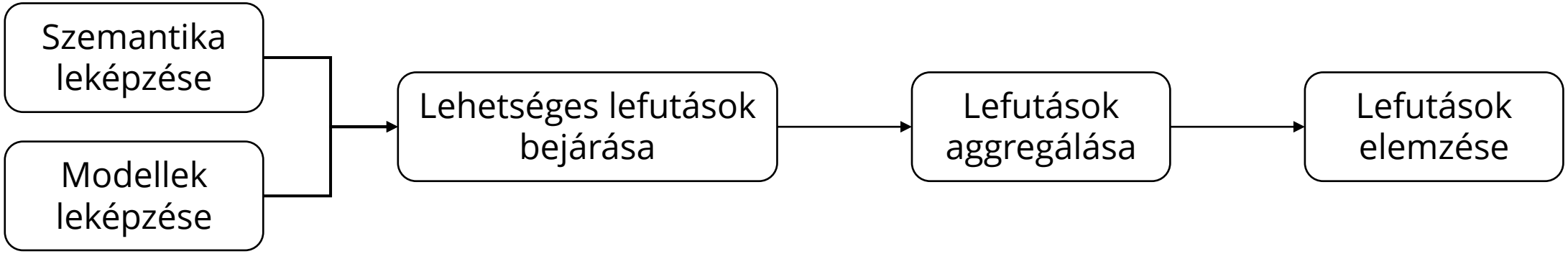
Szabvány validáció



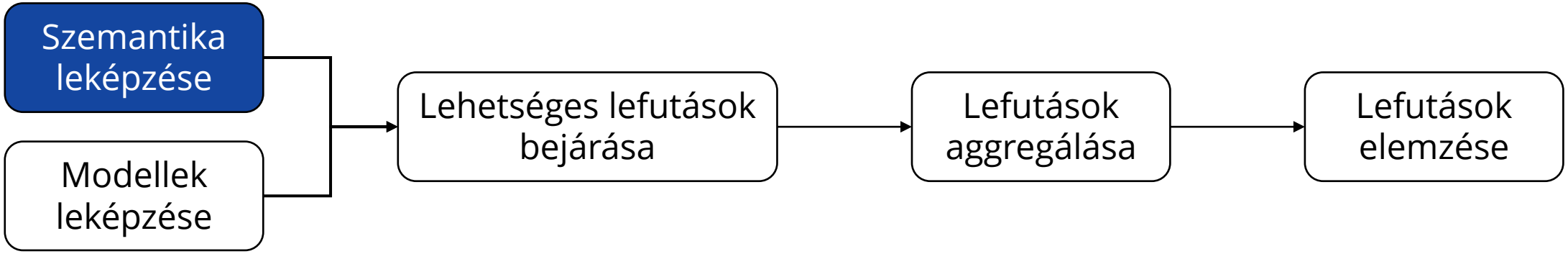
Szabvány validáció

- Lépések
  1. Teszt modellek → **formális** teszt modellek
  2. Formális módszerek → lehetséges lefutások **automatikus** előállítása
- Eredmények
  - Lehetséges lefutások vizualizálása
  - Szabvány validálása
- **Általános módszer** viselkedésmodell szabványokra
  - Pl. állapotgép, aktivitás
  - Esettanulmány: PSSM

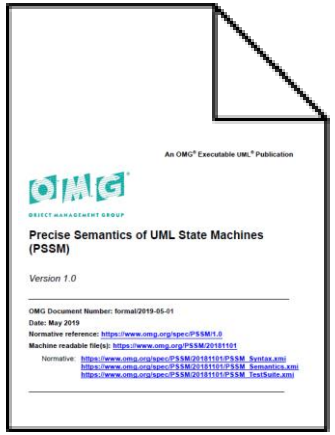
PSSM validációs folyamat



PSSM validációs folyamat



- PSSM operációs szemantika leképzése
  - Implicit komponensek (diszpécser, eseménysor)


An OMG® Executable UML® Publication

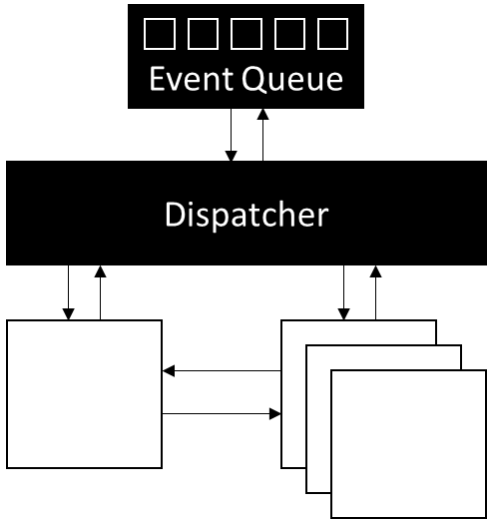
OMG

OBJECT MANAGEMENT GROUP

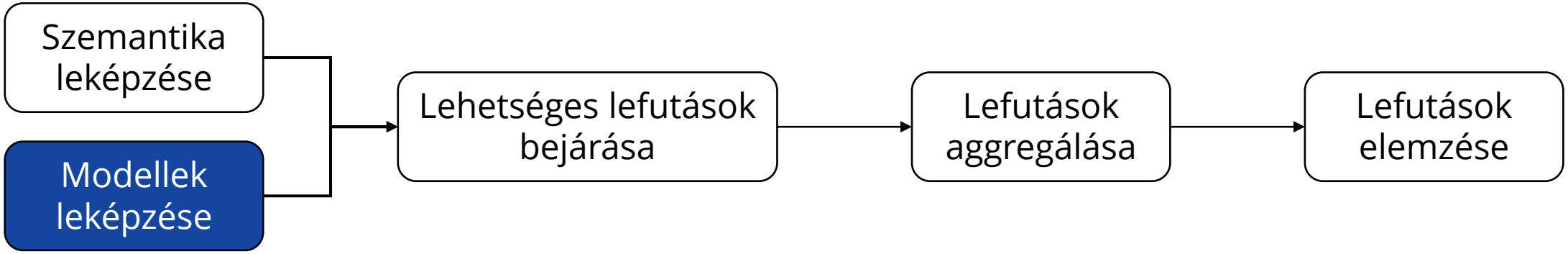
Precise Semantics of UML State Machines (PSSM)

Version 1.0

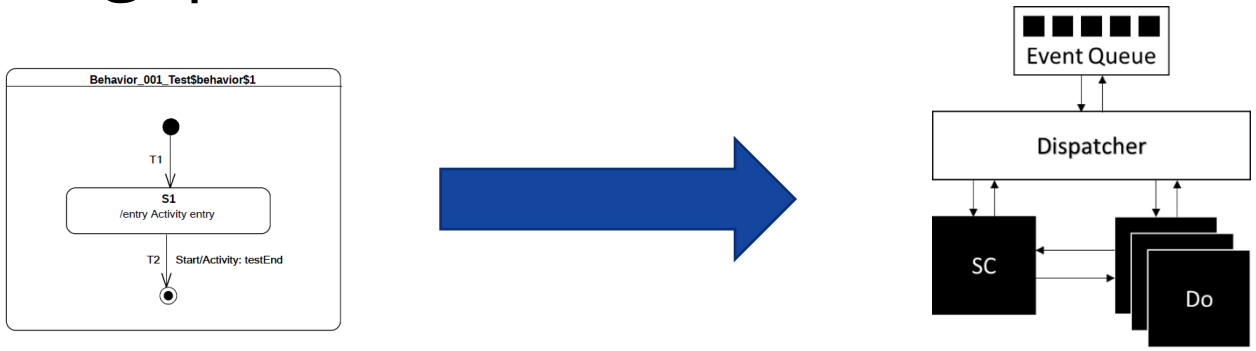
OMG Document Number: formal/2019-05-01
Date: May 2019
Normative reference: https://www.omg.org/spec/PSSM/1.0
Machine readable file(s): https://www.omg.org/PSSM/20181101
Normative: https://www.omg.org/spec/PSSM/20181101/PSSM_Syntax.xmi
https://www.omg.org/spec/PSSM/20181101/PSSM_Semantics.xmi
https://www.omg.org/spec/PSSM/20181101/PSSM_TestSuite.xmi



PSSM validációs folyamat



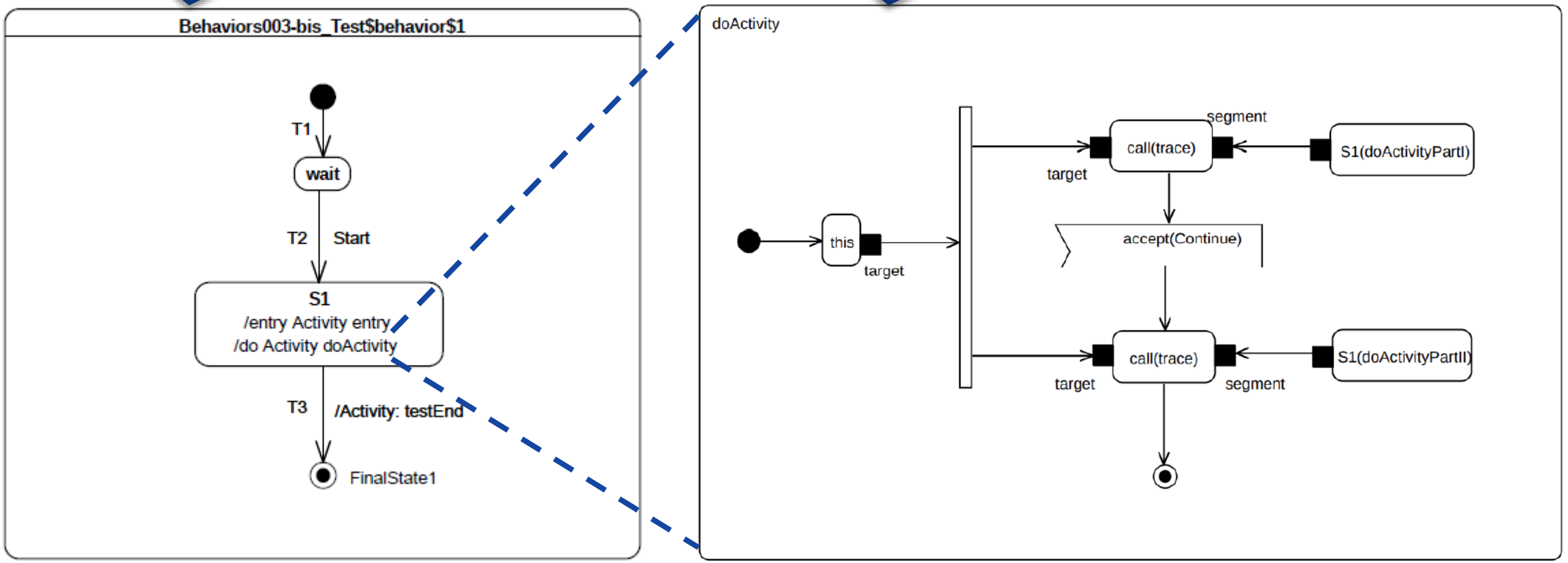
- Teszt modellek leképzése
  - Jelenleg még manuálisan, de szisztematikusan
  - Automatizálható (modelltranszformációkkal)
- Formális állapotgépek és aktivitások



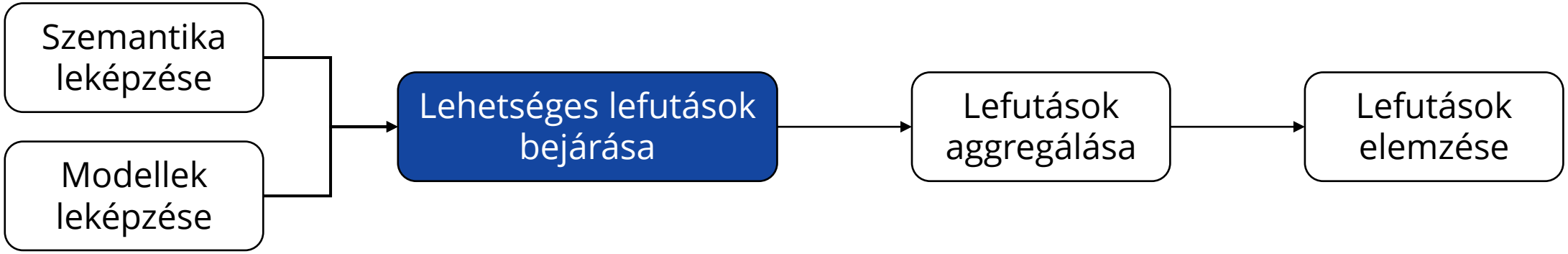
Modell példa (Behavior-003b)

Állapotgép

Aktivitás

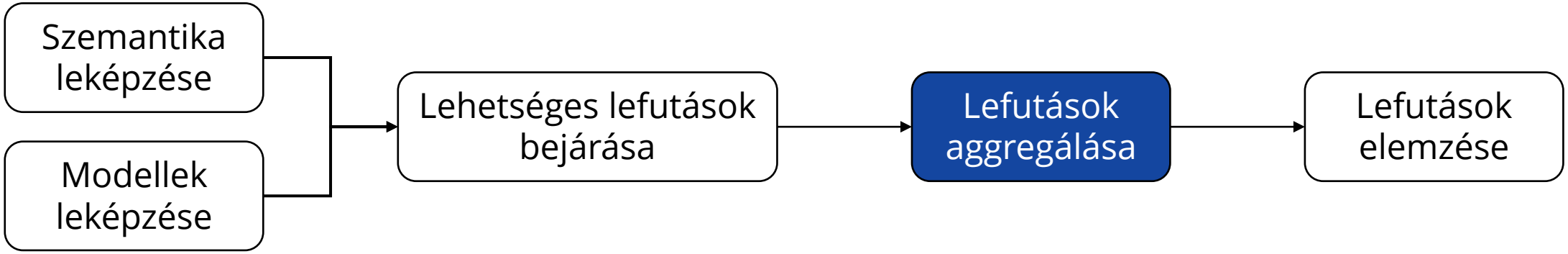


PSSM validációs folyamat

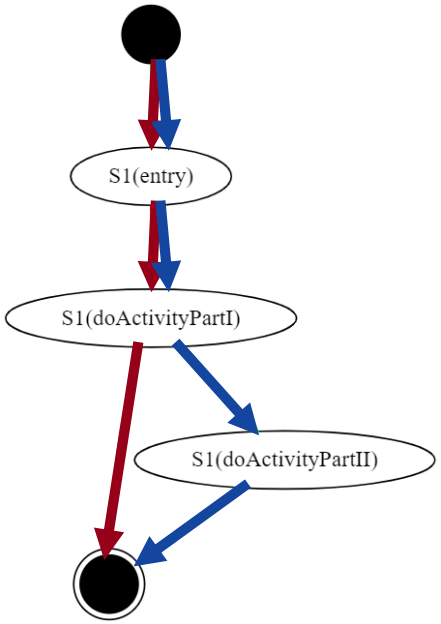


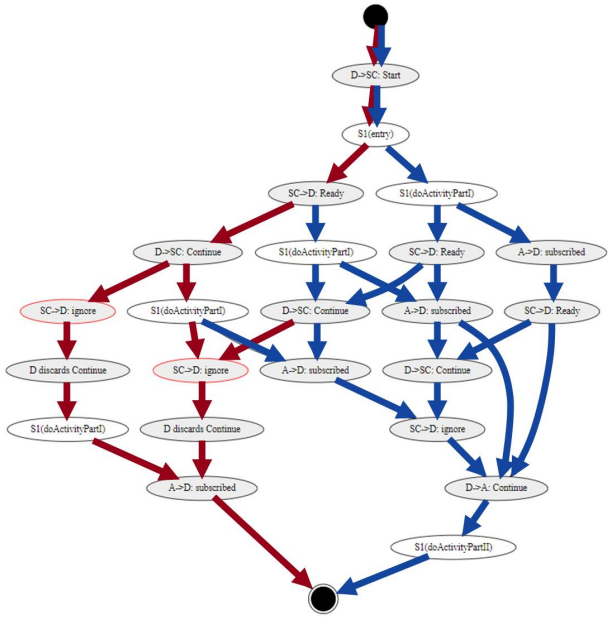
- Formális módszerek használata
- Lehetséges lefutások *kimerítő* bejárása

PSSM validációs folyamat



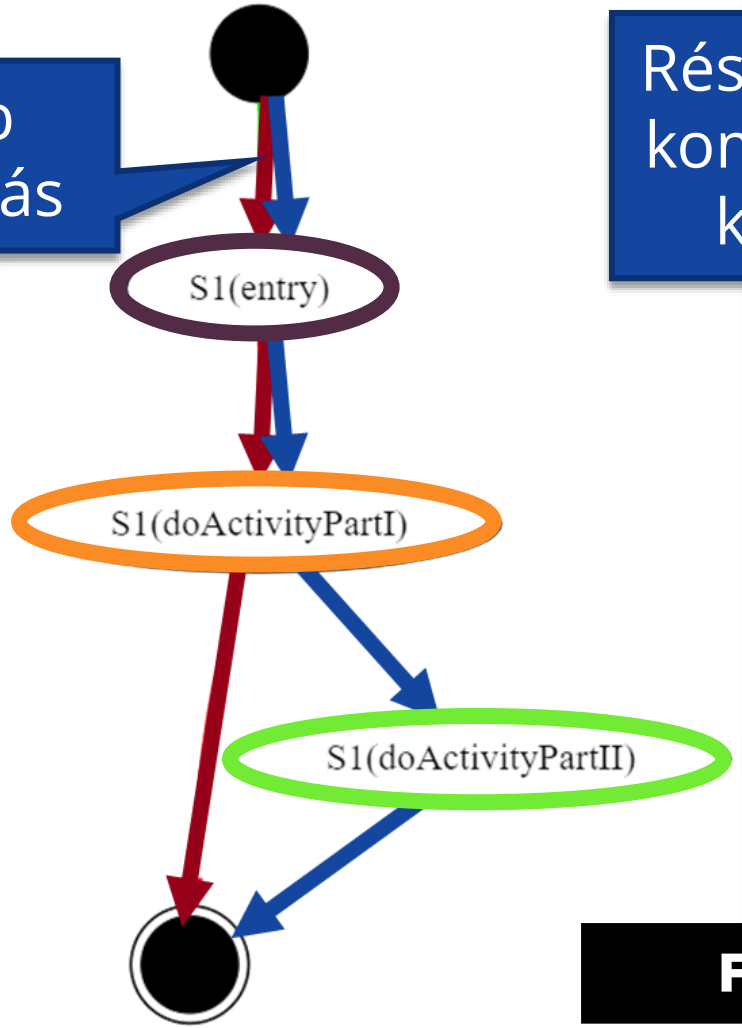
- Választható granularitás (megfigyelés részletessége)





Eltérő granularitás

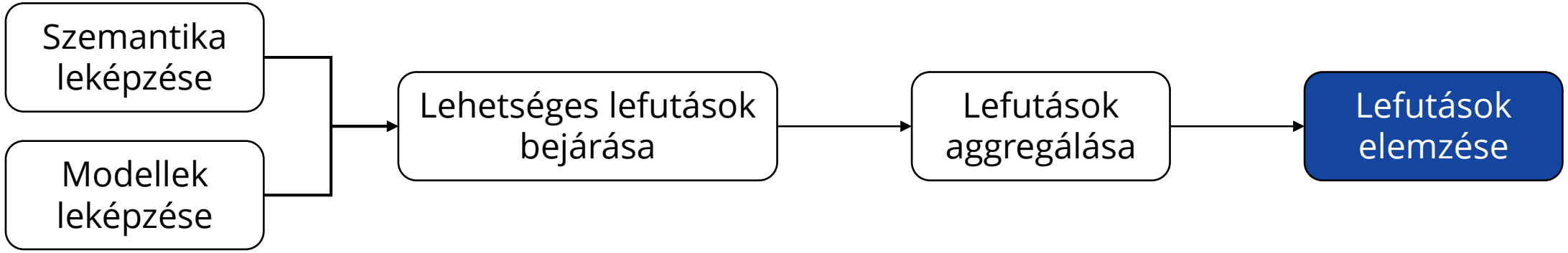
Durvább granularitás



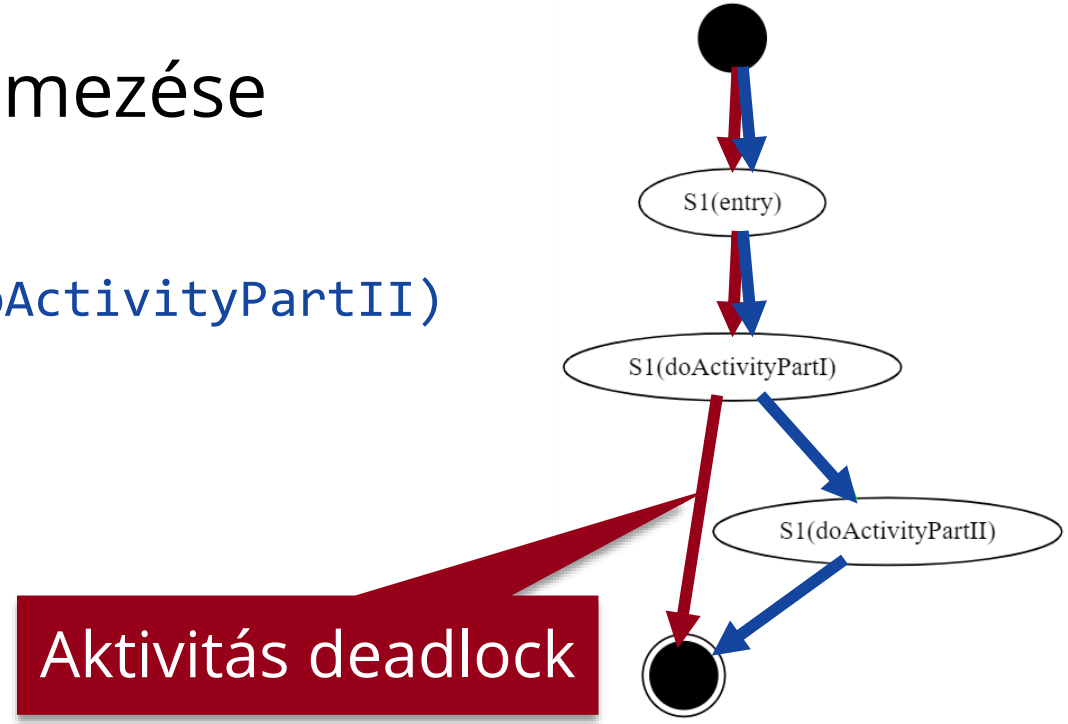
Részletesebb nézet: komponensek közti kommunikáció

Finomítás

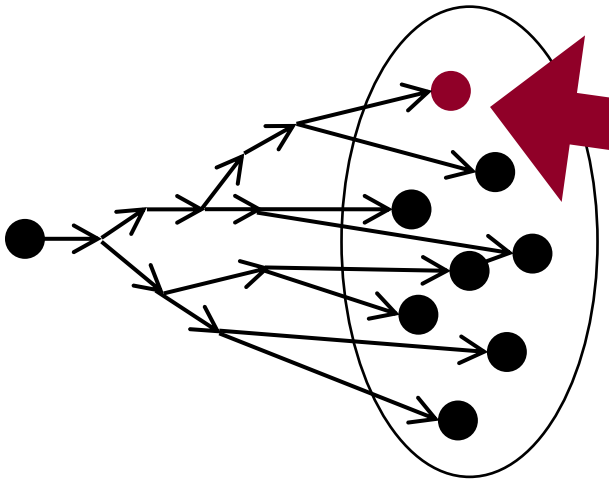
PSSM validációs folyamat



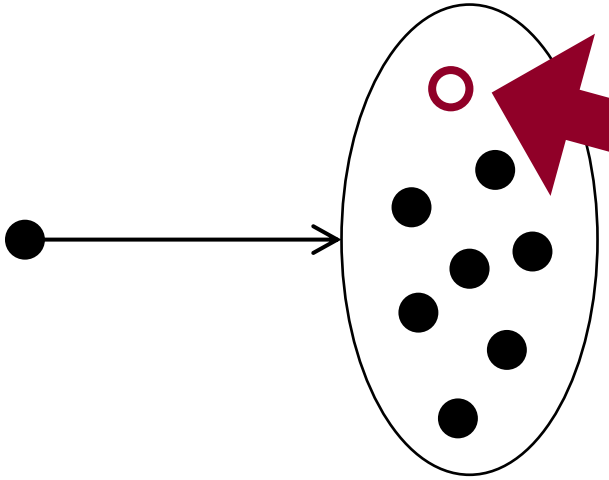
- Eredményül kapott lefutások értelmezése
- Összehasonlítás a szabvánnyal
  - `S1(entry)::S1(doActivityPartI)::S1(doActivityPartII)`
  - **`S1(entry)::S1(doActivityPartI)`**
    - Szemantika szerint szabványos lefutás
    - *Hiányzik* a Test Suite-ból



PSSM validációs folyamat

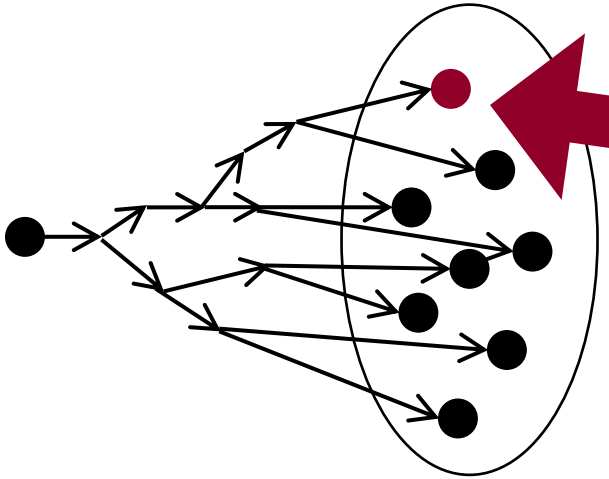


- PSSM operációs szemantika
  - Lehetséges lefutás

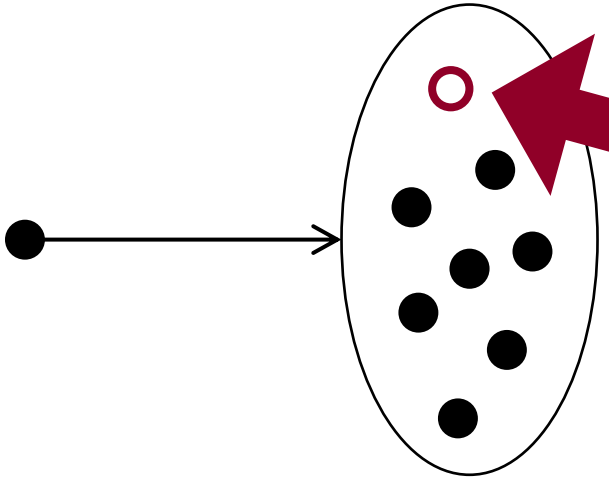


- PSSM Test Suite
  - Hiányzó lefutás

PSSM validációs folyamat



- PSSM operációs szemantika
  - Lehetséges lefutás

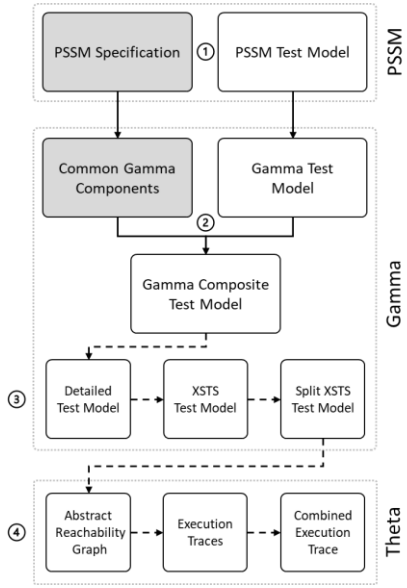


- PSSM Test Suite
  - Hiányzó lefutás

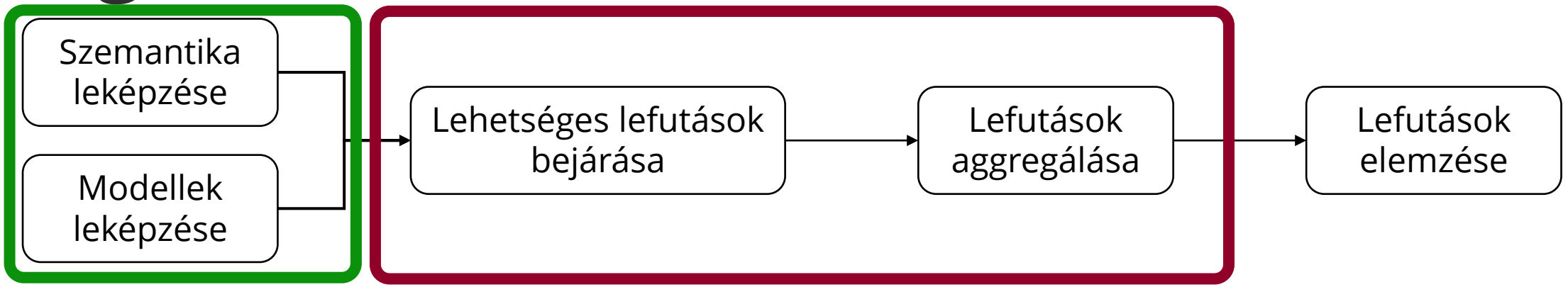
Következmények

- *Eszközök*: hibás konformancia eredmény
- *Mérnökök*: váratlan deadlock

Megvalósítás

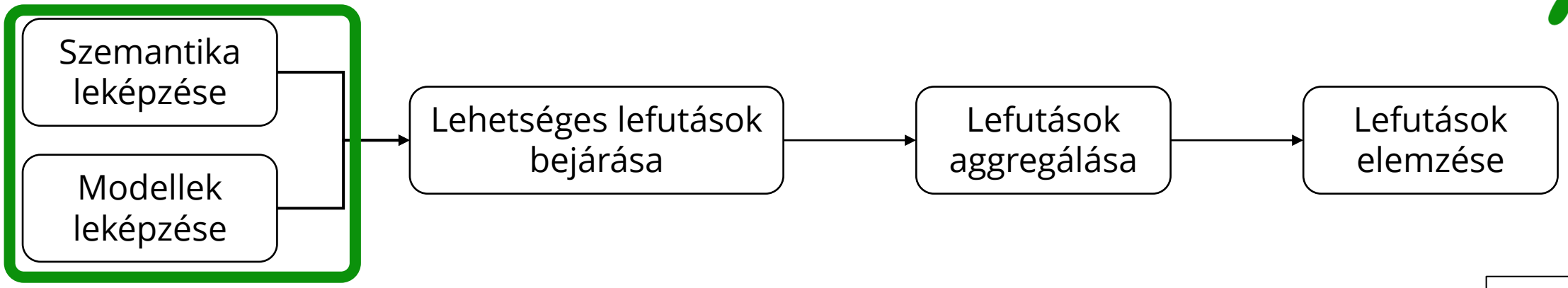


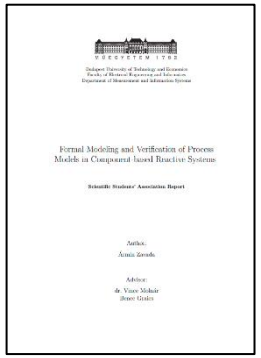
Megvalósítás



- Keretrendszerek részeként
  - Gamma állapotgép kompozíciós keretrendszer
    - Precíz, magas szintű modellezési nyelvek
    - Modelltranszformációk
  - Theta modellellenőrző keretrendszer
    - Formális modellek feldolgozása (formális verifikáció)
- Meglévő komponensek újrafelhasználása
- Nyílt forráskódú kontribúció

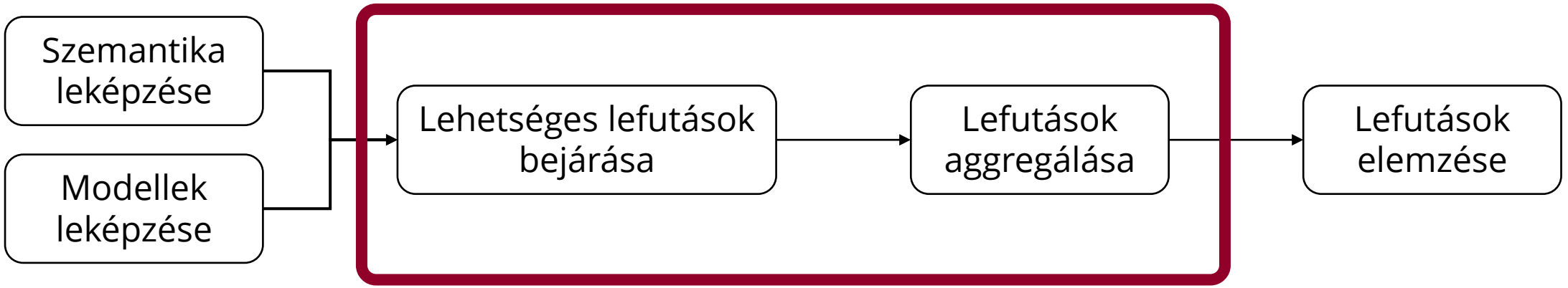
Gamma kontribúciók



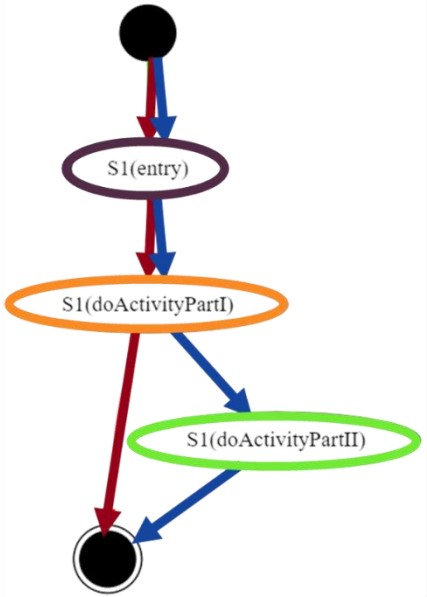


- **Viselkedés**
  - Állapotgép nyelv kiegészítése (log utasítás, internal transition)
  - Aktivitás nyelv továbbfejlesztése (TDK'21 bővítése)
- **Kompozíció**
  - Új aktivitás komponens bevezetése
- **Transzformáció**
  - Log utasítások injektálása
  - Gammában atomi lépések feldarabolása (nemdeterminizmus, átlapolódás)
  - Aszinkron rendszerek támogatása

Theta kontribúciók



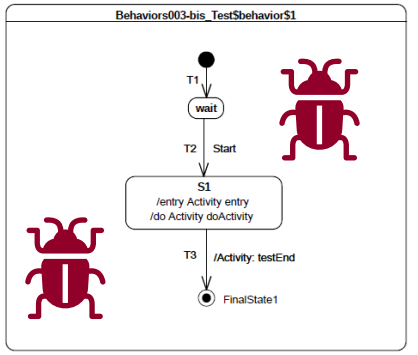
- **Modellszimulátor komponens**
  - Formális modellek tetszőleges bejárása
  - Konfigurálható granularitás
- **Állapottér teljes bejárása**
  - Modellszimulátor automatikus vezérlése
- **Lefutások feldolgozása**
  - Aggregálás egységes adatszerkezetbe
  - Kompakt, intuitív vizualizáció



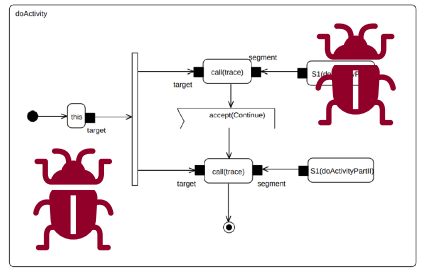
UML PSSM validáció esettanulmány

- PSSM teszt modellek leképezése
  - 44/103 modell
  - Legfontosabb modellelemek
  - Négy különböző granularitás
- Eredmények kiértékelése
  - **Ekvivalens** (30 modell)
    - Különböző granularitásokkal bemutatva
  - **PSSM szabványban talált hibák** (4 modell)
    - Aktivitások szinkronizálása
    - Ortogonális régiók sorrendezése
  - **Gamma limitációk** (10 modell)
    - Fork-join konstrukciók
    - Emlékező állapotok speciális használata (history)

UML PSSM



Állapotgép



Aktivitás

Bővebb kiértékelés a dolgozatban megtalálható

Összefoglalás

Elméleti eredmények

- Új megközelítés a modellezési nyelvek konformancia ellenőrzésére
- UML PSSM → Gamma leképezés
- Gamma aktivitás komponens bevezetése
- Formális modellek teljes lefutási gráfjának szisztematikus generálása

Gyakorlati eredmények

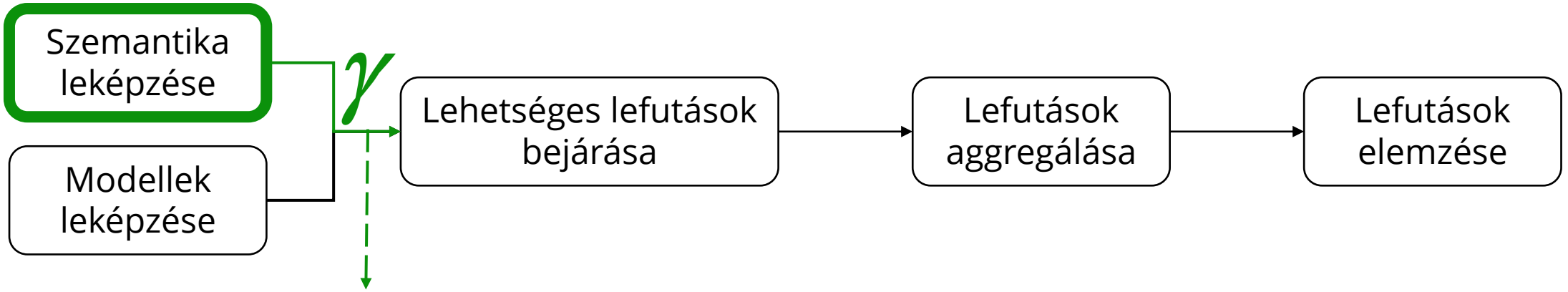
- Gamma eszköz kiegészítése
  - Modellezési nyelvek
  - Modelltranszformációk
- Theta eszköz kiegészítése
  - Formális modell szimulátor
  - Összes lefutás bejárása
- UML PSSM validáció esettanulmány kiértékelése
  - 44/103 tesztmodell leképezése
  - Hibák a szabványban

Továbbfejlesztési lehetőségek

- UML PSSM → Gamma leképezés automatizálása
- További modellelemek támogatása (pl. defer)
- Új esettanulmányok további nyelveken (pl. SysMLv2, SCXML)

Kérdések

1. PSSM konform állapotgépeket használó modellek általános validációja



- UML PSSM → Gamma leképezés + Gamma kiegészítések
- Gamma modell → Gamma funkciók
  - Modellellenőrzés (különböző backendek)
  - Kódgenerálás, tesztgenerálás
- Fókuszban a szabványok validációja volt
  - Az UML PSSM állapotgép-ellenőrzés részeredmény

2. A végrehajtási utak generálásának teljesítménye

- Gyakorlati alkalmazhatóság határa
  - Cél: szabvány validáció
    - Célirányos tesztek → egyszerű modellek
    - Kevésbé időkritikus
  - Nem tapasztaltunk limitációt → részletesen nem vizsgáltuk
  - Komplexitás a nemdeterminizmusoktól függ (pl. párhuzamosság)

Test Case		Time			
		Baseline		Detailed	
		Target	+Dispatcher	Target	+Dispatcher
History	001-D	1673	1509	1465	1648
	001-C	1346752	1408954	5125193	5739389
	001-B	124593	128966	439728	457177
	001-A	164138	170967	582949	609148
Final	001	122012	108968	564486	575411
Join	002	51108	57484	200990	198577
	001	45816	50858	210934	207330
Fork	002	1224	1143	1227568	1353007
Choice	005	61003	62564	235694	238359
	004	48908	52202	198542	204715
	003	39402	35465	133625	137988
	002	66450	75704	138119	146138
	001	88323	93678	329609	343179
Exiting	005	72006	70936	280906	297655
	003	42175	44355	168979	179954
	001	38466	42466	162601	167920
Entering	011	1254	1263	415416	417155
	010	303654	321621	1904130	2098313
Event	005	35432	39281	139654	138514
	018	83382	76457	262054	275134
	017-B	1254669	1290075	3697127	4022404
	017-A	33149	35332	141189	143549
	016-A	70158	67359	259740	266835
	015	63848	77424	201111	218394
	010	154888	166689	547928	560129
	009	322642	354685	1230666	1296129
	008	58501	71331	214213	238988
	002	35902	50639	150691	157965
	001	22086	43544	87902	93084
Transition	022	94499	151677	371111	409194
	020	79240	136302	304146	335689
	019	108086	152975	431324	457501
	017	4494013	5255950	16901423	17219816
	016	32040	76548	141416	154379
	015	225894	273536	672787	718464
	010	73220	115877	256480	273756
	007	85001	132313	315010	361875
	001	41346	75100	135022	148341
Behavior	004	1087615	1107949	3160934	3316438
	003-B	729293	802883	2187976	2271588
	003-A	659800	699857	2067522	2197197
	002	22394	48599	85445	104434
	001	20674	43186	91502	92329

- CircleVM – 32 mag – a 128Gb memória – párhuzamosan 16 mérés
- Leghosszabb: ~4,7 h – Második leghosszabb: 1,6 h – medián: ~3min

		Baseline		Detailed	
		Time			
		Target	+Dispatcher	Target	+Dispatcher
History	001-D	1673	1509	1465	1648
	001-C	1346752	1408954	5125193	5739389
	001-B	124593	128966	439728	457177
	001-A	164138	170967	582949	609148
Final	001	122012	108968	564486	575411
Join	002	51108	57484	200990	198577
	001	45816	50858	210934	207330
Fork	002	1224	1143	1227568	1353007
Choice	005	61003	62564	235694	238359
	004	48908	52202	198542	204715
	003	39402	35465	133625	137988
	002	66450	75704	138119	146138
	001	88323	93678	329609	343179
Exiting	005	72006	70936	280906	297655
	003	42175	44355	168979	179954
	001	38466	42466	162601	167920
Entering	011	1254	1263	415416	417155
	010	303654	321621	1904130	2098313
Event	005	35432	39281	139654	138514
	018	83382	76457	262054	275134
	017-B	1254669	1290075	3697127	4022404
	017-A	33149	35332	141189	143549
	016-A	70158	67359	259740	266835
	015	63848	77424	201111	218394
	010	154888	166689	547928	560129
	009	322642	354685	1230666	1296129
	008	58501	71331	214213	238988
	002	35902	50639	150691	157965
	001	22086	43544	87902	93084
Transition	022	94499	151677	371111	409194
	020	79240	136302	304146	335689
	019	108086	152975	431324	457501
	017	4494013	5255950	16901423	17219816
	016	32040	76548	141416	154379
	015	225894	273536	672787	718464
	010	73220	115877	256480	273756
	007	85001	132313	315010	361875
	001	41346	75100	135022	148341
	04	1087615	1107949	3160934	3316438
	03-B	729293	802883	2187976	2271588
	03-A	659800	699857	2067522	2197197
	02	22394	48599	85445	104434
	01	20674	43186	91502	92329

Gyors egyszerű modellek esetén

- CircleVM – 32 mag – a 128Gb memória – párhuzamosan 16 mérés
- Leghosszabb: ~4,7 h – Második leghosszabb: 1,6 h – medián: ~3min

Test Case				Detailed	
		Tar		Target	+Dispatcher
Behavior	001	206	6	91502	92329
	002	223	9	85445	104434
	003-A	659	57	2067522	2197197
	003-B	729	83	2187976	2271588
	004	1087	49	3160934	3316438
	001	413	0	135022	148341
	007	85001	132313	315010	361875
	010	73220	115877	256480	273756
	015	225894	273536	672787	718464
Transition	016	32040	76548	141416	154379
	017	4494013	5255950	16901423	17219816
	019	108086	152975	431324	457501
	020	79240	136302	304146	335689
	022	94499	151677	371111	409194
	001	22086	43544	87902	93084
	002	35902	50639	150691	157965
	008	58501	71331	214213	238988
	009	322642	354685	1230666	1296129
	010	154888	166689	547928	560129
Event	015	63848	77424	201111	218394
	016-A	70158	67359	259740	266835
	017-A	33149	35332	141189	143549
	017-B	1254669	1290075	3697127	4022404
	018	83382	76457	262054	275134
	005	35432	39281	139654	138514
Entering	010	303654	321621	1904130	2098313
	011	1254	1263	415416	417155
Exiting	001	38466	42466	162601	167920
	003	42175	44355	168979	179954
	005	72006	70936	280906	297655
Choice	001	88323	93678	329609	343179
	002	66450	75704	138119	146138
	003	39402	35465	133625	137988
	004	48908	52202	198542	204715
Fork	005	61003	62564	235694	238359
	002	1224	1143	1227568	1353007
Final	001	122012	108968	564486	575411
Join	002	51108	57484	200990	198577
	001	45816	50858	210934	207330
History	001-A	164138	170967	582949	609148
	001-B	124593	128966	439728	457177
	001-C	1346752	1408954	5125193	5739389
	001-D	1673	1509	1465	1648

Time

Lassabb részletes modellek esetén

- CircleVM – 32 mag – a 128Gb memória – párhuzamosan 16 mérés
- Leghosszabb: ~4,7 h – Második leghosszabb: 1,6 h – medián: ~3min

Nemdeterminizmus függvényében

Test Case	Baseline	+Dispatcher	Target	+Dispatcher
Time			**Detailed**	
Behavior				
002	22394	48599	85445	104434
001	20674	43186	91502	92329
004	1087615	1107949	3160934	3316438
003-B	729293	802883	2187976	2271588
003-A	659800	699857	2067522	2197197
007	85001	132313	315010	361875
001	41346	75100	135022	148341
Transition				
015	225894	273536	672787	718464
010	73220	115877	256480	273756
016	32040	76548	141416	154379
017	4494013	5255950	16901423	17219816
019	108086	152975	431324	457501
010	79240	136302	304146	335689
012	94499	151677	371111	409194
001	22086	43544	87902	93084
008	58501	71331	214213	238988
009	322642	354685	1230666	1296129
010	154888	166689	547928	560129
015	63848	77424	201111	218394
016-A	70158	67359	259740	266835
017-A	33149	35332	141189	143549
017-B	1254669	1290075	3697127	4022404
018	83382	76457	262054	275134
005	35432	39281	139654	138514
010	303654	321621	1904130	2098313
001	38466	42466	162601	167920
011	1254	1263	415416	417155
003	42175	44355	168979	179954
005	72006	70936	280906	297655
003	39402	35465	133625	137988
002	66450	75704	138119	146138
001	88323	93678	329609	343179
005	61003	62564	235694	238359
004	48908	52202	198542	204715
002	1224	1143	1227568	1353007
001	45816	50858	210934	207330
002	51108	57484	200990	198577
001	122012	108968	564486	575411
001-A	164138	170967	582949	609148
001-B	124593	128966	439728	457177
001-C	1346752	1408954	5125193	5739389
001-D	1673	1509	1465	1648
History				

- CircleVM – 32 mag – a 128Gb memória – párhuzamosan 16 mérés
- Leghosszabb: ~4,7 h – Második leghosszabb: 1,6 h – medián: ~3min

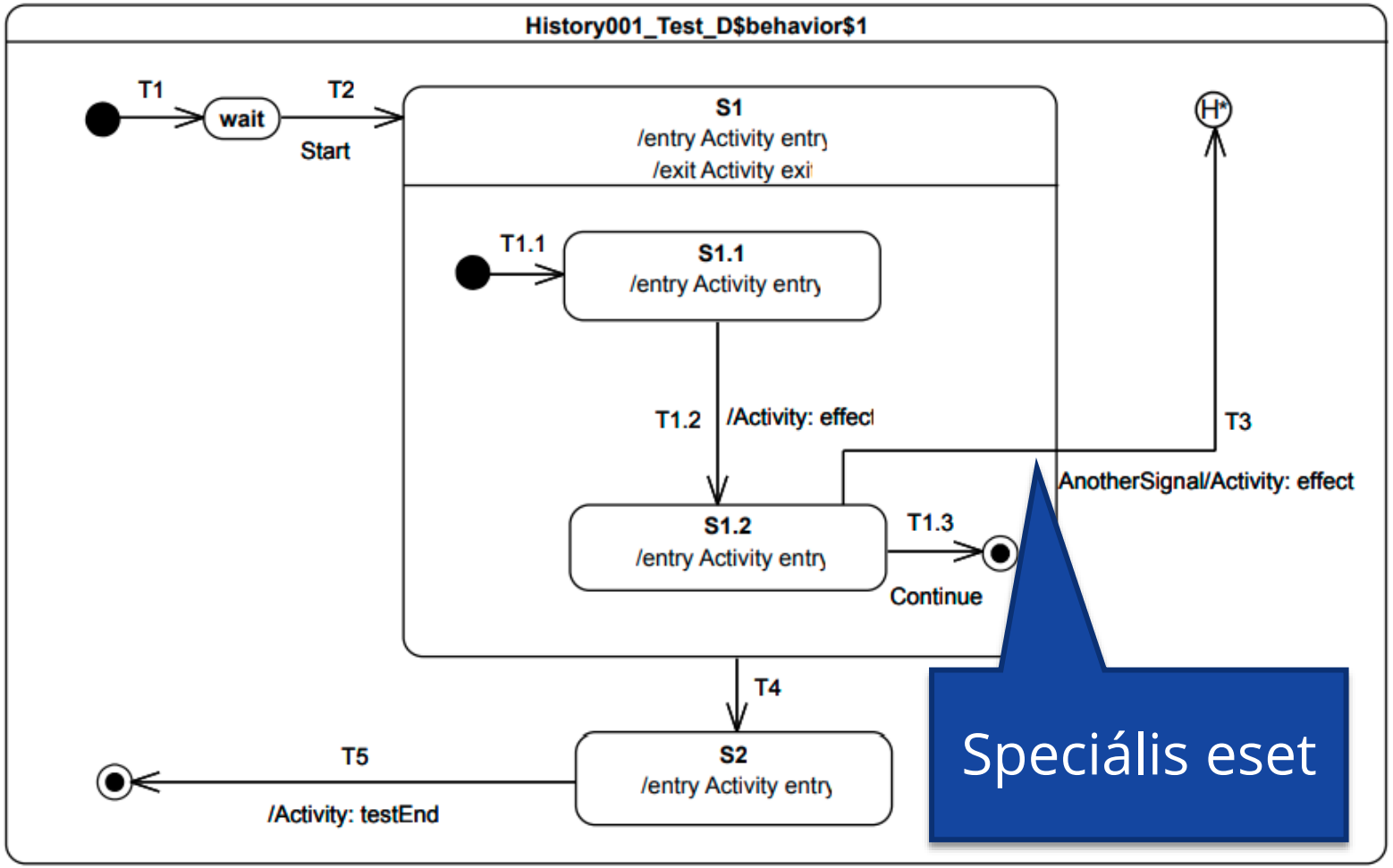
2. A végrehajtási utak generálásának teljesítménye

- Gyakorlati alkalmazhatóság határa
  - Cél: szabvány validáció
    - Célirányos tesztek → egyszerű modellek
    - Kevésbé időkritikus
  - Nem tapasztaltunk limitációt → részletesen nem vizsgáltuk
  - Komplexitás a nemdeterminizmusoktól függ (pl. párhuzamosság)

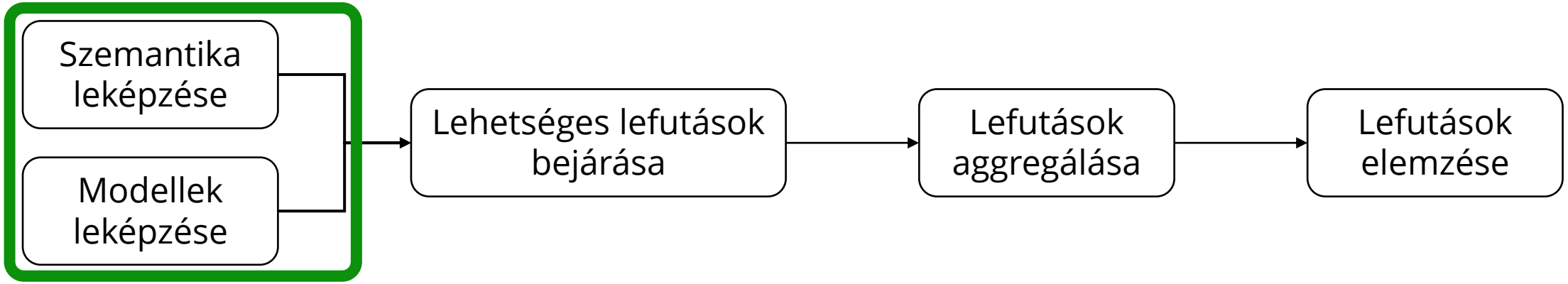
- Hatékonyság fokozása
  - Konfigurálható: durvább granularitás → gyorsabb lefutás
  - Mögöttes modellellenőrző hatékonysága

3. Képes-e helyesen feldolgozni a módszer a H* elemet többszörösen összetett állapotok esetén is?

- Gamma limitáció
  - Speciális eset nincs támogatva
- Egyéb esetben támogatott
  - Pl. `History 001-B` tesztmodell



4. Mennyire alkalmazható a módszer más modellezési nyelvekre?



- A megközelítés viselkedési modellekre általános
  - Pl. állapotgépek, aktivitások
  - Moduláris: csupán a Gamma leképzést kell kicserélni
- További példa nyelvek
  - SysMLv2 (már létezik leképzés egy részhalmazra)
  - SCXML (más hallgató már dolgozik a Gamma leképzésen)

5. A „változók megfelelő választása esetén…” pontosan mit jelent, hogyan érhető el?

- Formális modellben változókat követünk
  - Tetszőleges részhalmaz választható
- Transzformáció során minden elem változókra képződik le
  - Állapotgép változói
  - Események
  - Vezérlési helyek
  - Log utasítások
  - …