MŰSZER AUTOMATIKA CÉGCSOPORT

Modellellenőrzés a vasút automatikai rendszerek fejlesztésében

XIX. Közlekedésfejlesztési és beruházási konferencia

Bükfürdő 2018.04.25-27.

Tartalom

1. Formális módszerek – state of the art
2. Esettanulmány
3. Kutatási téma célja, elért eredmények
4. Modellellenőrzés

MŰSZER AUTOMATIKA CÉGCSOPORT

FORMÁLIS MÓDSZEREK

State of the art

Formális módszerek (FM)

MŰSZER AUTOMATIKA CÉGCSOPORT

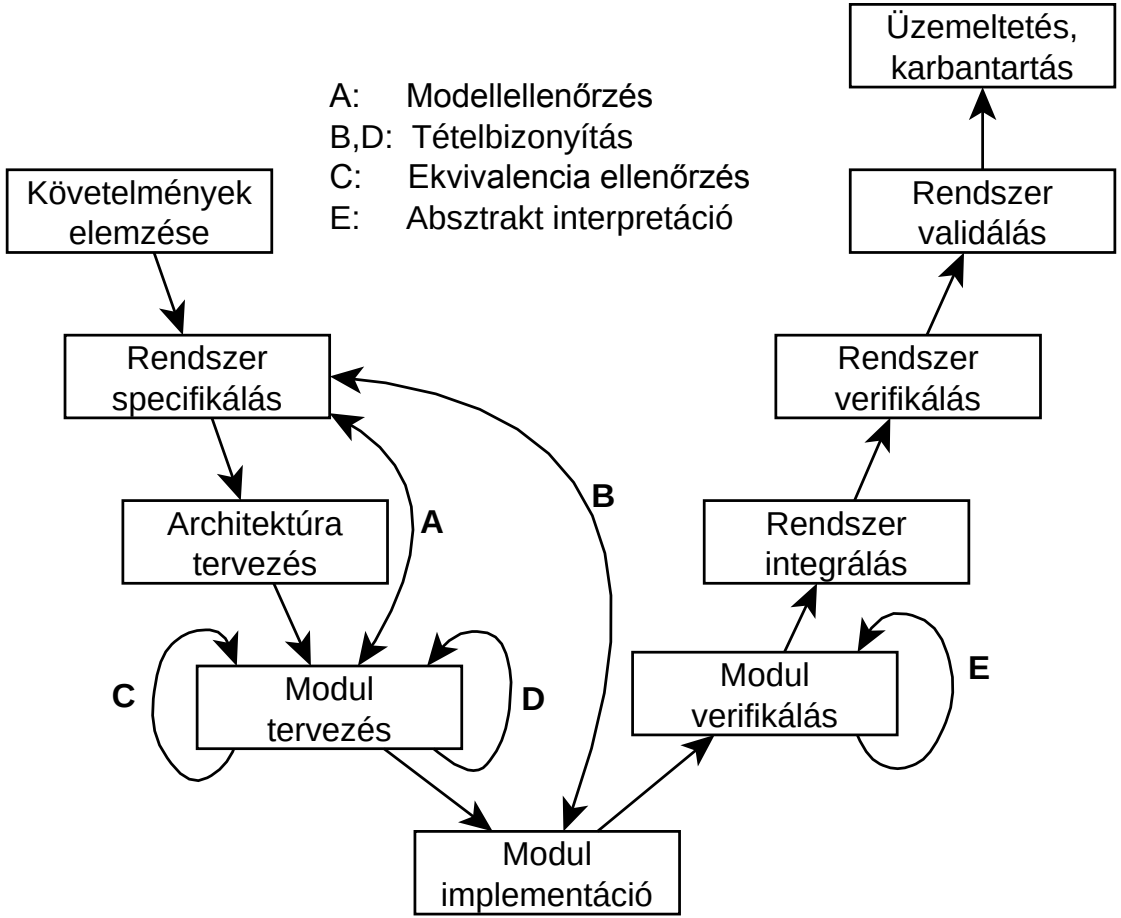
Definíció

- Matematikán alapuló technikák
  - diszkrét matematika
  - matematikai logika
- SW és HW rendszerek specifikációja, tervezése és verifikációja
- Kemény számítási módszerek

Célok

- Kritikus rendszerek
- Szigorú specifikáció, tervezés és verifikáció támogatása
  - Hiányzó pontos specifikáció
  - Ellenőrizetlen tervek
  - Specifikációs, tervezési, implementációs hibák
  - HW, konfigurációs, kezelői hibák a működő termékben
  - Tesztelés, szimuláció nem garantáltan teljeskörű
- Komplex viselkedésű rendszerek modellezése

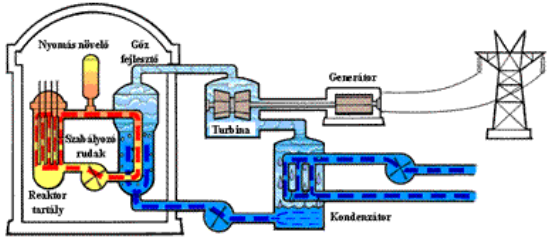
FM – Verifikációs technikák



[Formális verifikációs technikák az életciklusban]

FM – Példák I.

- Atomenergetika
  - PRISE, Paks (primary-secondary leaking)
  - Biztonsági folyamat verifikációja
  - Modellellenőrzés, Színezett Petri hálók



  - PLC alapú vezérlő szoftver verifikációja (CERN)
  - Specifikációs-verifikációs folyamat definiálása
  - Modellellenőrzés

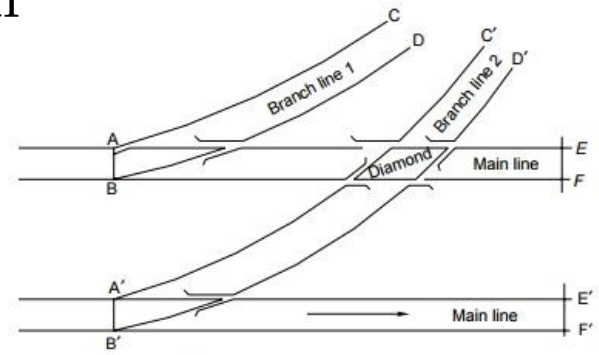
- Űrkutatás
  - Űrrepülőgép navigációs követelmények formalizálása
  - Tételbizonyítás, PVS (Prototype Verification System) specifikációs nyelv

Hivatkozások: PRISE CERN NASA

FM – Példák II.

- Beléptető kapu vezérlő viselkedésének leírása B-módszerrel
  - Újrahasznosítható modellek
  - Hatékonysági problémák
    (pl. B modell transzformációja létra diagramra)

- Kétvágányú pálya elágazásának modellezése CSP és B formalizmusok együttes használatával
  - Az esemény- és állapot-alapú modellezés kombinációja előnyös
  - A kétféle formalizmus nehézséget okoz az értelmezésben



Hivatkozások: Beléptető kapu Elágazás

FM – Példák III.

- Elektromechanikus jelfogó probléma megoldása Z-módszerrel
  - A Z jelölésrendszer korlátai (pl. idő kezelés, konkurens viselkedés)
  - A Z-t célszerű egy másik formalizmussal kombinálni (pl. CSP, Communicating Sequential Processes)

- ETCS távolság és sebességfelügyelet
  - SRS formalizálása SPARK nyelven
  - Tételbizonyítás Alt-Ergo használatával
  - A kódot célszerű a tételbizonyítás szellemében írni
  - A tételbizonyító elvesztheti a kvantorok feletti uralmat
  - Kód módosítása: túl sok munkaidő az újbóli bizonyítás

Hivatkozások: Jelfogó ETCS

MŰSZER AUTOMATIKA CÉGCSOPORT

ESETTANULMÁNY

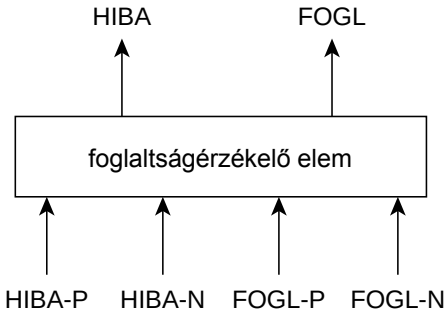
Foglaltság-érzékelő elem

Követelmény specifikáció (részlet)

MŰSZER AUTOMATIKA CÉGCSOPORT

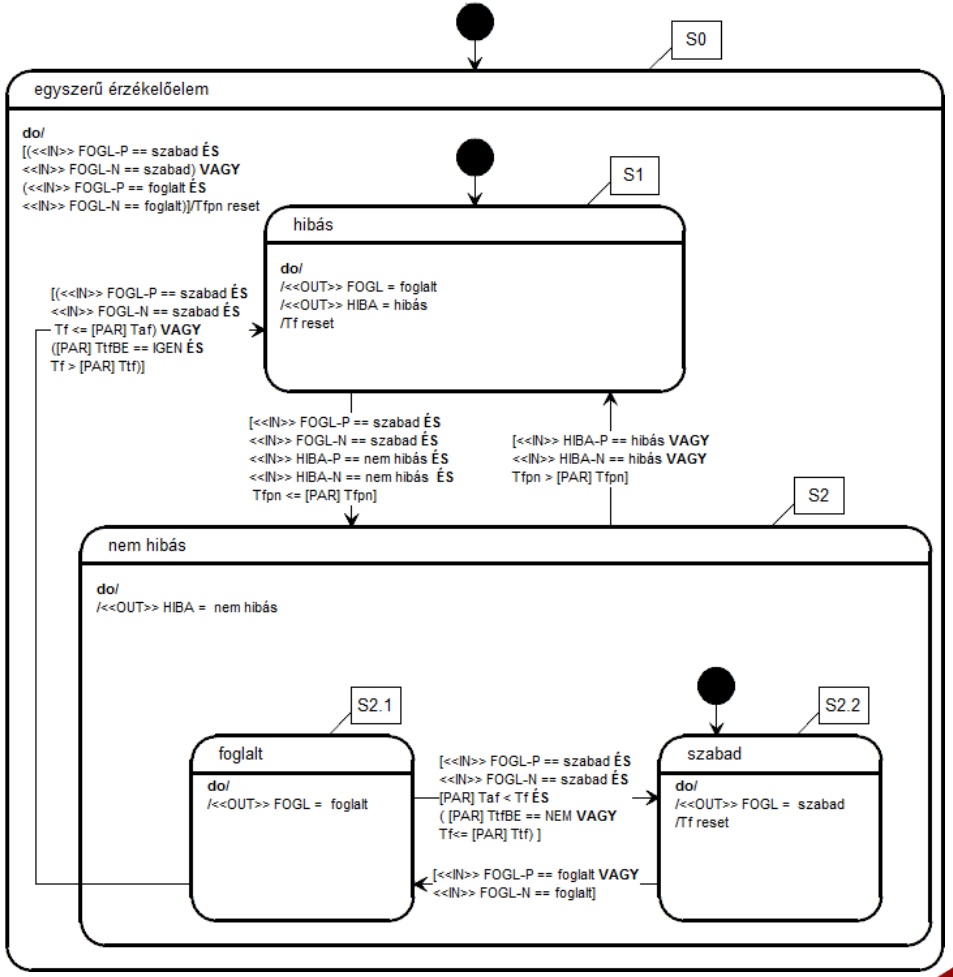
Fejezet	Id.	Követelmény
…	…	…
Általános követelmények	REQ-005	A komponenseknek rendelkezniük kell típusazonosítóval és egyedi azonosítóval.
…	…	…
Definíciók	REQ-062	Az érzékelőelem egy olyan eszköz, amely a hatókörében érzékeli a vonat jelenlétét.
…	…	…
Funkcionális követelmények	REQ-085	Ha az érzékelőelem hibás, akkor a kimenetein mindig hibásat és foglaltat kell adnia.
…	…	…

Részletes tervezés (részletek)



Egyszerű érzékelőelem bemenete			
Jelölés	**Értékkészlet**	**Alapértelmezett érték**	**Magyarázat**
FOGL-P	[foglalt | szabad]	szabad	foglaltság, ponált
FOGL-N	[foglalt | szabad]	szabad	foglaltság, negált
HIBA-P	[hibás | nem hibás]	nem hibás	hiba, ponált
HIBA-N	[hibás | nem hibás]	nem hibás	hiba, negált
Megjegyzés: az alapértelmezett érték a bemenet nem létezése esetén értelmezett.			

Egyszerű érzékelőelem kimenete			
Jelölés	**Értékkészlet**	**Kezdőérték**	**Magyarázat**
FOGL	[foglalt | szabad]	lásd. állapotgép	foglaltság
HIBA	[hibás | nem hibás]	lásd. állapotgép	hiba
Megjegyzés: a kezdőérték a modul kimenetein inicializáskor beállítandó érték.			



A specifikáció értékelése

MŰSZER AUTOMATIKA CÉGCSOPORT

Részletes terv

- Leírások formalizáltsági szintje
  - Informális
  - Félformális
  - Formális
- Véges számú elemkészlet
  - Állapotgép
  - Időd iagram
  - Stb.

Követelmény specifikáció

- Követelmények formalizálhatósága
  - Formalizálható
  - Modellezési szint függő
  - Nem formalizálható

Konklúzió

A specifikáció és a tervek jó kiindulási alapot jelentenek az automatizált formalizáláshoz!

A KUTATÁS TÉMA ÖSSZEFOGLALÁSA

Automatizált modellellenőrzési bemenet generálás és a modellellenőrzés eredményének szakterületi mérnöki fogalomrendszerre való visszavetítése a vasúti automatikai rendszerek fejlesztésének támogatására

Motiváció, cél, módszer

MŰSZER AUTOMATIKA CÉGCSOPORT

- Motiváció
  - FM vs. Szakterületi mérnökök
  - Kihívások (rendszer integráció, verifikációs eredmények)
- Cél
  - A szakterületi mérnökök számára a matematikai és számítástudományi háttér elrejtése
- Módszer
  - Meglévő módszerek, eszközök egységes, gyakorlatban hatékonyan alkalmazható eszközkészletbe szervezése

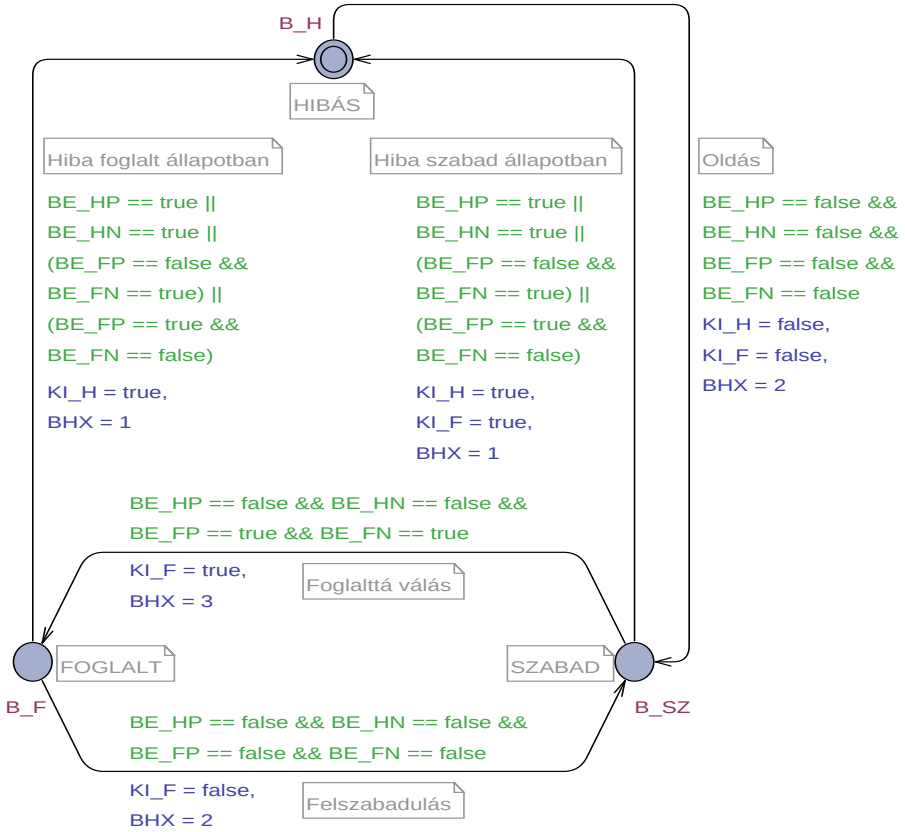
Elért eredmények I.

- Követelmények formalizálása

1.	**Eredeti követelmény**	**Id.**		**Természetes nyelvű leírás**			
		REQ-085		Ha az érzékelőelem hibás, akkor a kimenetein mindig hibásat és foglaltat kell adnia.			
2.	**Előkészített követelmény**	**CTL Op.**	**HA**	**Kifejezés**	**AKKOR**	**Kifejezés**	**Modell-ellenőrzés elvárt kimenete**
		AG	+	<<BH>> B_H == hibás	+	(<<KI>> HIBA == hibás) *ÉS* (<<KI>> FOGL == foglalt)	Igaz
3./a.	**PDN forma**	AG		(Det.B_F=1)	–>	(DET.KI_F_F=1 & DET.KI_H_H=1)	Igaz
3./b.	**UPPAAL forma**	A[]		(BHX == 1)	imply	((KI_H == true) && (KI_F == true))	Igaz

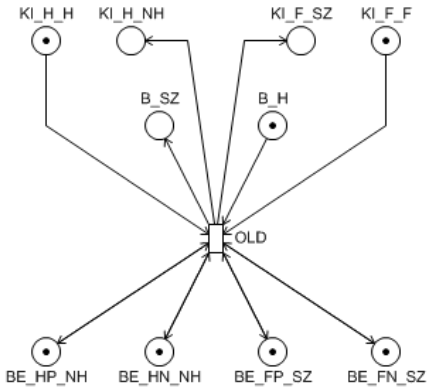
Elért eredmények II.

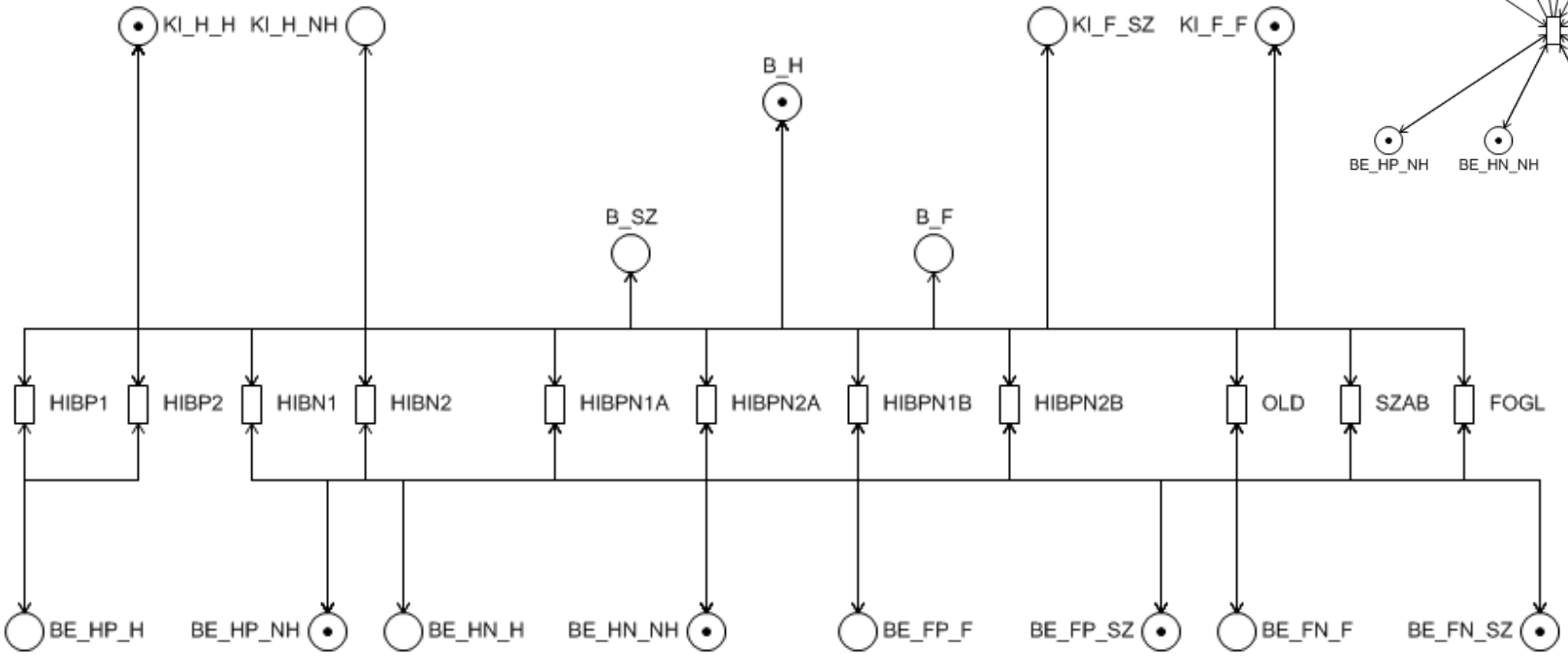
- Érzékelőelem UPPAAL automata modellje



Elért eredmények III.

- Érzékelőelem Petri-háló modellje



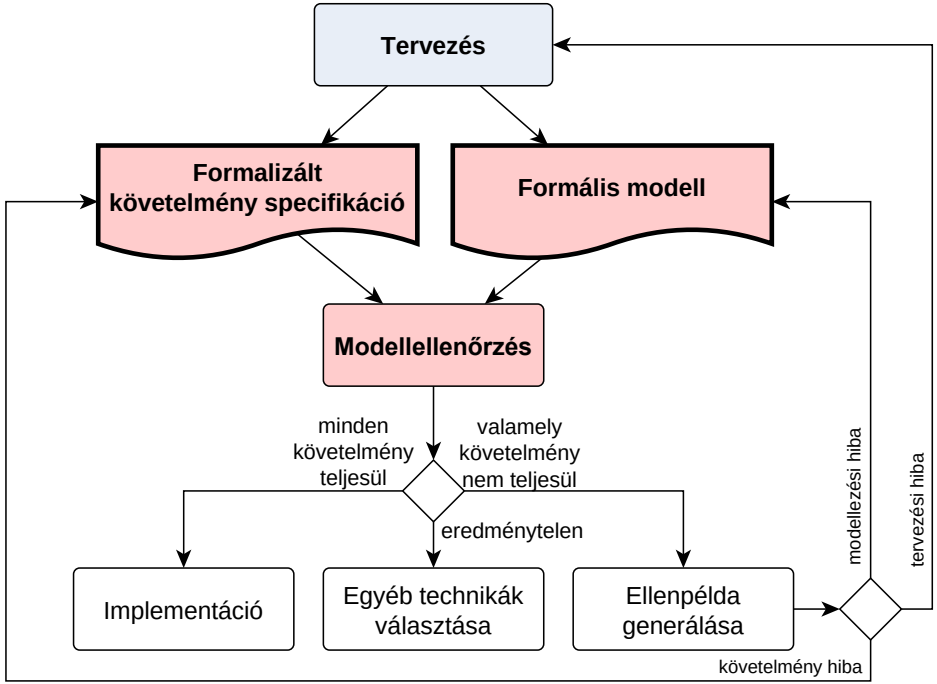


MODELLELLENŐRZÉS

Ellenpéldák visszavetítése a mérnöki leírások fogalomrendszerére

Problémafelvetés

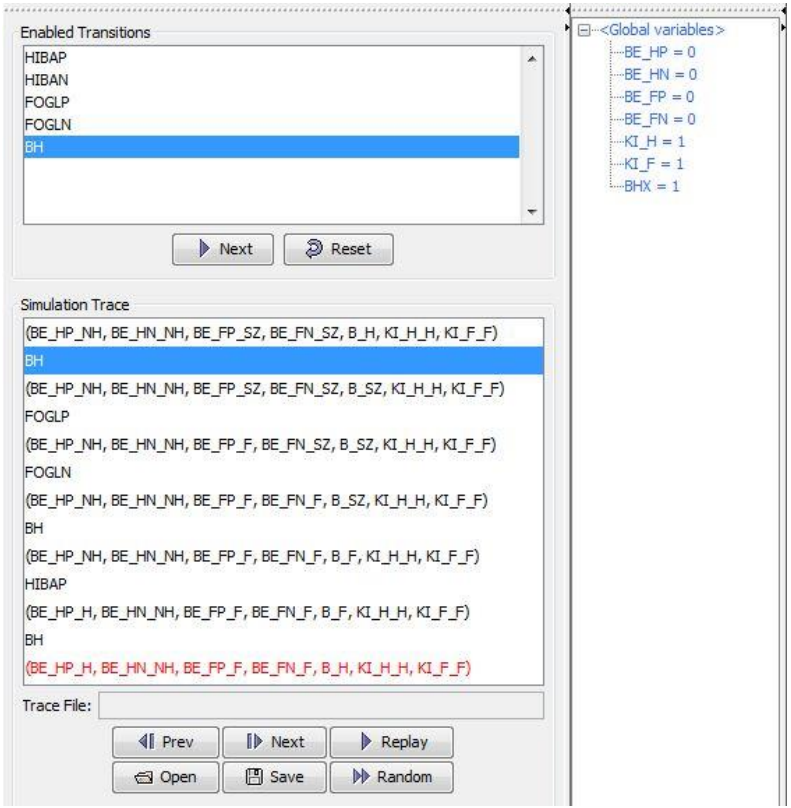
- A modellellenőrzés eredményének visszavetítése a szakterületi mérnökök által használt fogalmakra
- Hol keressük a nem-megfelelőséget?



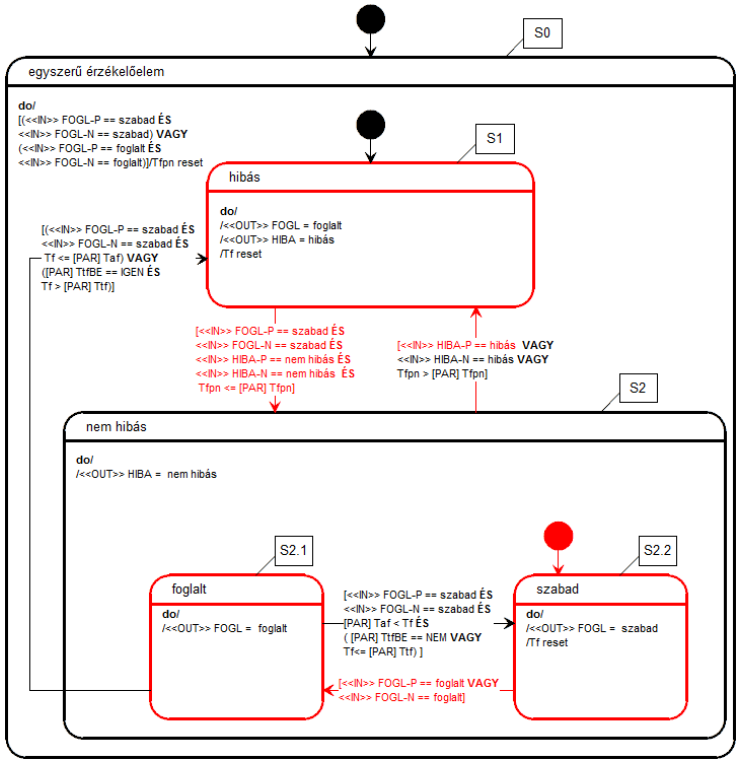
Példa visszavetítésre

MŰSZER AUTOMATIKA CÉGCSOPORT

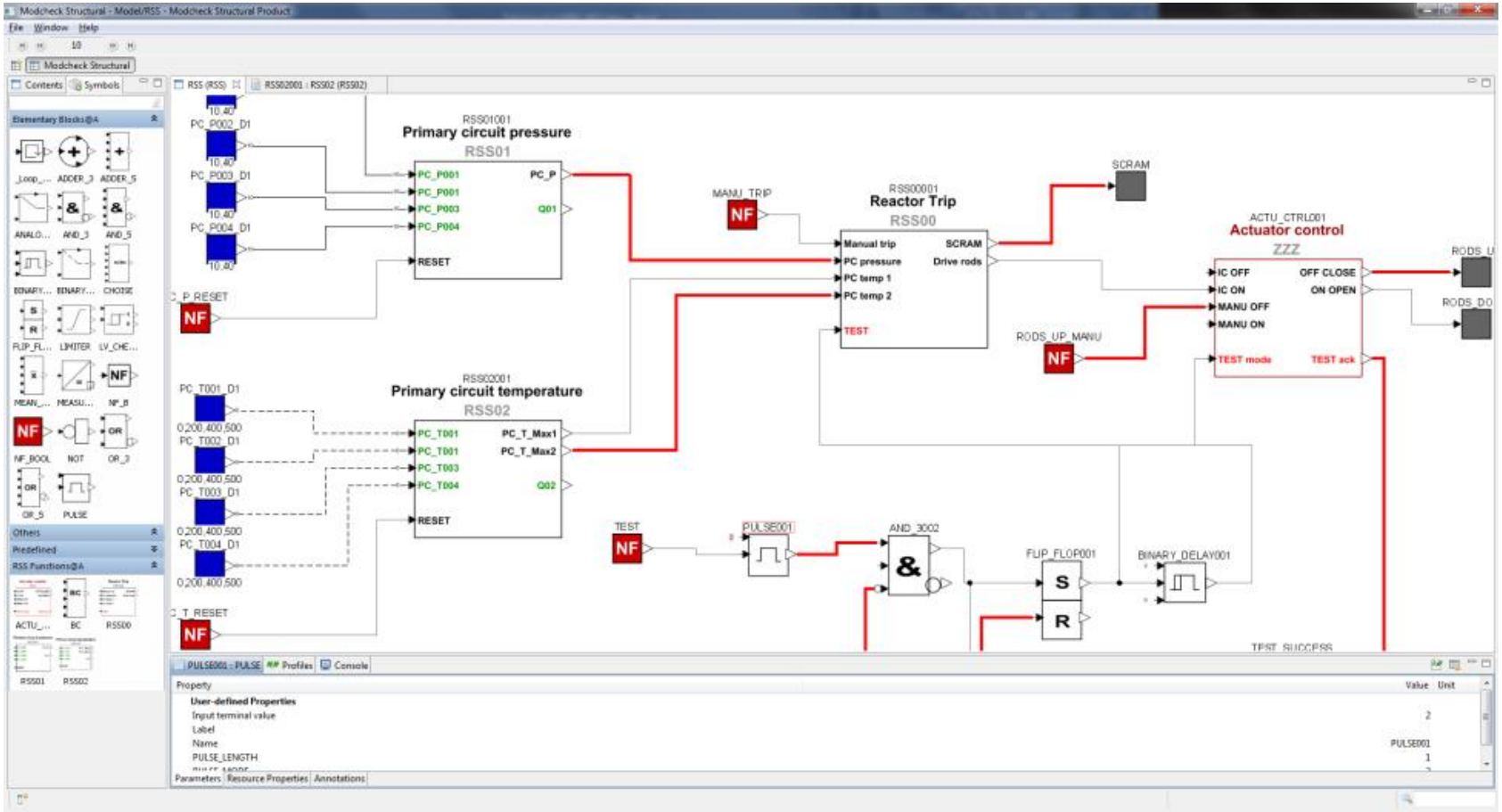
UPPAAL ellenpélda transzformációja



S1→S2.2→S2.1→S1



Hogyan csinálják mások?



Hivatkozások: [MODCHK]

MŰSZER AUTOMATIKA CÉGCSOPORT

TANULSÁGOK

Az elért eredmények összefoglalása,kihívások

Összefoglalás

MŰSZER AUTOMATIKA CÉGCSOPORT

- Tanulságok:
  - Nem célszerű a szakterületi mérnökök FM továbbképzése
    - Hatékonyság
    - Költségek (idő, erőforrás, stb.)
  - Célszerű kombinált formális módszer csomagot alkalmazni
    - Esemény és az állapot alapú leírás egyidejűleg
- Kihívások:
  - Domain specifikus mesterséges nyelv (követelmények)
  - A formalizmusok, eszközök korlátai és azok kezelése
  - Állapottér növekedés (vagy akár robbanás)
    - Időzítések, konfigurációs elemek, rendszerintegráció

Köszönöm a figyelmet!

Műszer Automatika Kft.
2040 Budaörs, Komáromi u. 22.
www.muszerautomatika.hu
mautom@muszerautomatika.hu
(23) 365-280, (23) 414-922, (23) 414-923

Lukács Gábor
vezető fejlesztő
Közlekedés Automatizálási Csoport
lukacs.gabor@mktm.hu
+36 20 665 1078

Budapesti Műszaki és Gazdaságtudományi Egyetem
Közlekedés- és Járműirányítási Tanszék
Formális Módszerek Kutatócsoport