ProRIS-E
Formális verifikációs módszerek

Prolan-VKE: Elosztott logikájú vasúti elektronikus biztosítóberendezés fejlesztése

Dr. Graics Bence
Dr. Simon Balázs és Golarits Zsigmond diái alapján

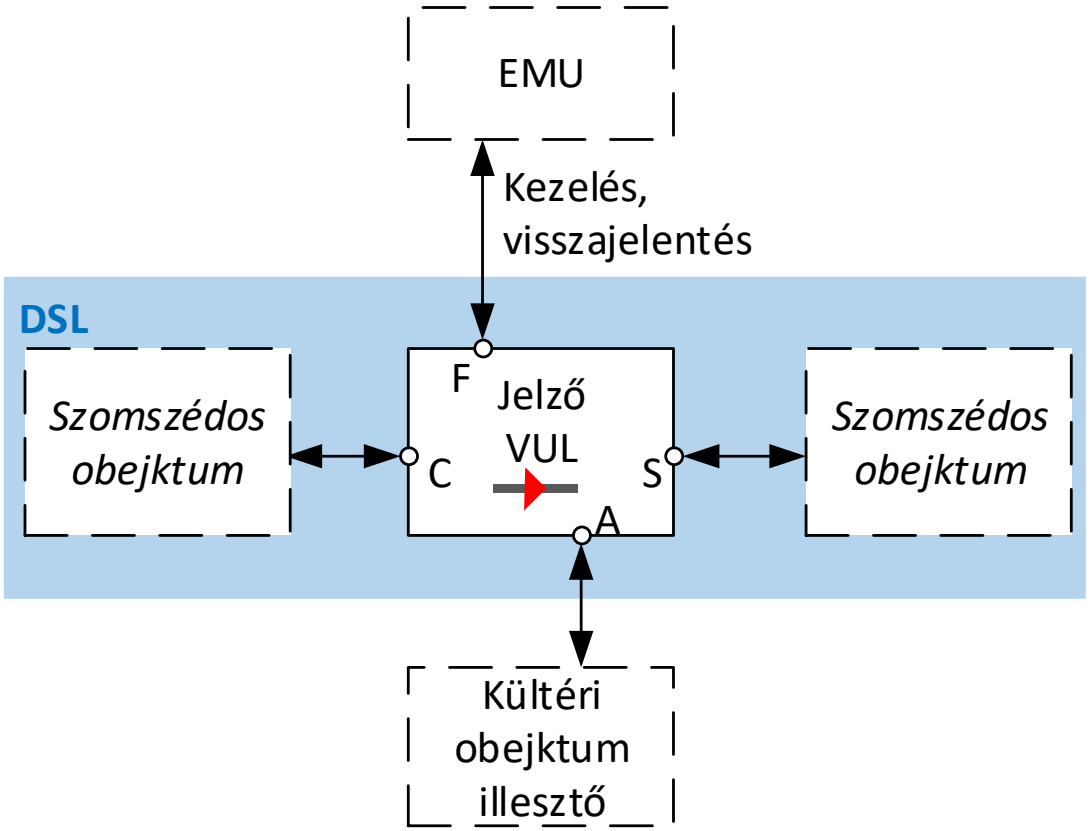
MŰEGYETEM 1782

Budapest University of Technology and Economics
Department of Artificial Intelligence Systems Engineering
Critical Systems Research Group

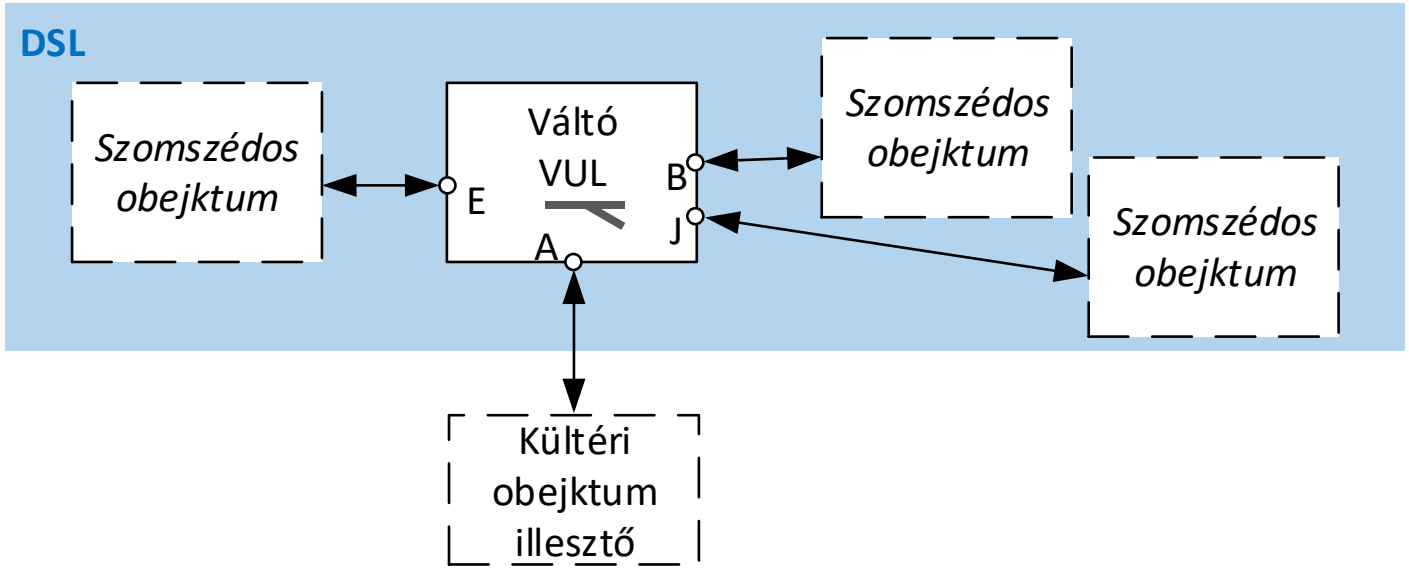
ftsrg

Objektumok

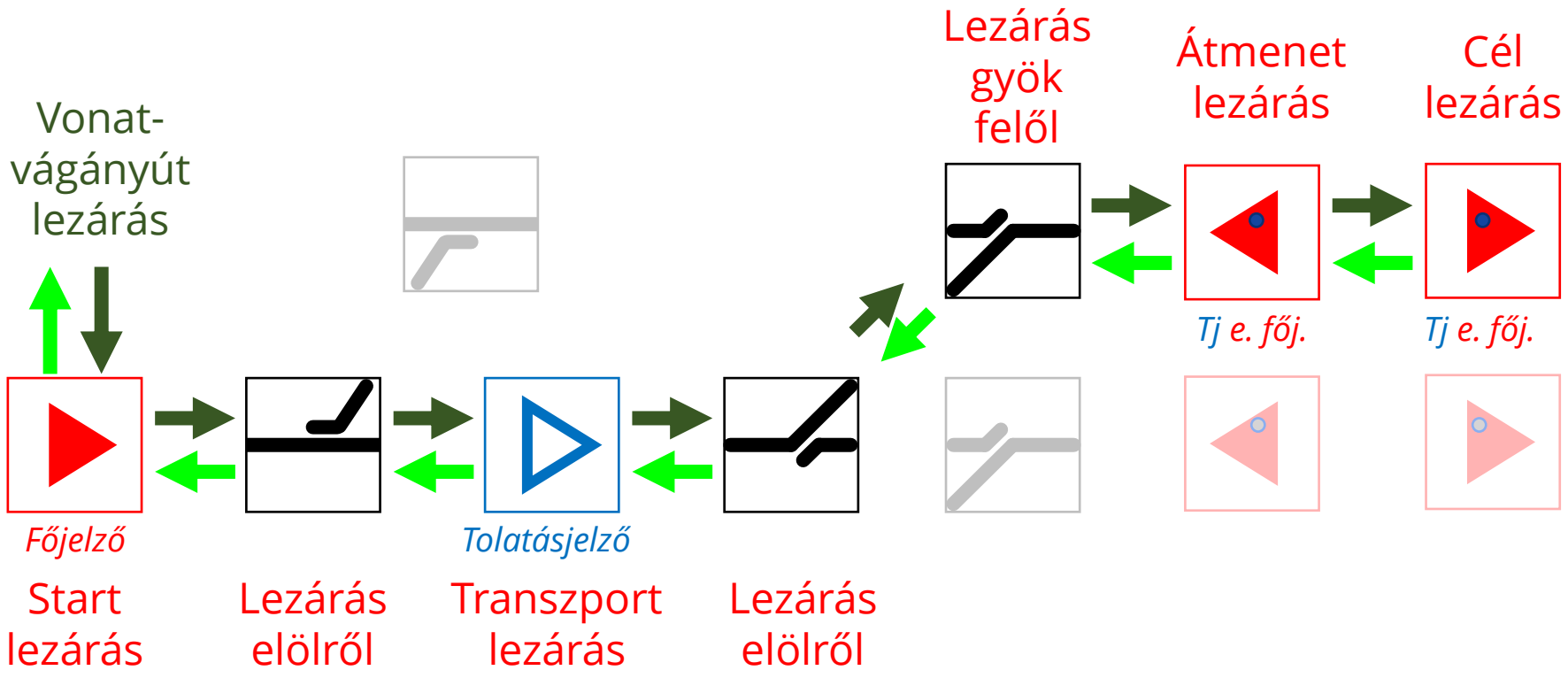
Jelző



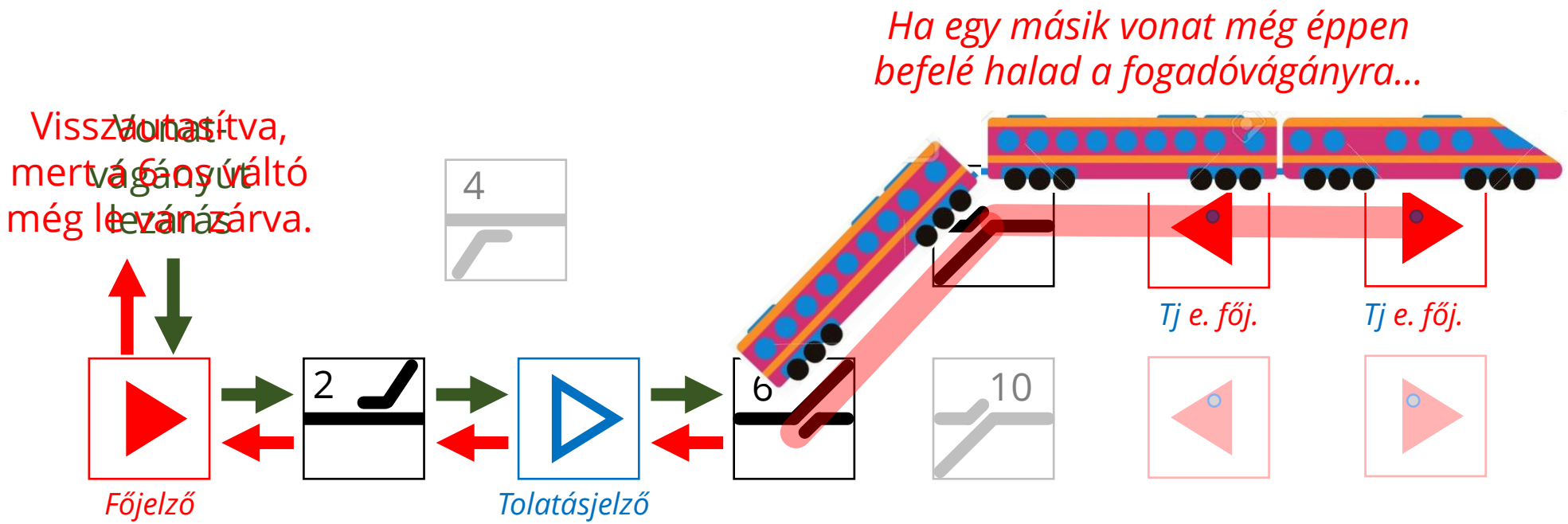
Váltó



Funkció: sikeres vágányút lezárás



Sikertelen vágányút lezárás

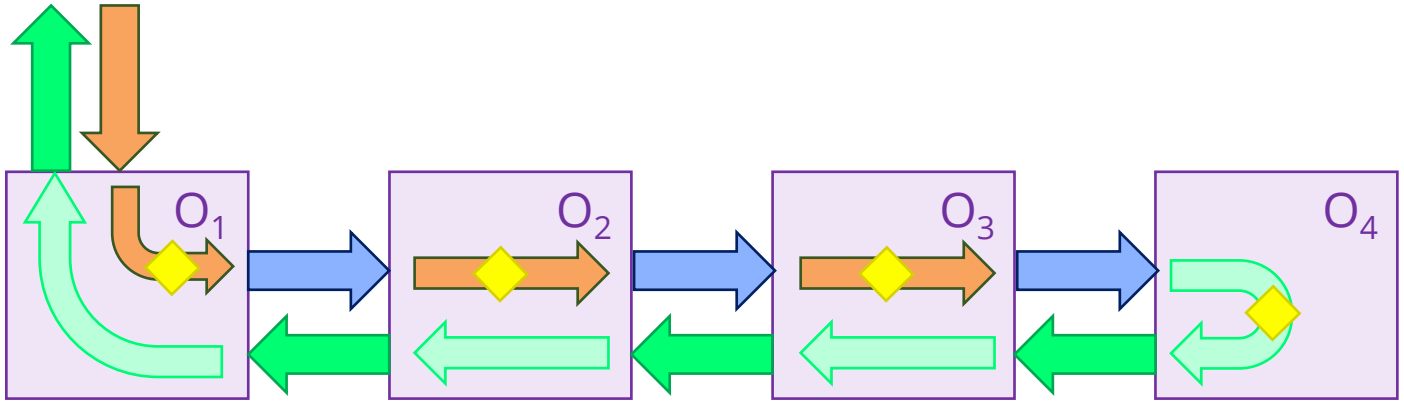


Prolan Interlocking Language (PIL)

Célok

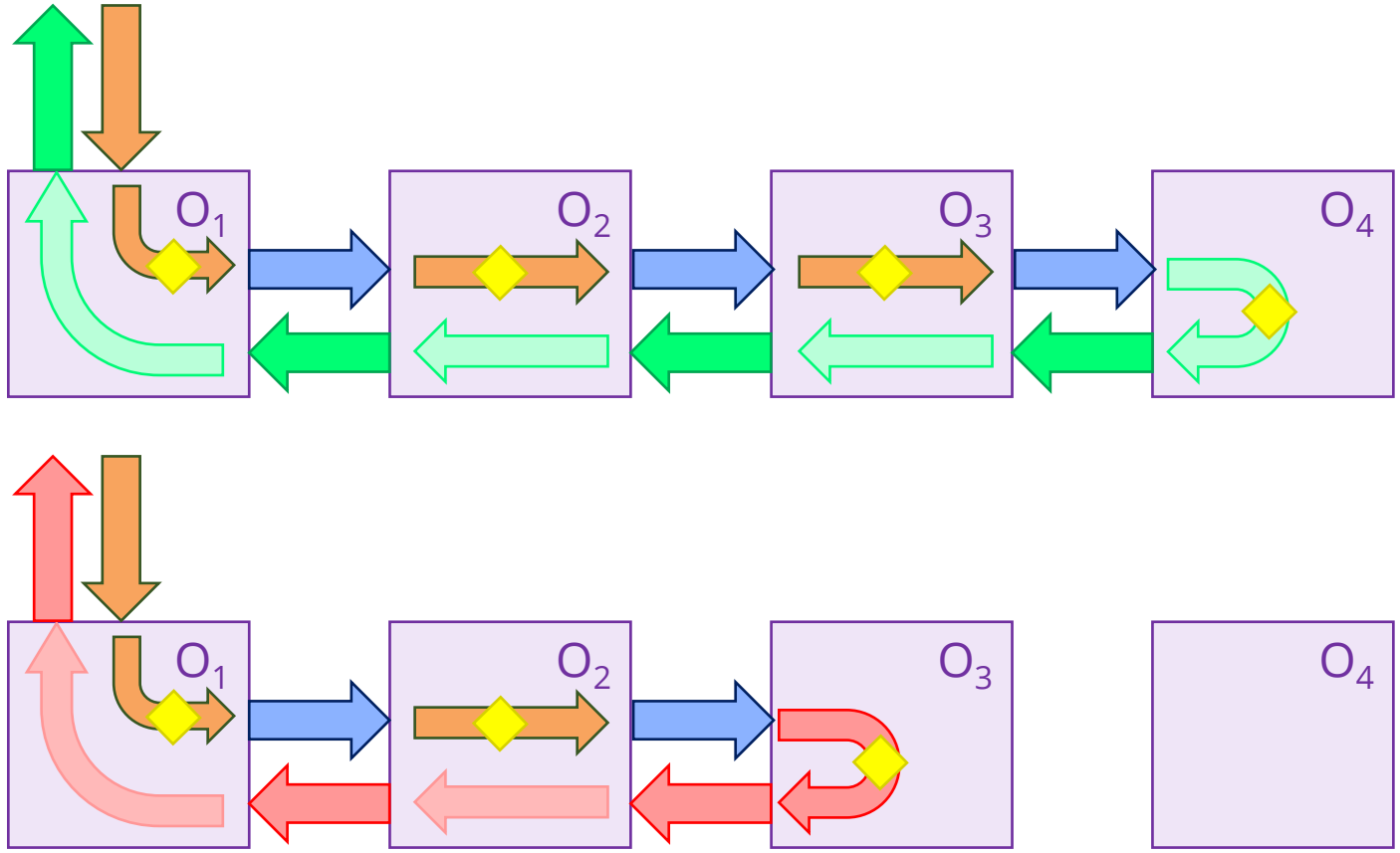
- Tömör
- Áttekinthető
- Célorientált, magas szintű
- Legyen ez maga a specifikáció
- A fordító minél több mindent ellenőrizzen
- Okos válasz
- Rendszerszintű diagnosztika - logging

Alapelv



- Vasúti objektumok
- Bejövő kérés - Request
- Feltétel ellenőrzés
- Kérés átadás
- Pozitív válasz
- Válasz átadás

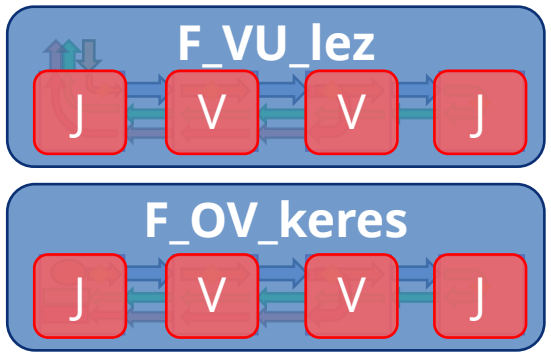
Alapelv



- Vasúti objektumok
- Bejövő kérés - Request
- Feltétel ellenőrzés
- Kérés átadás
- Negatív válasz
- Válasz átadás

Fő nyelvi elemek

Bontás



- **QUERY:**
- Funkciónkénti bontás üzenet-csoport névvel azonosítva

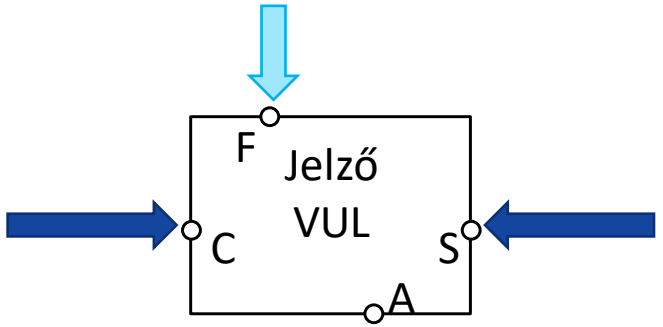
- **OBJECT:**
  A funkciókon belül objektumtípusonkénti bontás

- A specifikus alkalmazást (Állomást) majd külön leíróval határozza meg a ProRIS-CAD

- Ha objektum típusonként külön kódot generálunk, a fordító válogatja ki

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    ...
  EOBJECT Jelzo;
  OBJECT Valto;
    ...
  EOBJECT Valto;
EQUERY F_VU_lez;

QUERY F_OV_keres;
  OBJECT Jelzo;
    ...
  EOBJECT Jelzo;
  OBJECT Valto;
    ...
  EOBJECT Valto;
EQUERY F_OV_keres;
```

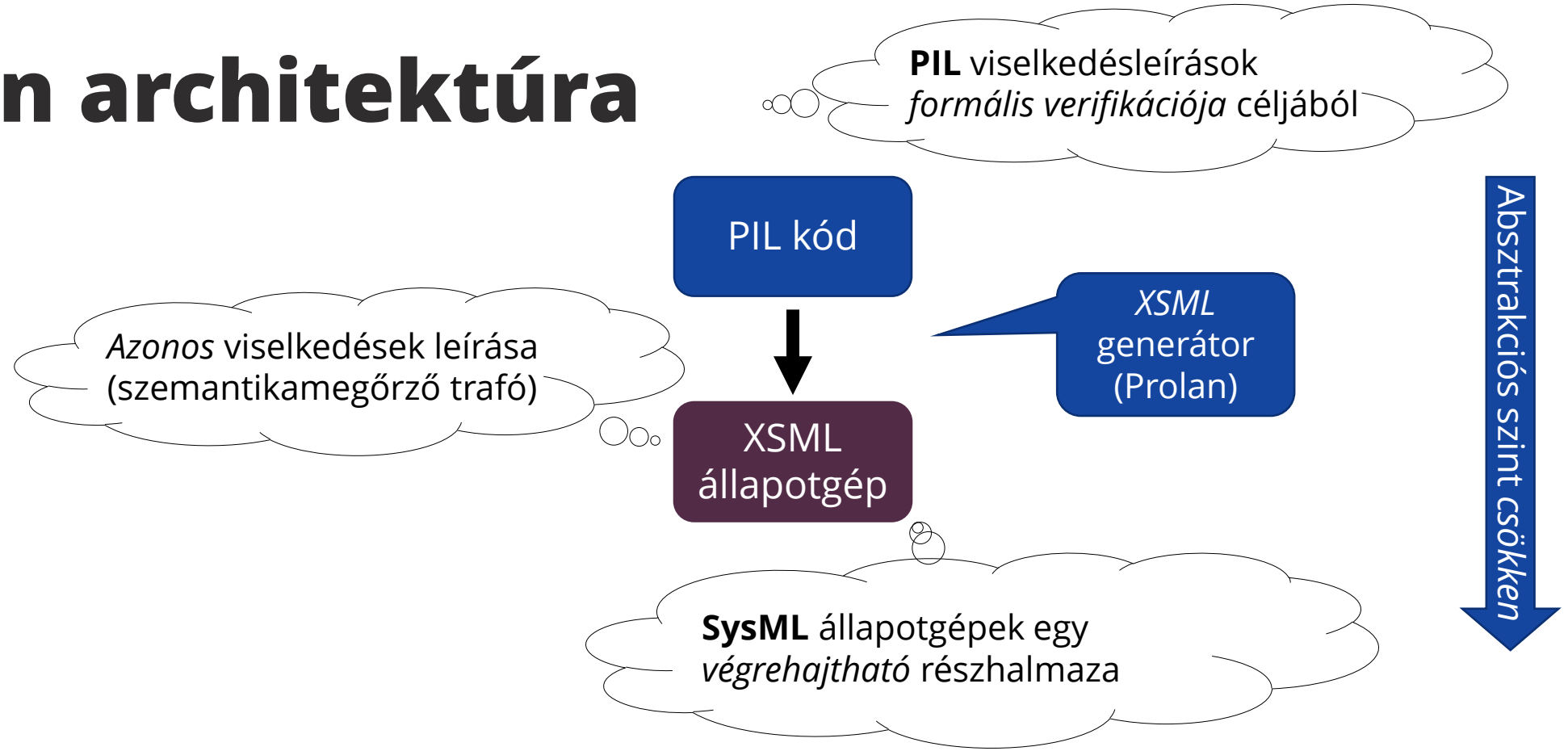
Input



- Az objektumon belül **INPUT**ok vannak. Akkor kerül a vezérlés az input sor alá, ha
  - az adott porton a Query-hez tartozó Kérés érkezik,
  - az adott porton egy megnevezett parancs érkezik – ez egy feltétel

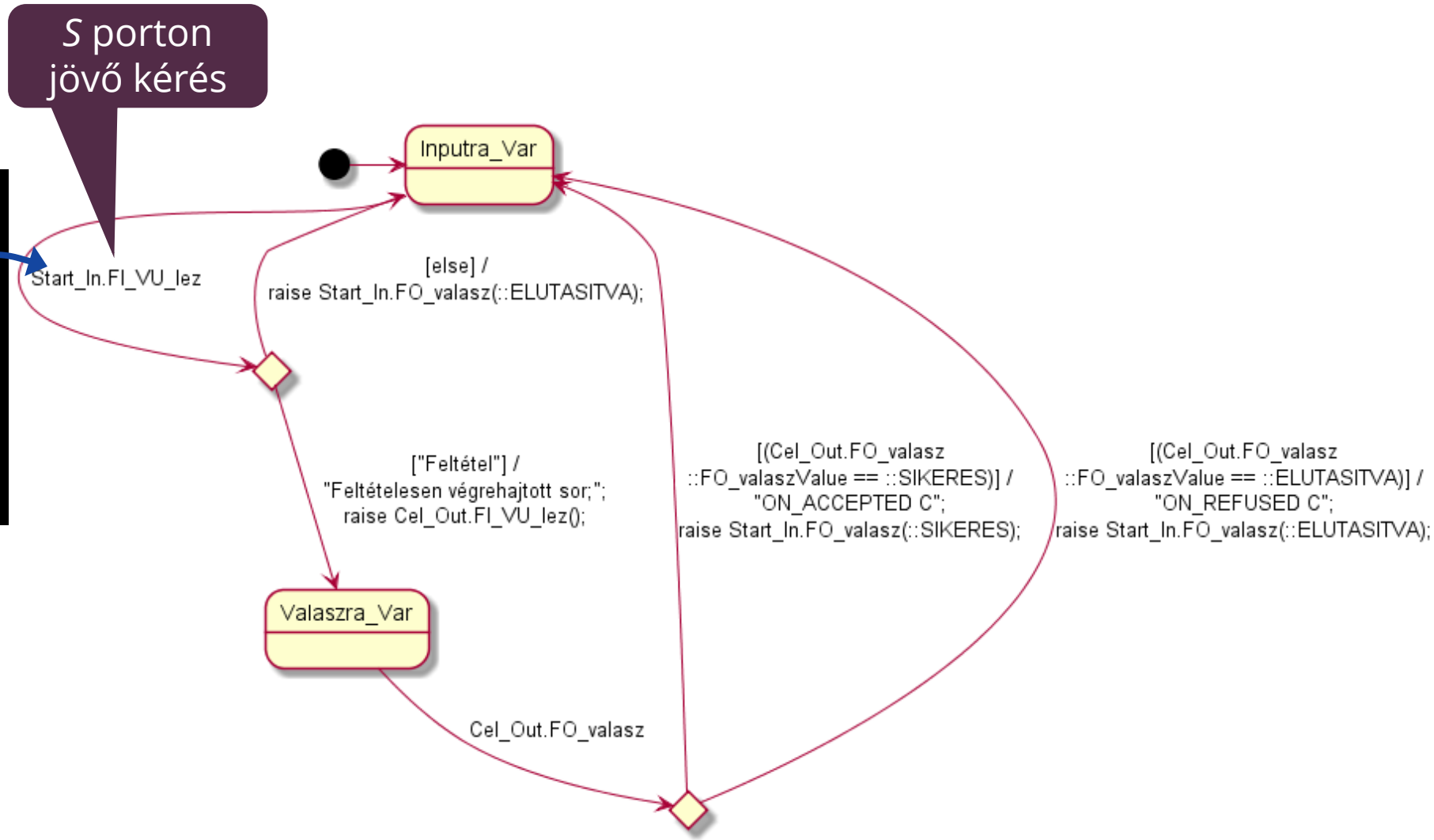
```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT C;
      ...

    INPUT S;
      ...

    INPUT F.VU_Lez;
      ...

  EOBJECT Jelzo;
  ...

EQUERY F_VU_lez;
```

Toolchain architektúra



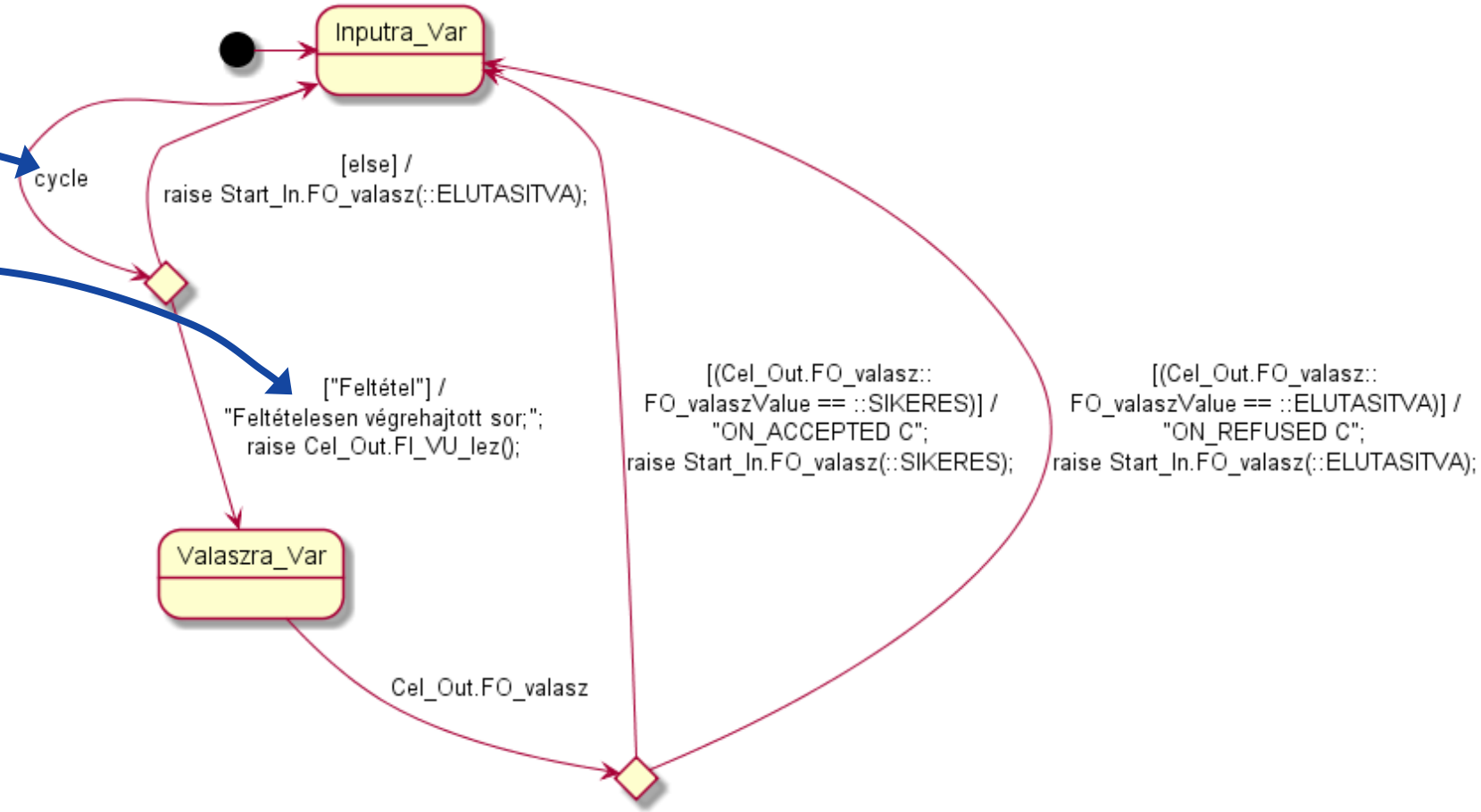
Input (Query – Pulse üzemmód)

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT S;
      …
  EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```



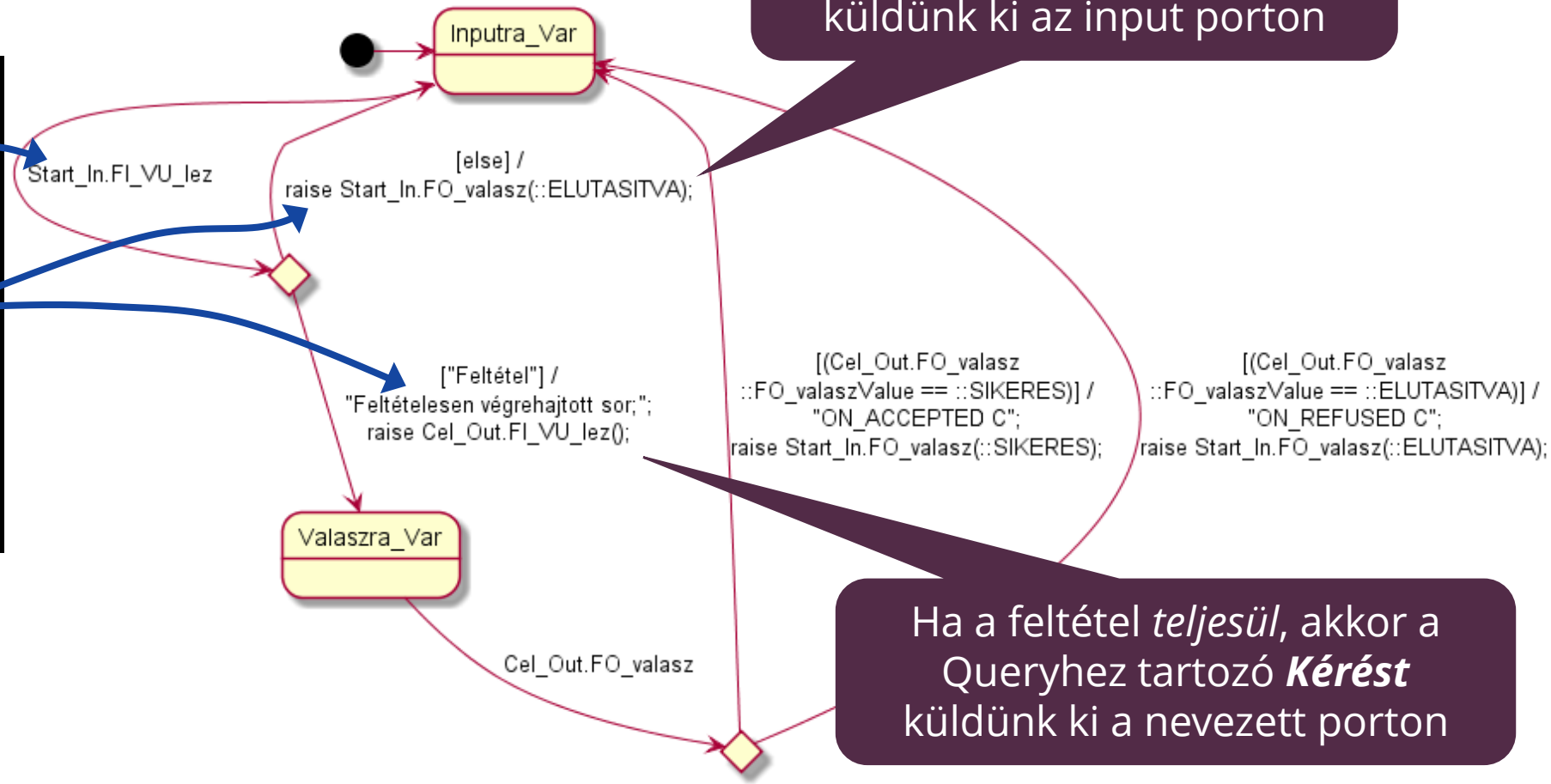
Trigger

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    TRIGGER
      feltétel;
      …
  EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```



Kérés továbbítás

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT S;
      REQ C
        [feltétel];
      …
  EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```

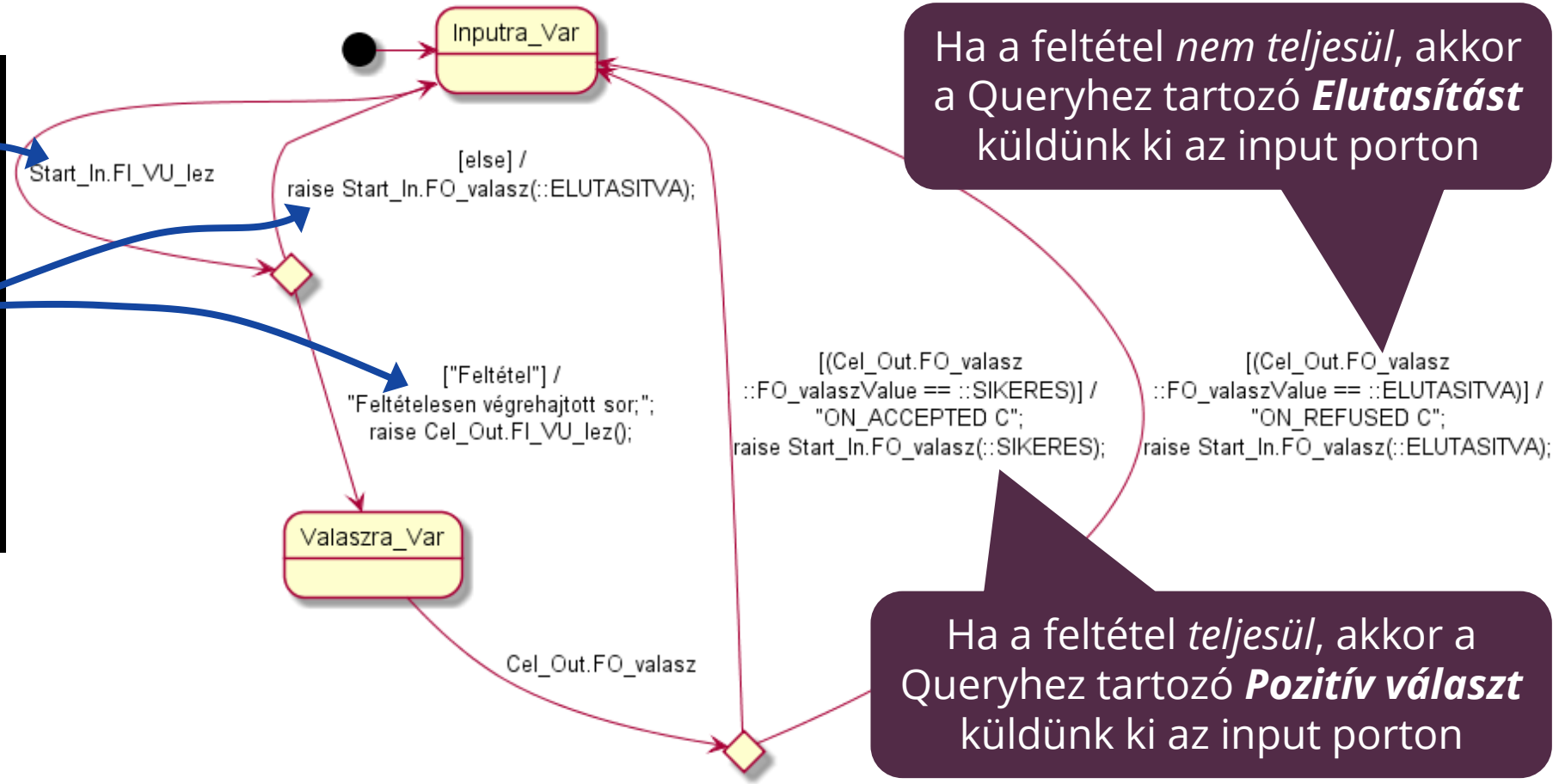


Ha a feltétel *nem teljesül*, akkor a Queryhez tartozó ***Elutasítást*** küldünk ki az input porton

Ha a feltétel *teljesül*, akkor a Queryhez tartozó ***Kérést*** küldünk ki a nevezett porton

Pozitív és negatív válasz

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT S;
      REQ C
        [feltétel];
      …
  EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```

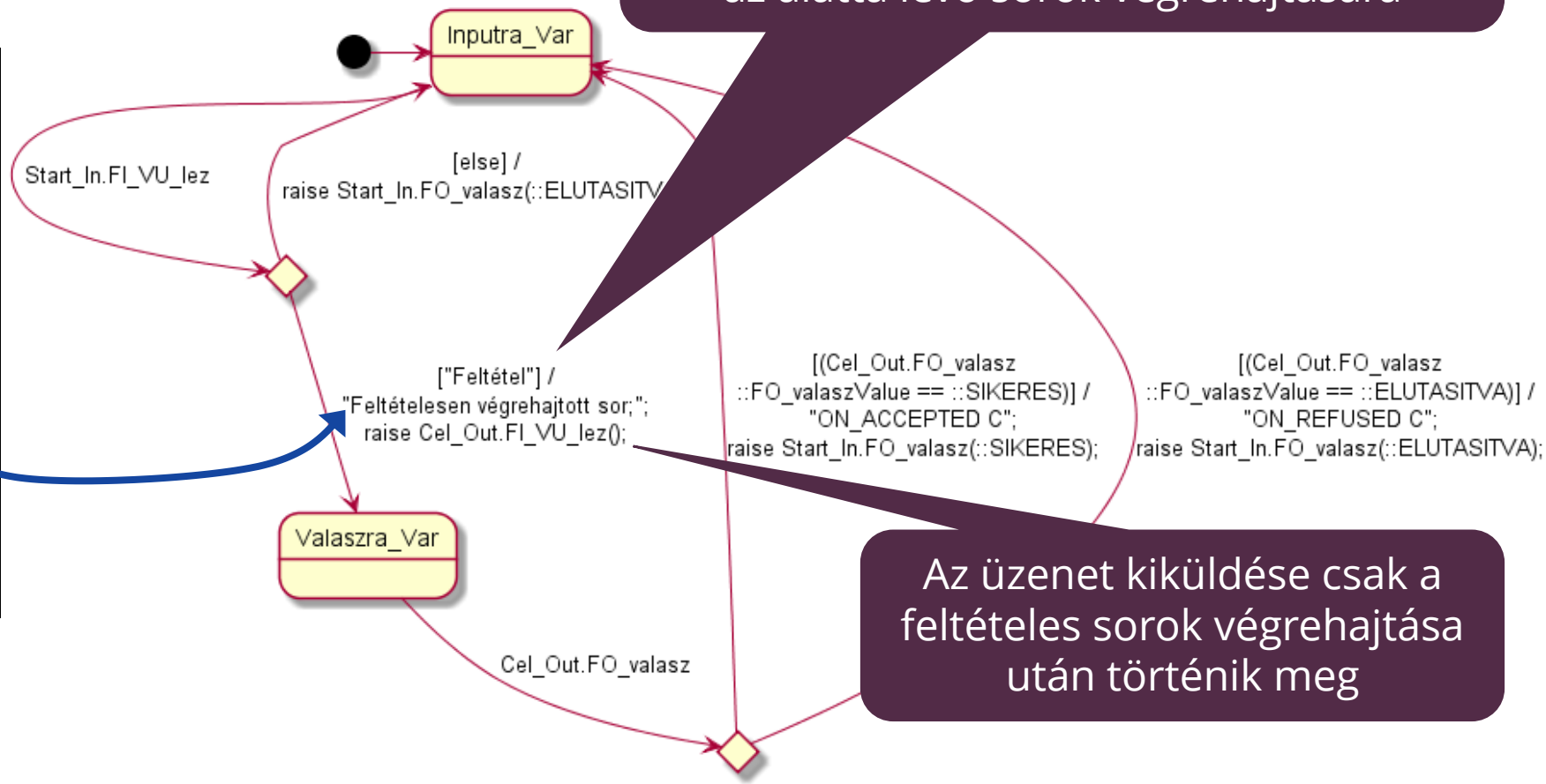


Ha a feltétel *nem teljesül*, akkor a Queryhez tartozó ***Elutasítást*** küldünk ki az input porton

Ha a feltétel *teljesül*, akkor a Queryhez tartozó ***Pozitív választ*** küldünk ki az input porton

Üzenetküldés feltételes hatása

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT S;
      REQ C
        [feltétel];
        Feltételesen
végrehajtott sor;
EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```

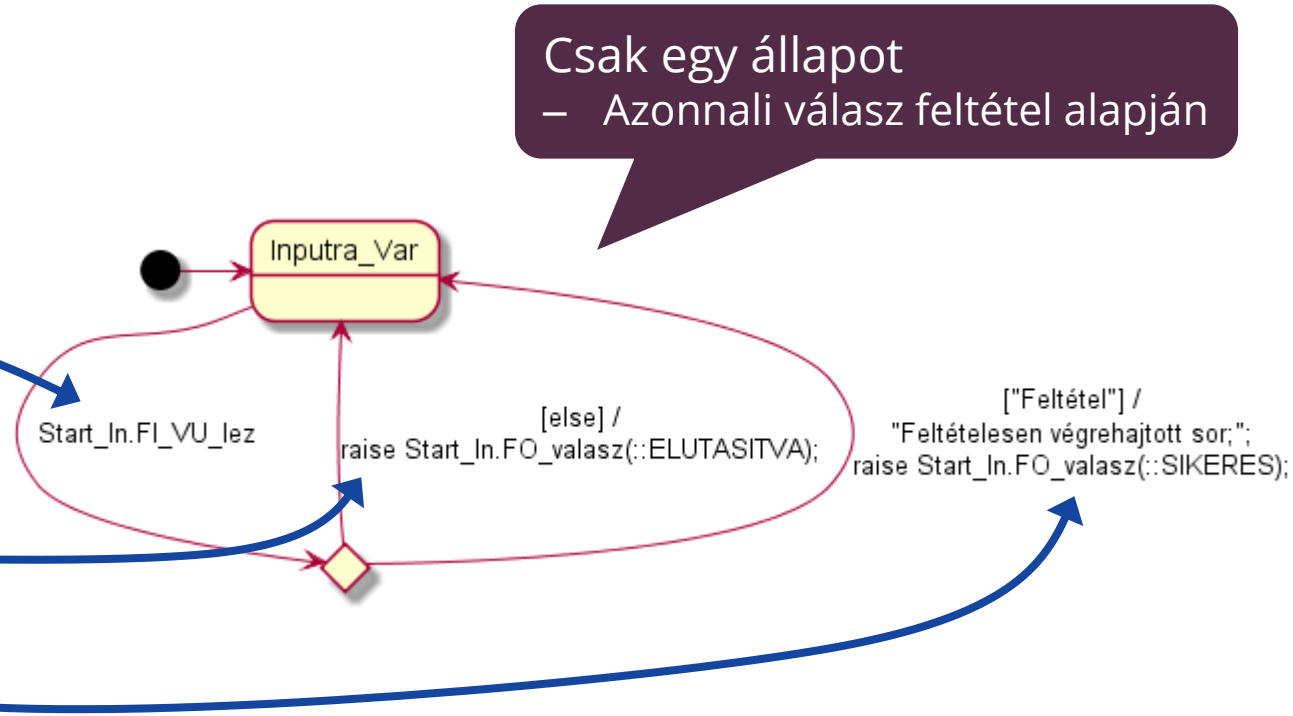


A REQ és ACCEPT utasítás feltételt formál az **utasítás blokkon belül** az alatta lévő sorok végrehajtására

Az üzenet kiküldése csak a feltételes sorok végrehajtása után történik meg

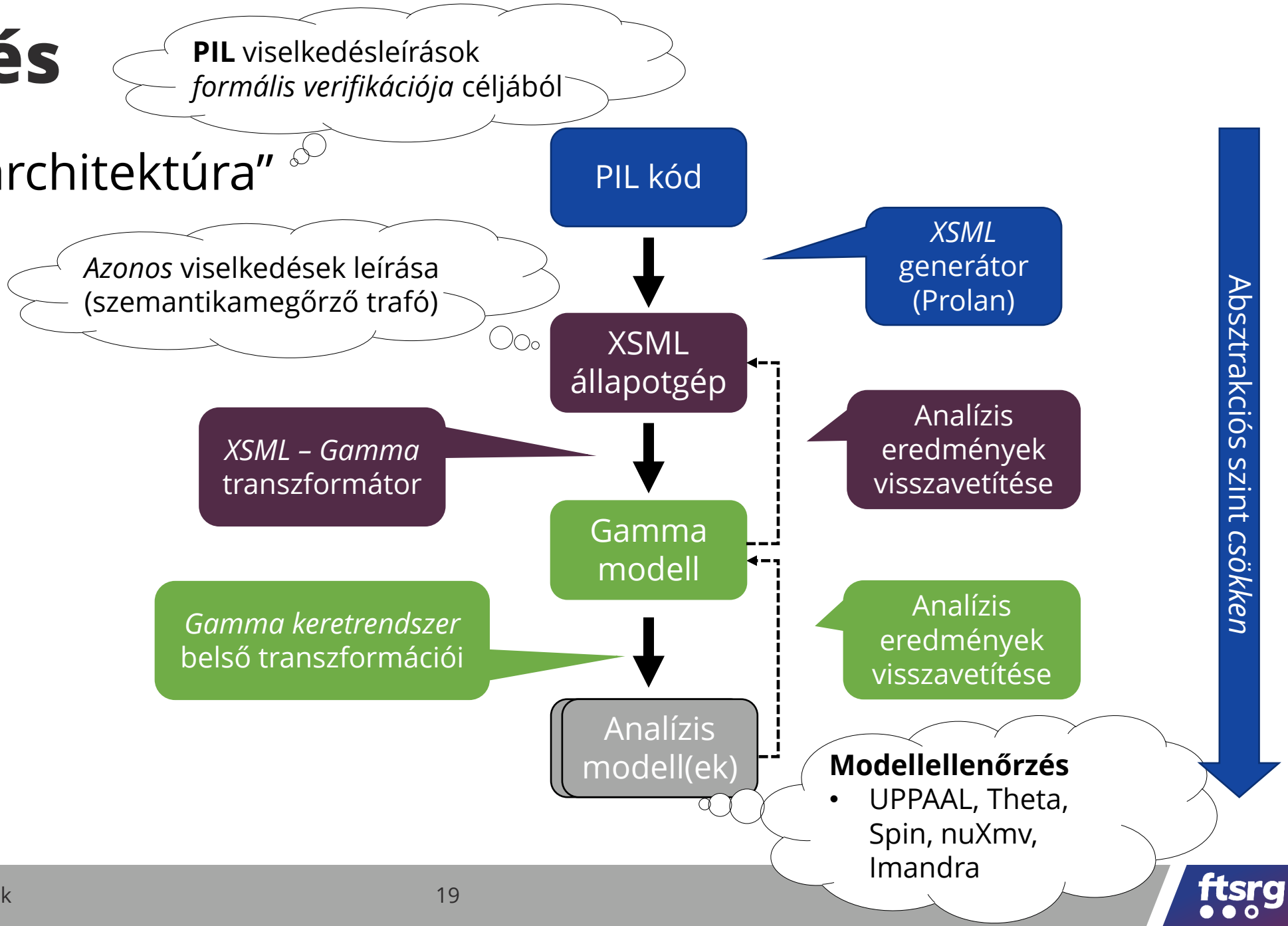
Accept

```
QUERY F_VU_lez;
  OBJECT Jelzo;
    INPUT S;
      ACCEPT
        [feltétel];
      …
  EOBJECT Jelzo;
  …
EQUERY F_VU_lez;
```



Bevezetés

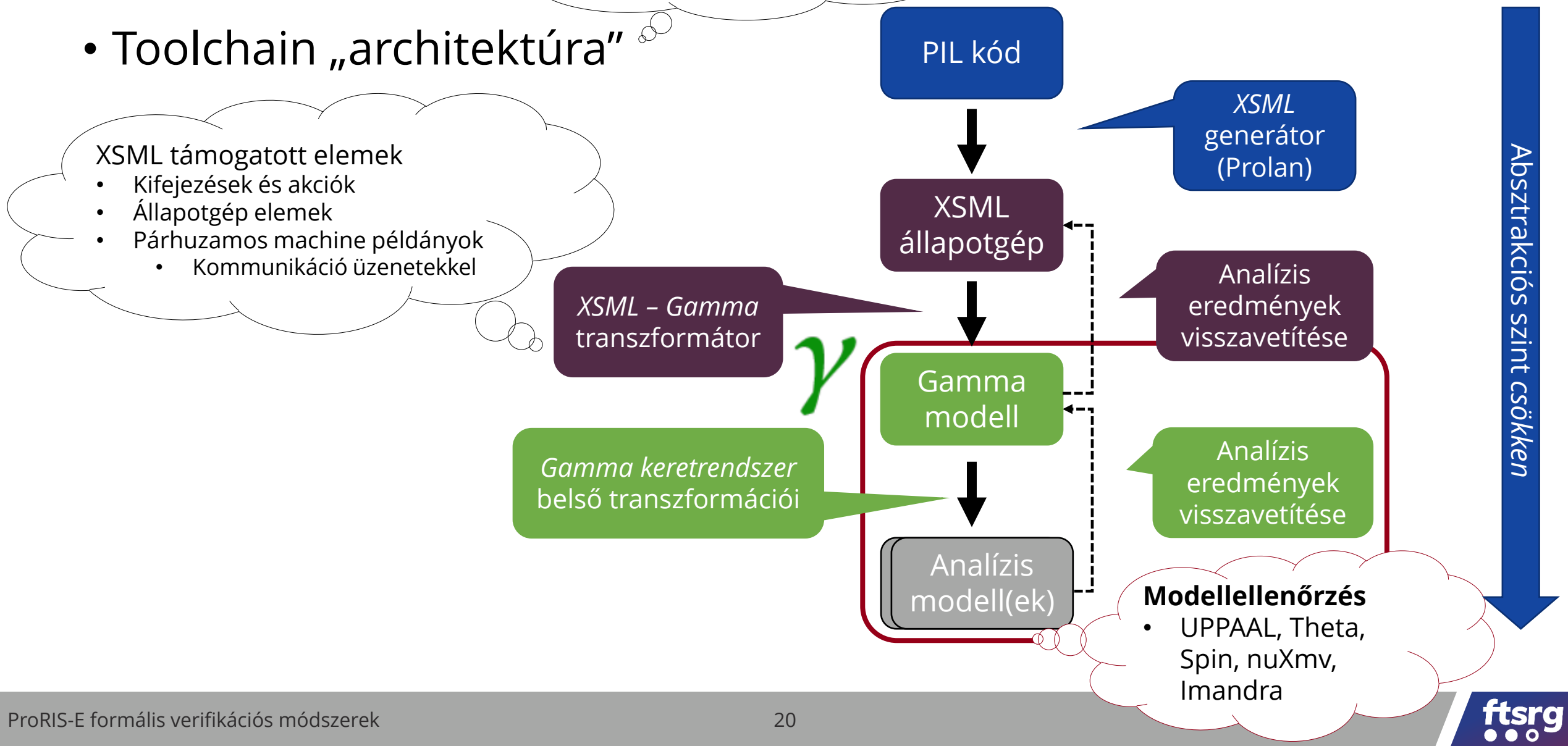
- Toolchain „architektúra”



Fókusz

PIL viselkedésleírások
formális verifikációja céljából

- Toolchain „architektúra”

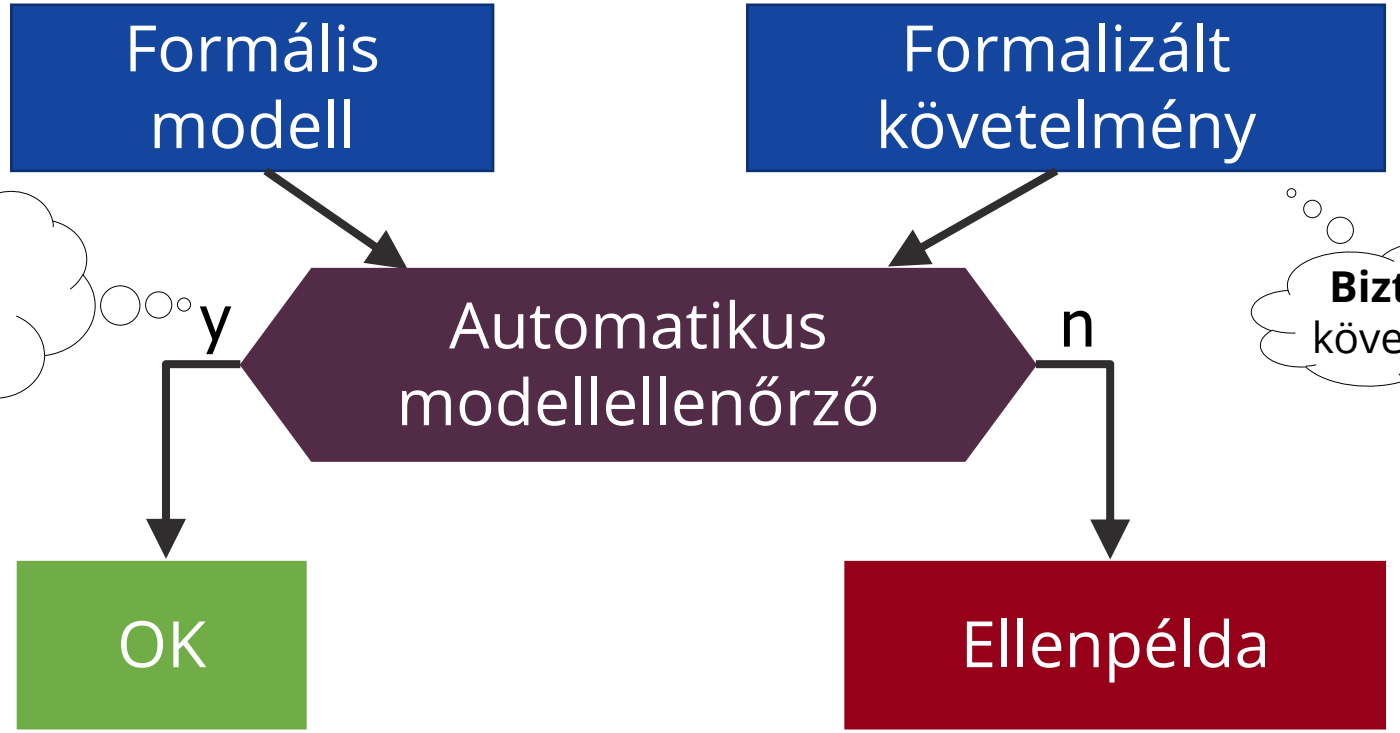


Modellellenőrzés áttekintés

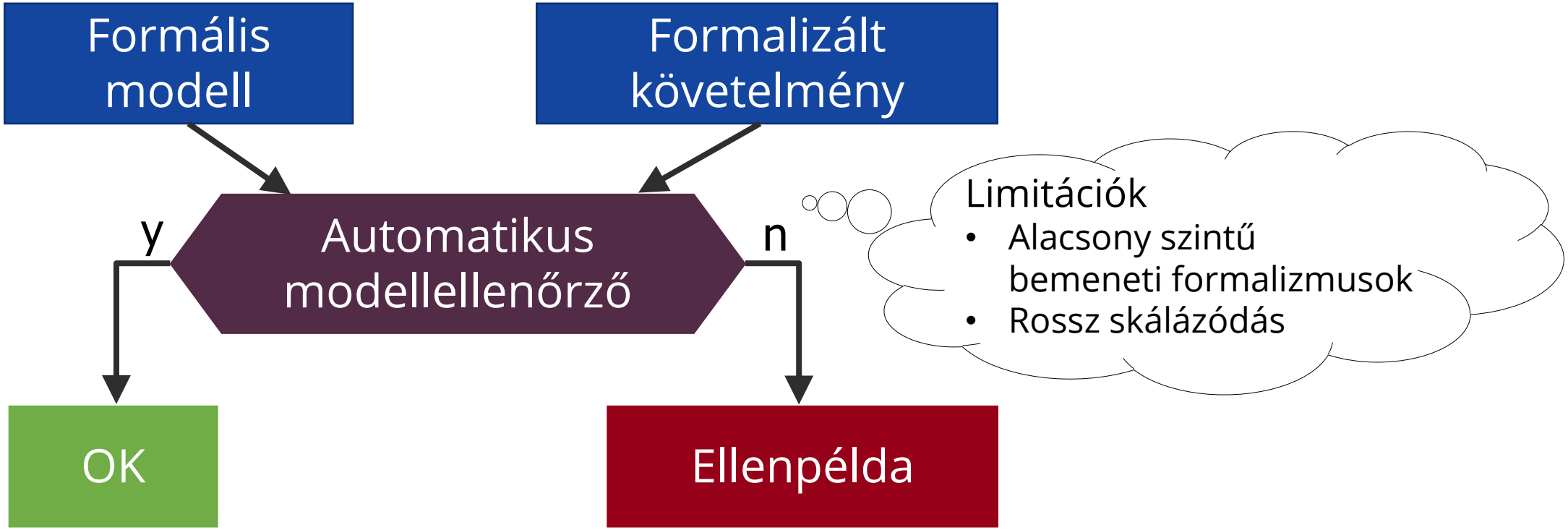
Mit várhatunk ettől a technikától?

Matematikailag precíz modell; leírja a rendszer viselkedését
- Időzített automata, tranzíciós rendszer, …

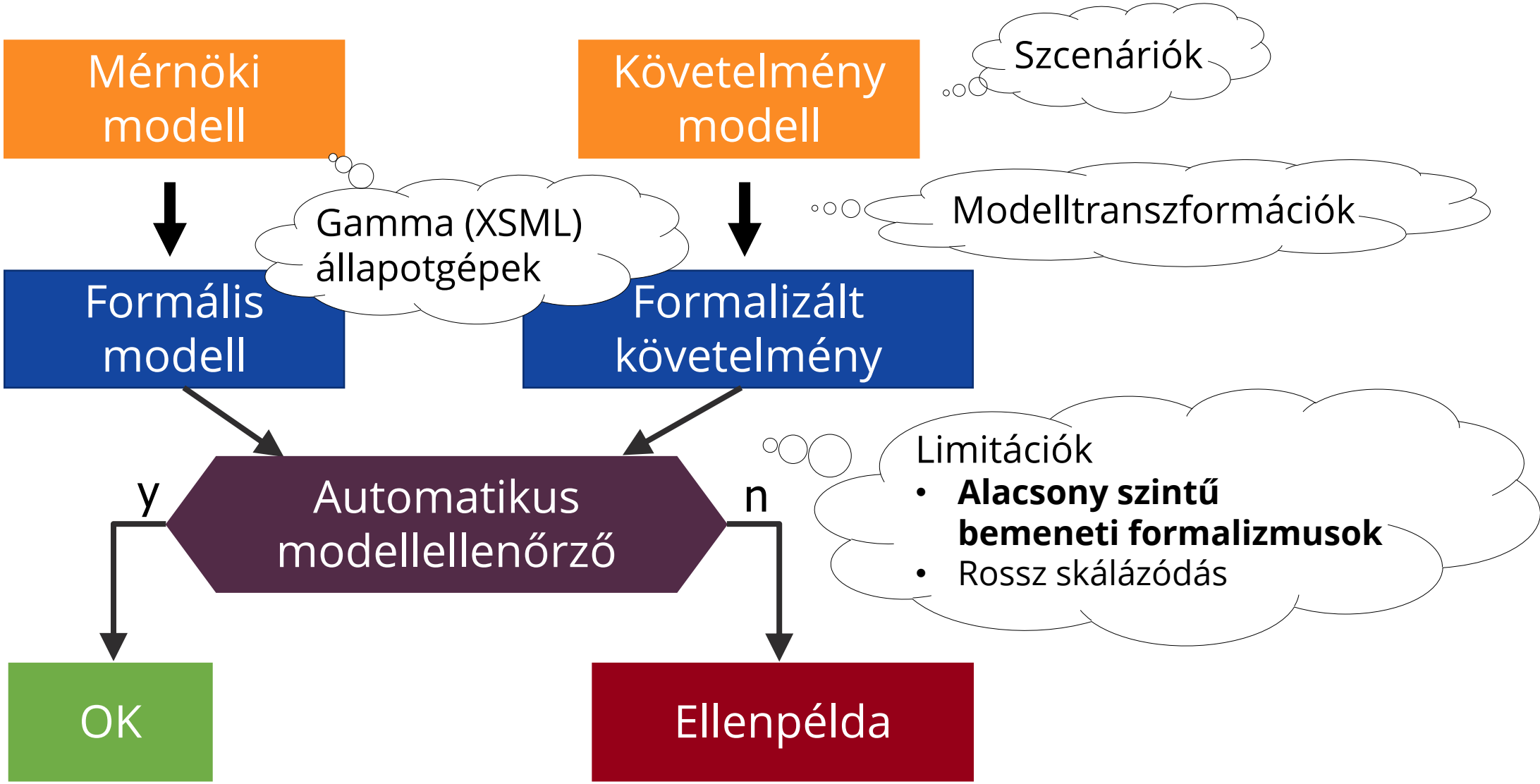
Precíz megfogalmazása a (funkcionális) tulajdonságnak
- Temporális logika, …



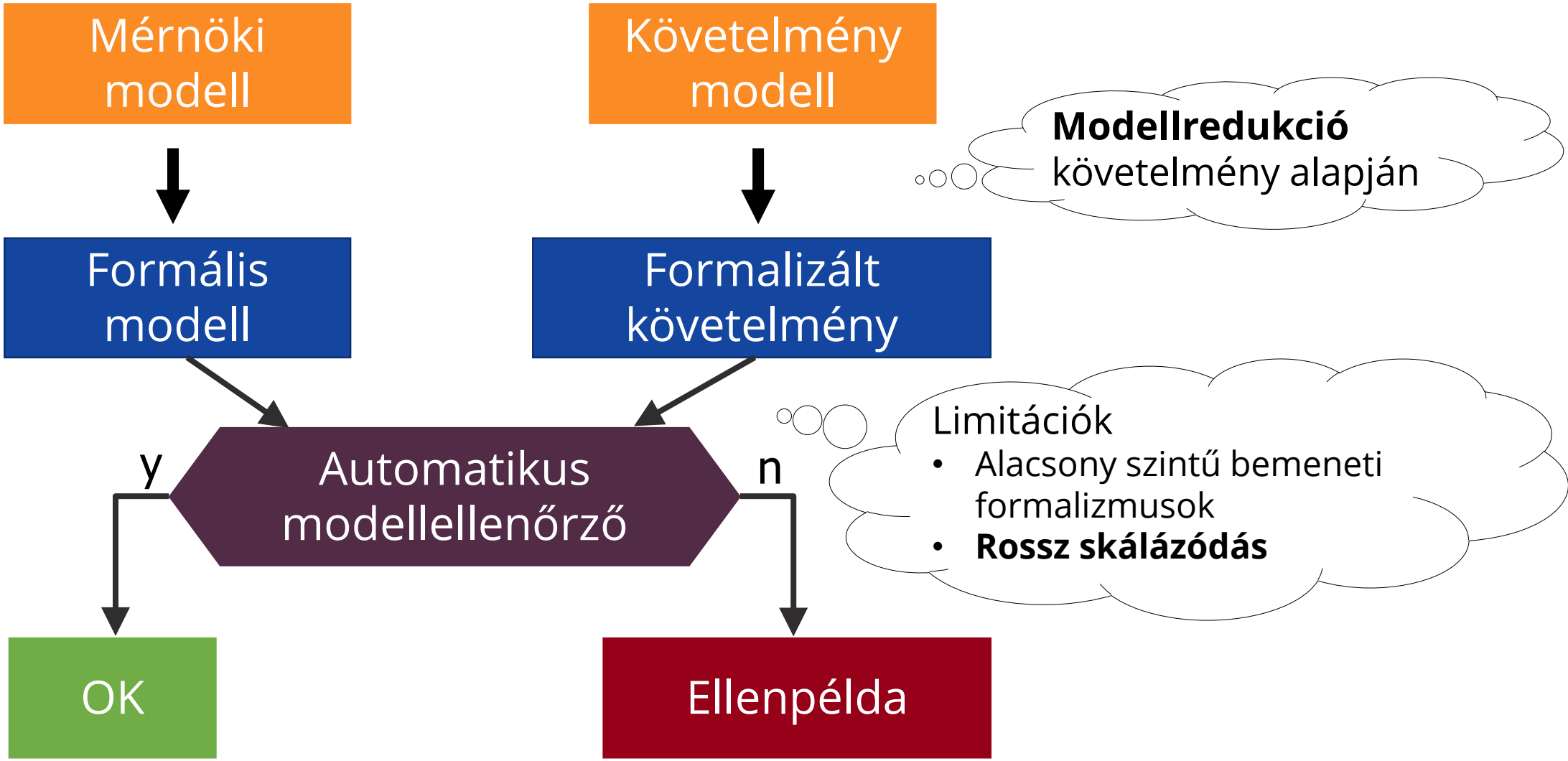
Modellellenőrzés limitációi



Modellellenőrzés limitációinak kezelése



Modellellenőrzés limitációinak kezelése



Viselkedés helyességének ellenőrzése

- *Funkcionális* viselkedés **kimerítő** elemzése
- Szükséges input a **helyességi kritériumok** köre
  - Állapot elérhetőségi tulajdonságok
    - Pl. **hibás** (veszélyes) állapot nem elérhető, **kívánt** (helyes) állapot elérhető
    - További *összetett* tulajdonságok
  - Kontraktusoknak való megfelelés
    - Kontraktusok **szcenáriók** formájában történő specifikációja (követelmény szcenáriók)
    - Pl. adott **kérést engedélyezzük** vagy **elutasítjuk**

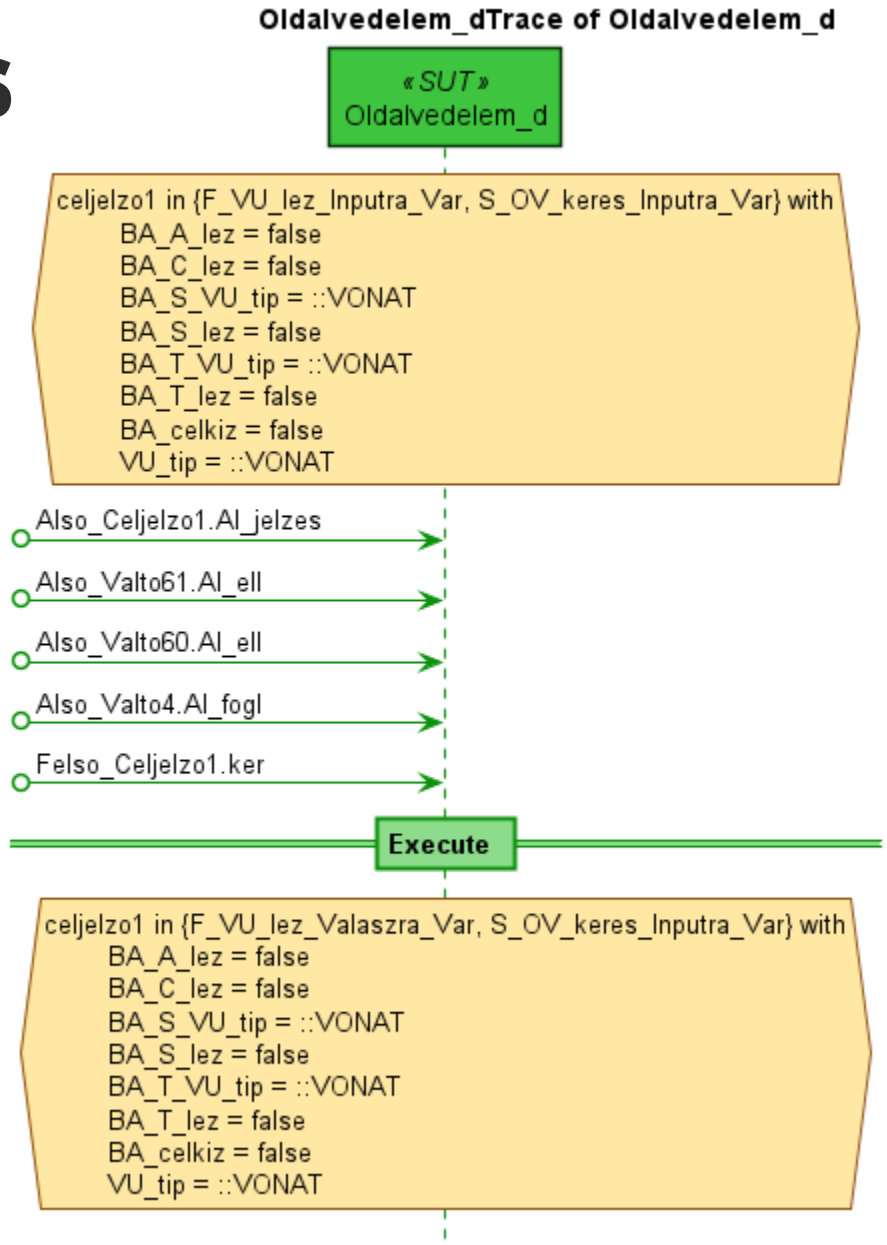
*PIL-XSML-Gamma-** lánc

Must always
Must eventually
Might always
Might eventually
„Leads to”

```
scenario RequestHandling {
  // Ha fogadunk egy kérést
  cold receives request
  // Akkor vagy…
  alternative {
    // … engedélyezzük
    hot sends grant
  } or {
    // … vagy elutasítjuk
    hot sends refuse
  }
  // Más nem elfogadható
}
```

Modellalapú tesztgenerálás

- **Tesztgenerálás** implementációhoz
  - Modellbeli **fedettségi kritériumok** alapján
    - Állapot, tranzíció, tranzíció-pár
    - Komponensek közötti interakciók
    - Változók írása és olvasása (def-use)
  - Futó **implementáció** a **modell** által leírt **viselkedést** valósítja meg?
- Alapötlet
  - *Vezéreljük* úgy a modellellenőrzőt, hogy **generáljon végrehajtási útvonalakat**
    - Csapda tulajdonság (*trap property*)
  - Ezek tekinthetők **absztrakt teszteseteknek**
    - *Konkretizálhatók* különböző környezetekhez (C, Java, …)



A megközelítés „lelke”

- Modelltranszformációk helyessége
  - „*Szemantikamegőrző*” tulajdonság
  - Forrás- és célmodell **ugyanazt** a viselkedést írja le
- **XSML-Gamma transzformáció** esetén két „szint”
  - „Atomi” állapotgépek
  - Kompozíció (integráció)
    - Végrehajtás
      - Pl. szekvenciális, konkurens, párhuzamos
    - Kommunikáció
      - Pl. *jelekkel* vagy üzenetsorokban tárolt *üzenetekkel*

PIL – XSML
XSML – Gamma
Gamma – UPPAAL/Theta/Spin

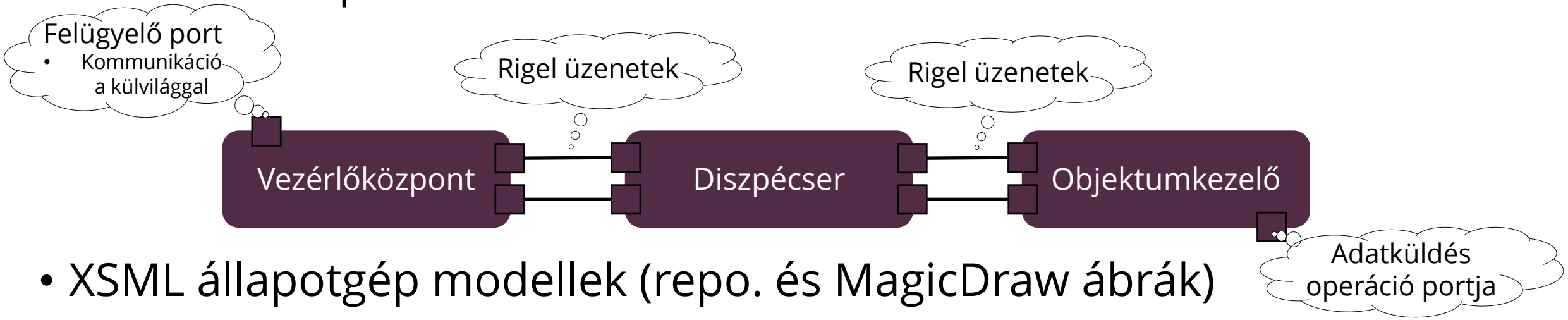
Kompozíció egyelőre **manuálisan** Gamma *kompozíciós módjait* felhasználva

gépek esetén
nogatott
ódik még
Union típus
Update üzenet

Lokális üzenetsorok **megtelése** és üzenetek **eldobása** esetén *inkonzisztens* viselkedés

Demo – PRORIS-H RIGEL protokoll spec.

- ProRIS-H „EMU2 – PS-B alrendszerek közötti alkalmazás szintű kommunikációs (RIGEL) protokoll”
- Három szereplő

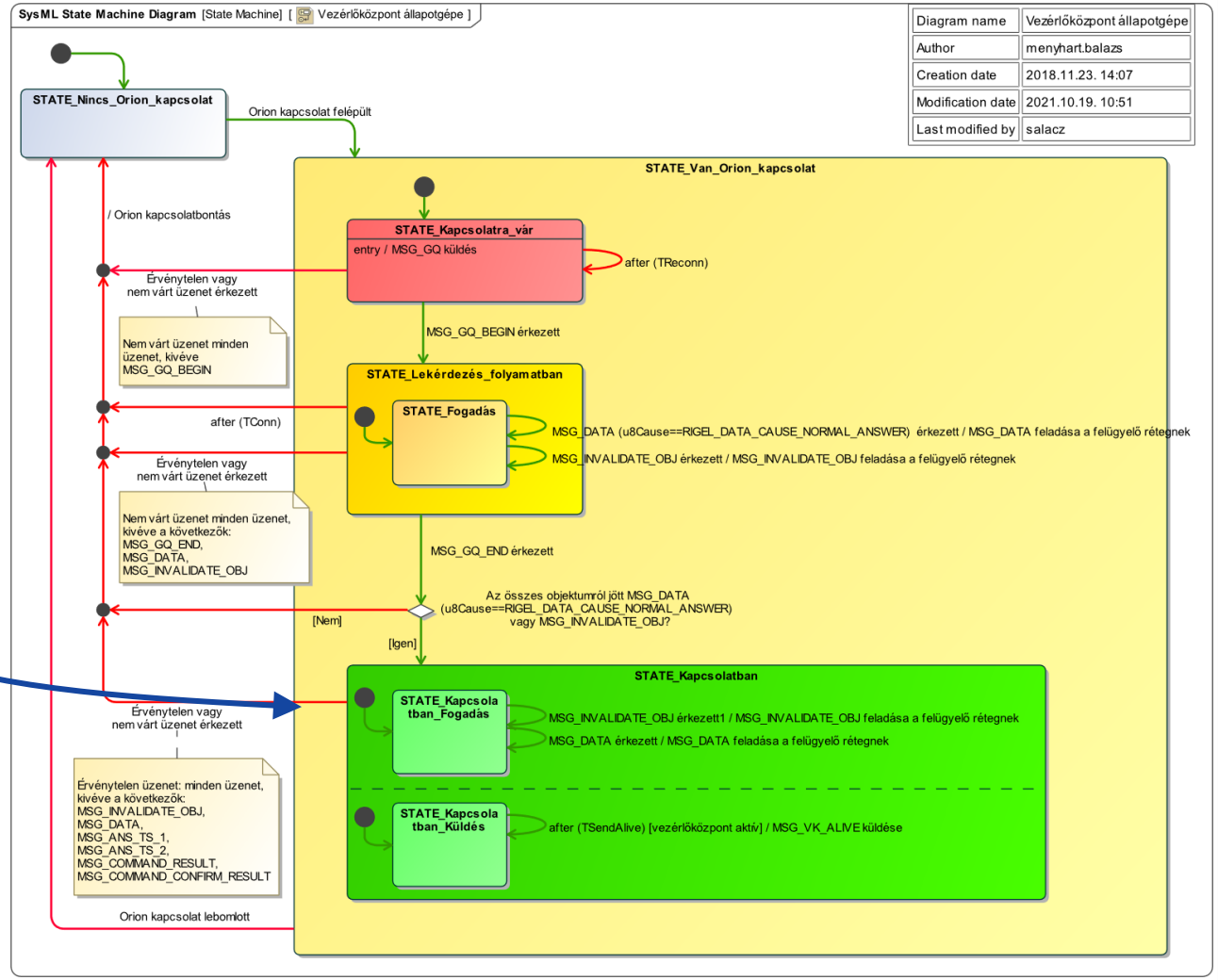


- XSML állapotgép modellek (repo. és MagicDraw ábrák)
- Transzformáció Gammára automatizáltan
- Topológia definiálása manuálisan

Demo – PRORIS-H RIGEL protokoll spec.

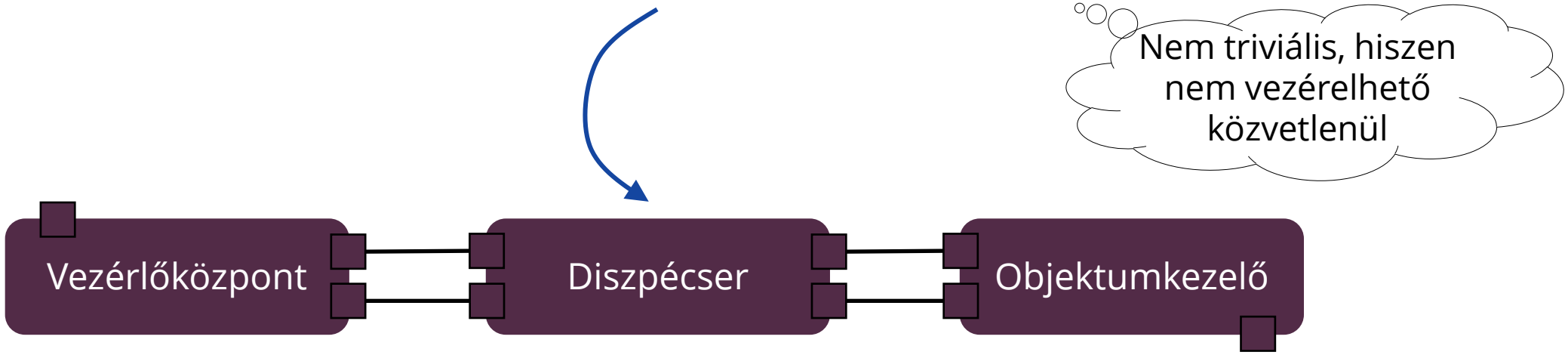
- Formális verifikáció
  - Elérhető-e a **vezérlőközpont** állapotgépben a **Kapcsolatban** állapot?

Lehetséges **modellredukció** a tulajdonság alapján



Demo – PRORIS-H RIGEL protokoll spec.

- Tesztgenerálás
  - Minden **állapotot** fedjünk le a **diszpécser** állapotgépben!



Összefoglalás

- Toolchain XSML (PIL) formális verifikációhoz
  - Modellellenőrzés
  - Tesztgenerálás
- Támogatott elemek, javaslatok, hiányosságok
  - XSML állapotgépek teljeskörűen támogatottak
- Determinisztikus viselkedés nagyban segíti a skálázhatóságot