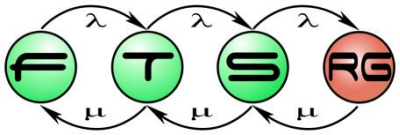
Modellellenőrzés alkalmazása egy biztonságkritikus rendszer védelmi logikájának verifikációjára

Vörös András



Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Motiváció

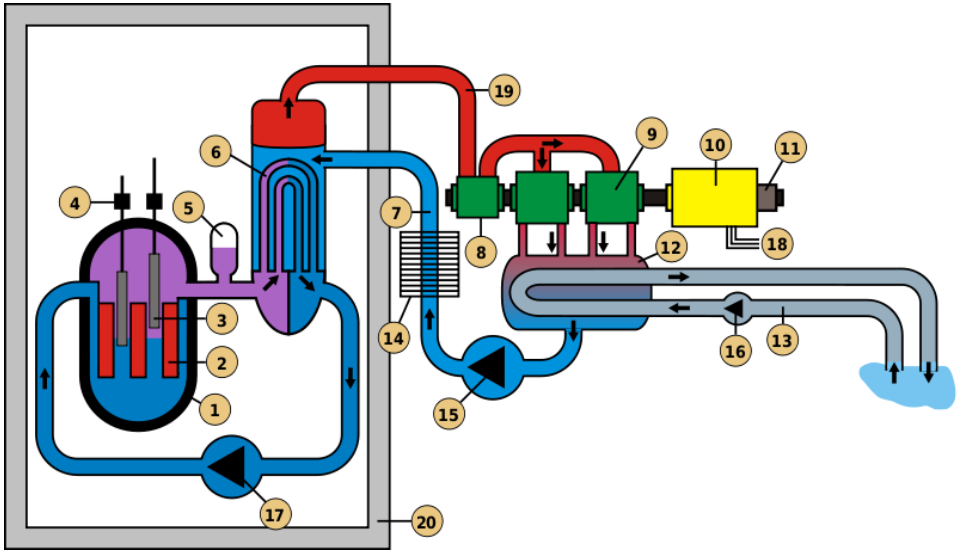
- Biztonságkritikus rendszerek
  - Fontos a helyes működés
- Formális verifikáció alkalmazása
  - Fejlesztés korai fázisában kiszűrhetőek a hibák
  - Tervek, modellek vizsgálatával
- Modellellenőrzés
  - Automatikus (formális) verifikációs technika
  - Rendszer modelljét vizsgálja
    - Diszkrét, véges állapotterű
  - Specifikációs követelmények teljesülését ellenőrzi

Előadás

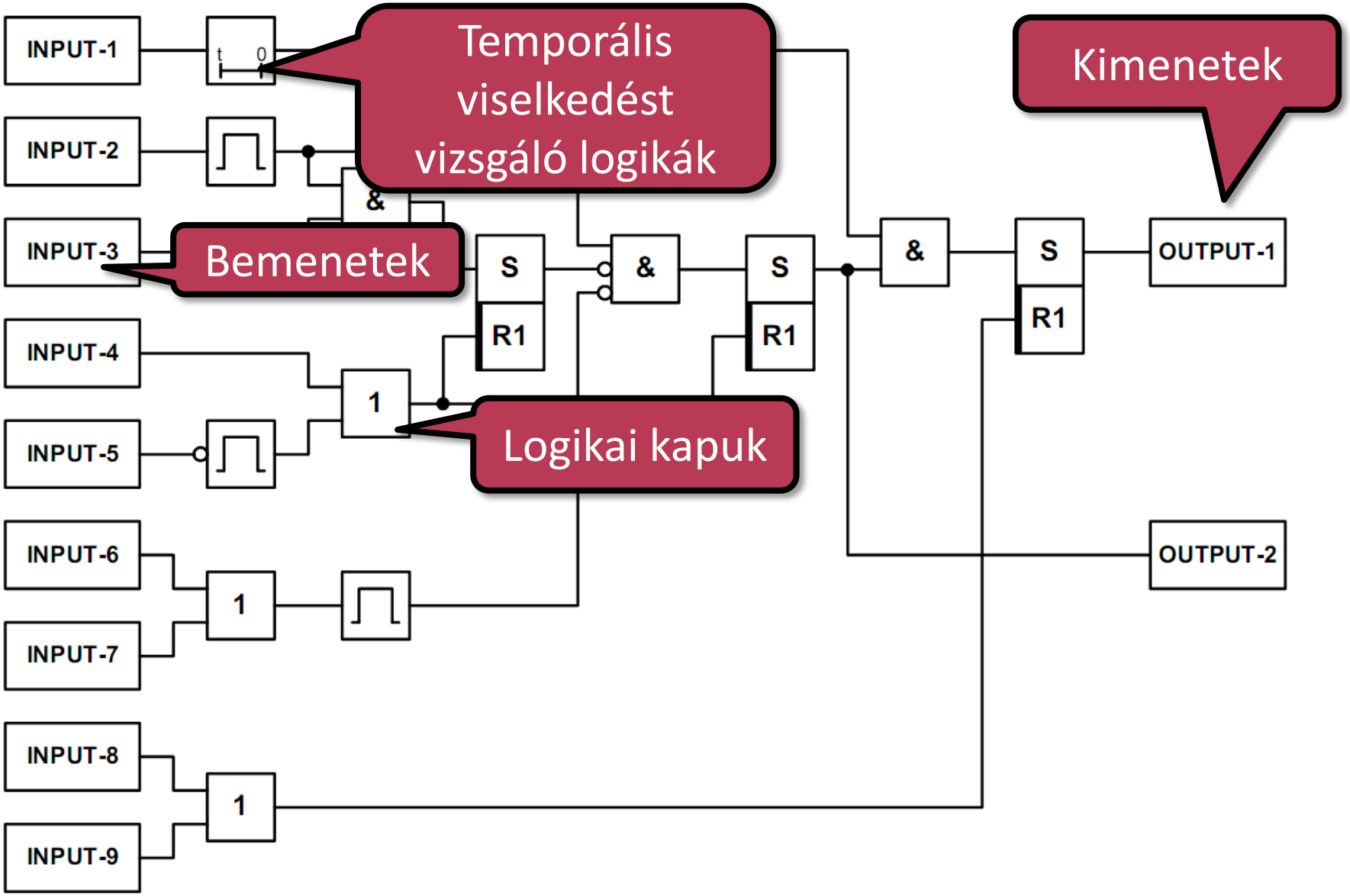
- Egy biztonságkritikus rendszer vizsgálata
  - Modellezés
  - Specifikáció formalizálása
    - Elágazó idejű temporális logikák segítségével
  - Ellenőrzés

Biztonságkritikus rendszer

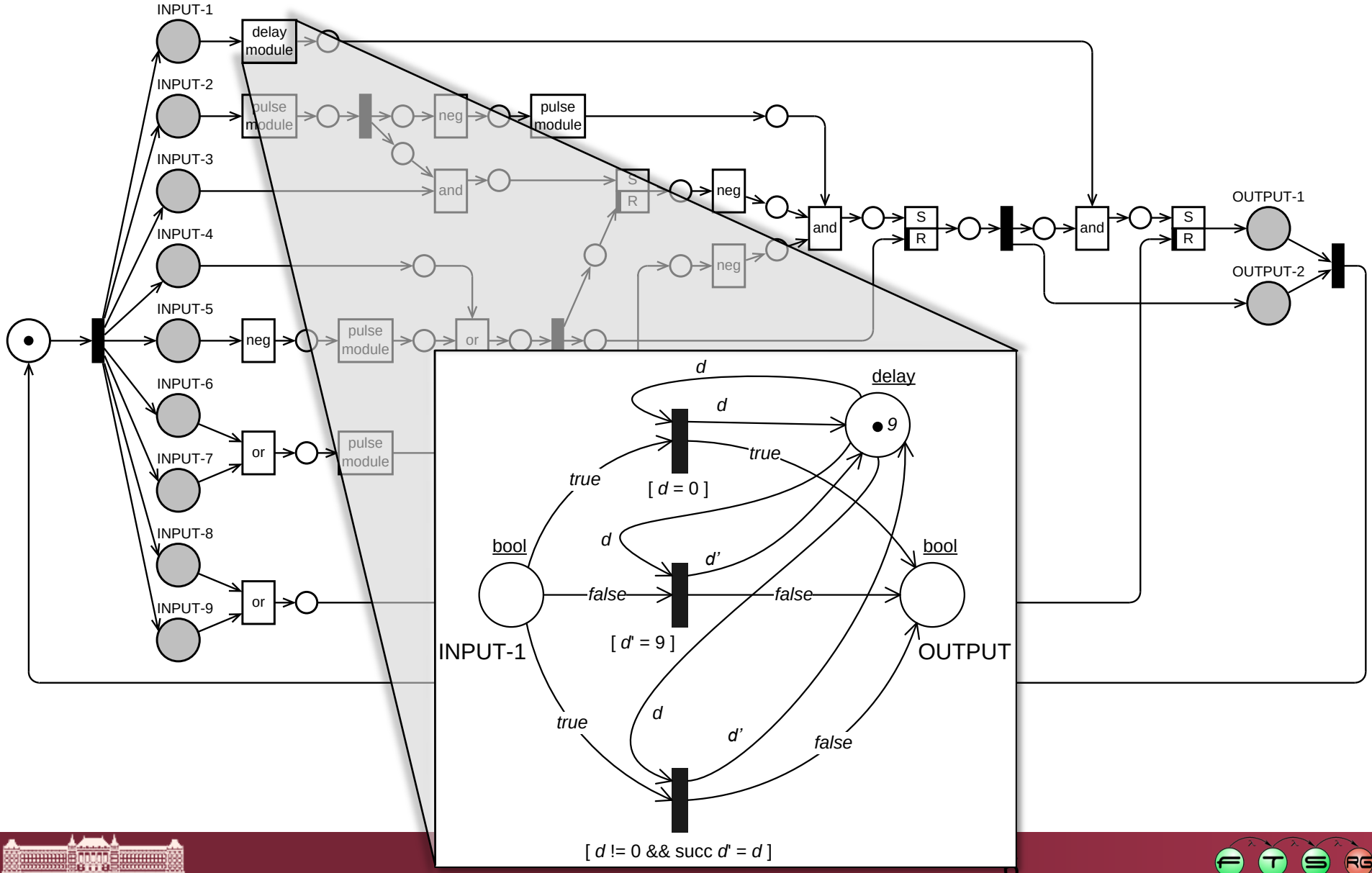
- Paksi Atomerőmű egyik védelmi funkciójának indító logikája
  - Valós ipari rendszer
- Célja detektálni a radioaktív hűtővíz szivárgását a primer körből a szekunder körbe



Indító logika blokkdiagramja

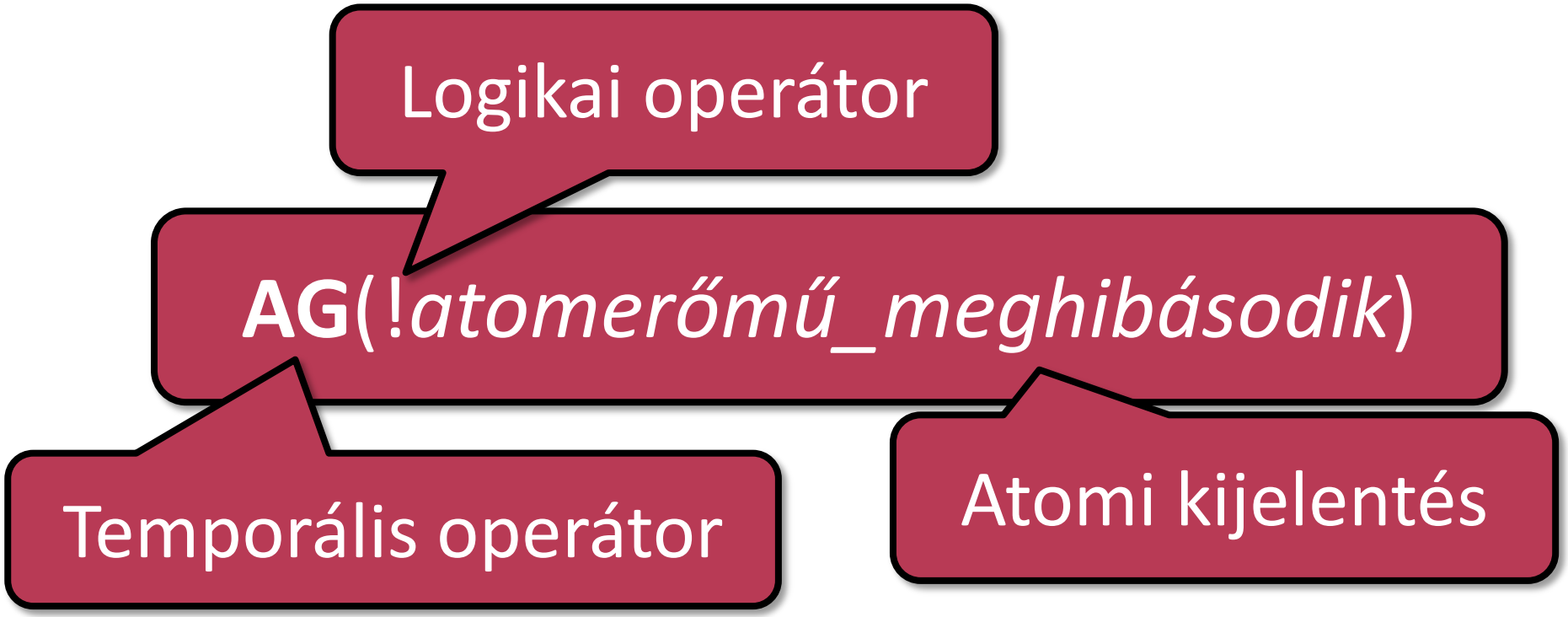


Magas szintű CPN modell - PRISE



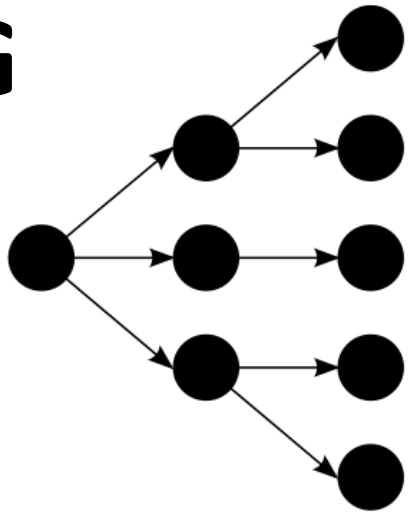
Specifikáció

- Elágazó idejű temporális logika segítségével formalizáltuk (CTL – Computational Tree Logic)

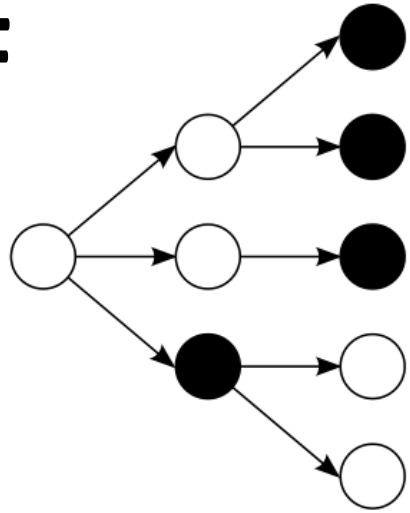


CTL operátorok

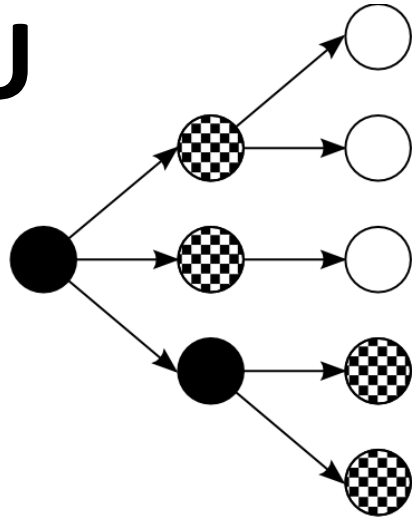
AG



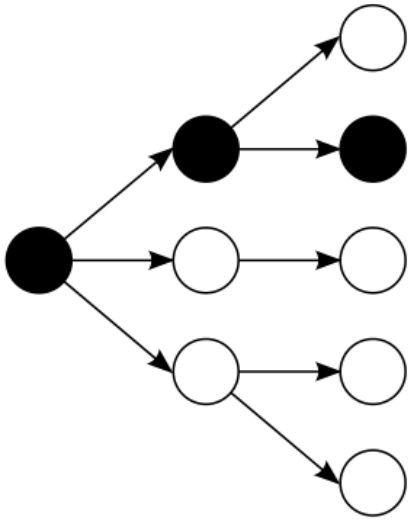
AF



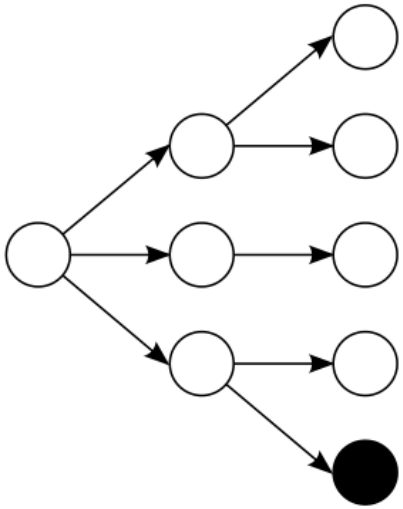
AU



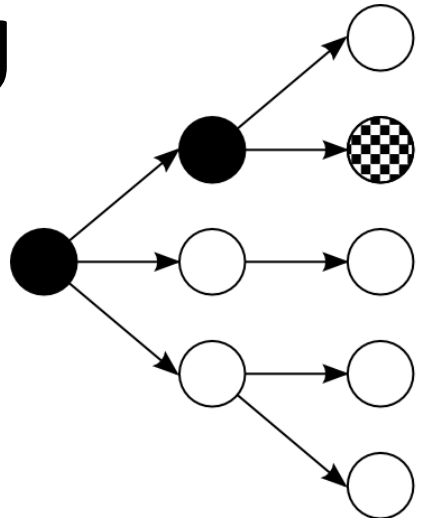
EG



EF



EU



Követelmények

- Általános követelmény
  - Nem következik be holtpont
- Biztonsági követelmény
  - Nem mulasztunk el egy biztonsági eseményt
- Helyességi követelmény
  - Nem történik téves riasztás

- Követelményeket formalizáltuk CTL segítségével

Verifikáció

- Korábbi verifikációs kísérletek sikertelenek voltak
  - verifikáció csak redukált modellre
  - explicit technikákkal (DesignCPN, UPPAAL)
  - szimbolikus technikákkal (SAL, korábbi szaturációs algoritmusok)

- Vizsgálatok
  - Formális modell megalkotása
    - Petri-hálók segítségével
  - Tanszéken fejlesztett eszköz segítségével
    - teljes állapottér-felderítés + kritérium-ellenőrzés

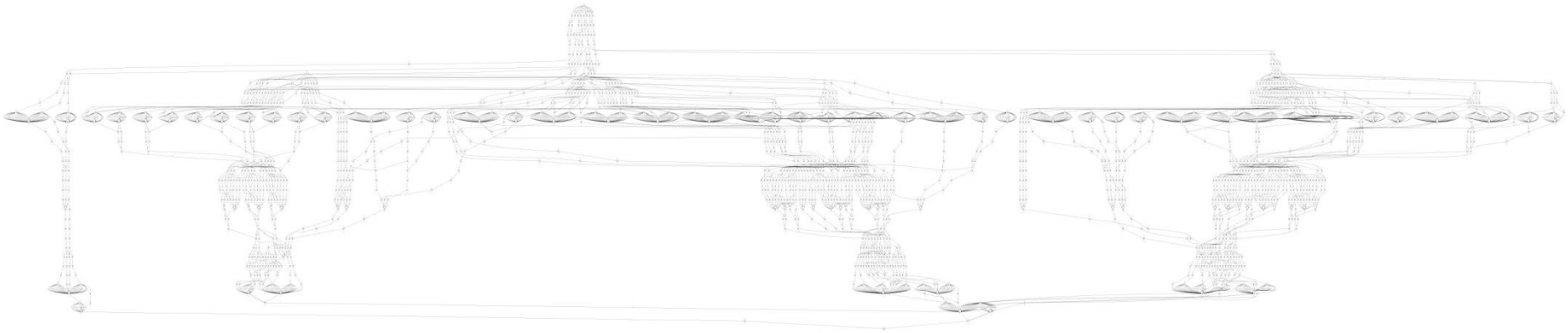
Állapotfelderítési jellemzői

- Futási idő: 950 s
- Memóriafoglalás: 2,53 GB
- Globális állapotok száma: $4{,}8 \cdot 10^{12}$

Szimbolikus kódolás hatékonysága:

- Állapottér MDD csomópontszáma: kb. 1500
- Lokális állapotátmenetek száma: 10.082.881

Állapottér reprezentáció



Összefoglalás

- Elkészült a biztonsági logika működésének modellje
  - Félformális modellek alapján
- Elkészültek a formalizált specifikációs követelmények
- Ellenőriztük a biztonsági logika helyes működését
  - Korábbi megközelítések nem jártak sikerrel