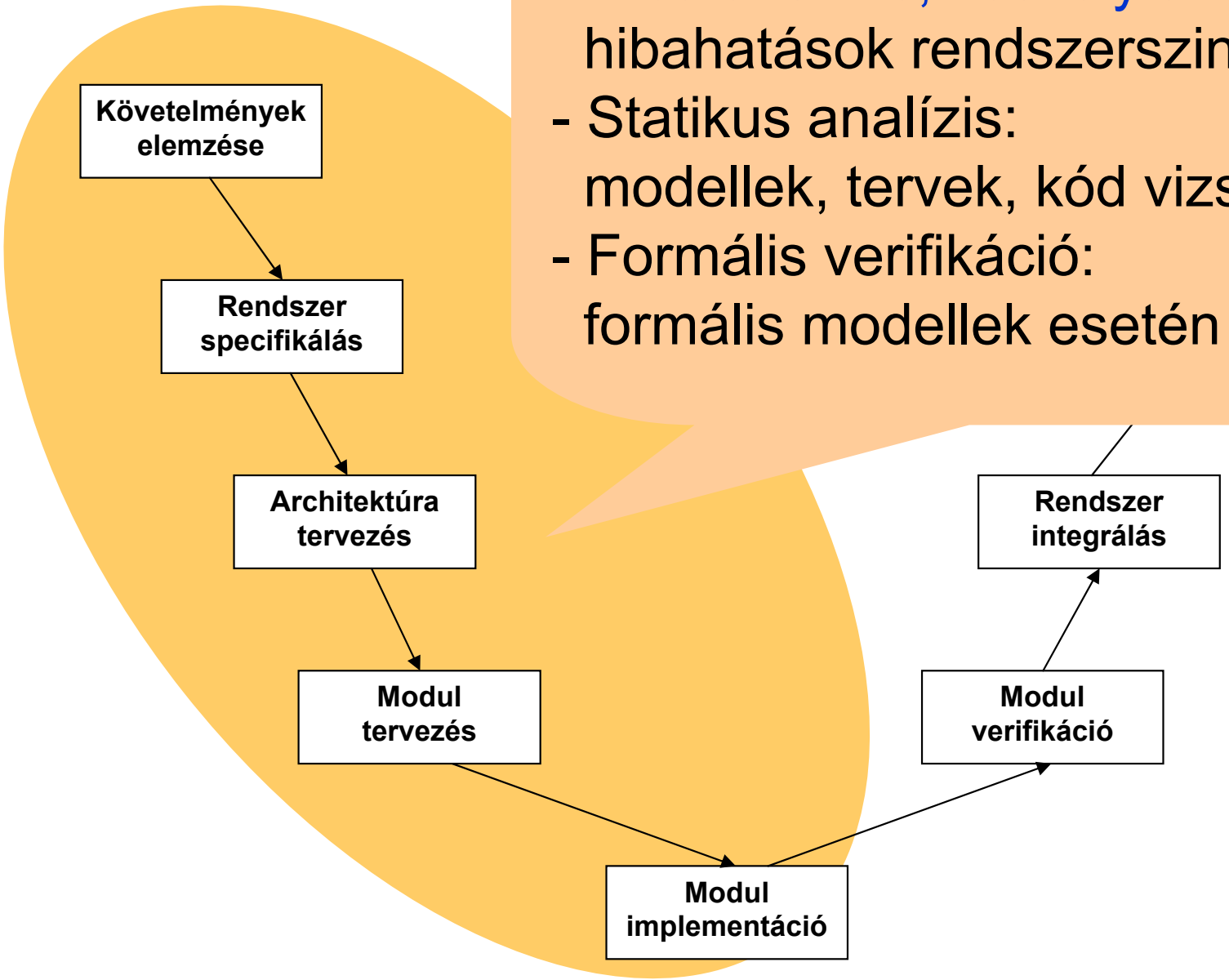
A szolgáltatásbiztonság kvalitatív analízise

Majzik István
Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék
http://www.mit.bme.hu/

Ellenőrzések a tervezési fázisban

- Hiba analízis, veszély analízis:
  hibahatások rendszerszintű felmérése
- Statikus analízis:
  modellek, tervek, kód vizsgálata
- Formális verifikáció:
  formális modellek esetén



Hibahatások analízise

- Feladatok:
  - Tervezési fázis: Hibamódok, hibahatások felmérése
  - Átadási fázis: Szolgáltatásbiztonság igazolása
  - Működési fázis: Módosítások felülvizsgálata
- Analízis célja: Komponens hibák rendszerszintű hatásának kiderítése
  - Ok-okozati szempontból:
    - Előrelépő (induktív): Esemény hatásainak vizsgálata
    - Visszalépő (deduktív): Hibahatás okainak felderítése
  - Rendszerhierarchia szempontból:
    - Alulról felfelé: Alrendszerek (komponensek) felől
    - Felülről lefelé: Rendszerszintről lebontva
- Kvalitatív analízis: Szisztematikus módszerek

Az analízis módszerei (áttekintés)

1. Ellenőrző lista
2. Hibafa
3. Eseményfa
4. Ok-következmény analízis
5. Veszély és működőképesség analízis
6. Hibamód és hatás analízis (FMEA)
7. Emberi hibák analízise
8. Állapot alapú analízis

1. Ellenőrző lista

- Technika:
  - Tapasztalatok rendszerezett összegyűjtése
  - „Ökölszabályok” megfogalmazása, ezek alkalmazása
- Biztosítja:
  - Ismert hibahatások nem maradnak ki
  - Kipróbált módszereket alkalmaz
- Hátrányok:
  - A lista nem teljes és nehezen kezelhető
  - Téves biztonságérzetet ad
  - Más környezetben az alkalmazhatóság kérdéses
- Szabványosítás:
  - Veszély indexek (pl. Dow Index, 1964)

2. Hibafa analízis

Rendszerszintű hibajelenség okainak vizsgálata

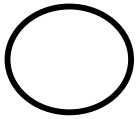
- Tipikusan felülről lefelé haladó analízis
- Felderíti a kezelendő hibaokokat és -kombinációkat

Hibafa konstrukció:

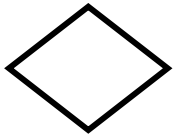
1. Rendszerszintű hibajelenség azonosítása:
   környezet, követelmények, szabványok
2. Közbenső események, pszeudo-események:
   hibajelenséghez vezetnek,
   alacsonyabb szintű események Boole-logikai kombinációi
   (AND, OR)
3. Elsődleges (alapszintű) események:
   további felbontás nincs

Hibafa grafikus elemkészlet

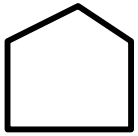
Legfelső szintű vagy közbenső esemény



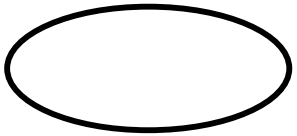
Elsődleges (alapszintű) esemény



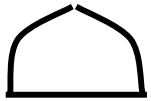
Tovább nem vizsgált esemény



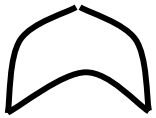
Normál esemény (nem hiba vagy veszély)



Feltétel egy összetett esemény bekövetkezéséhez

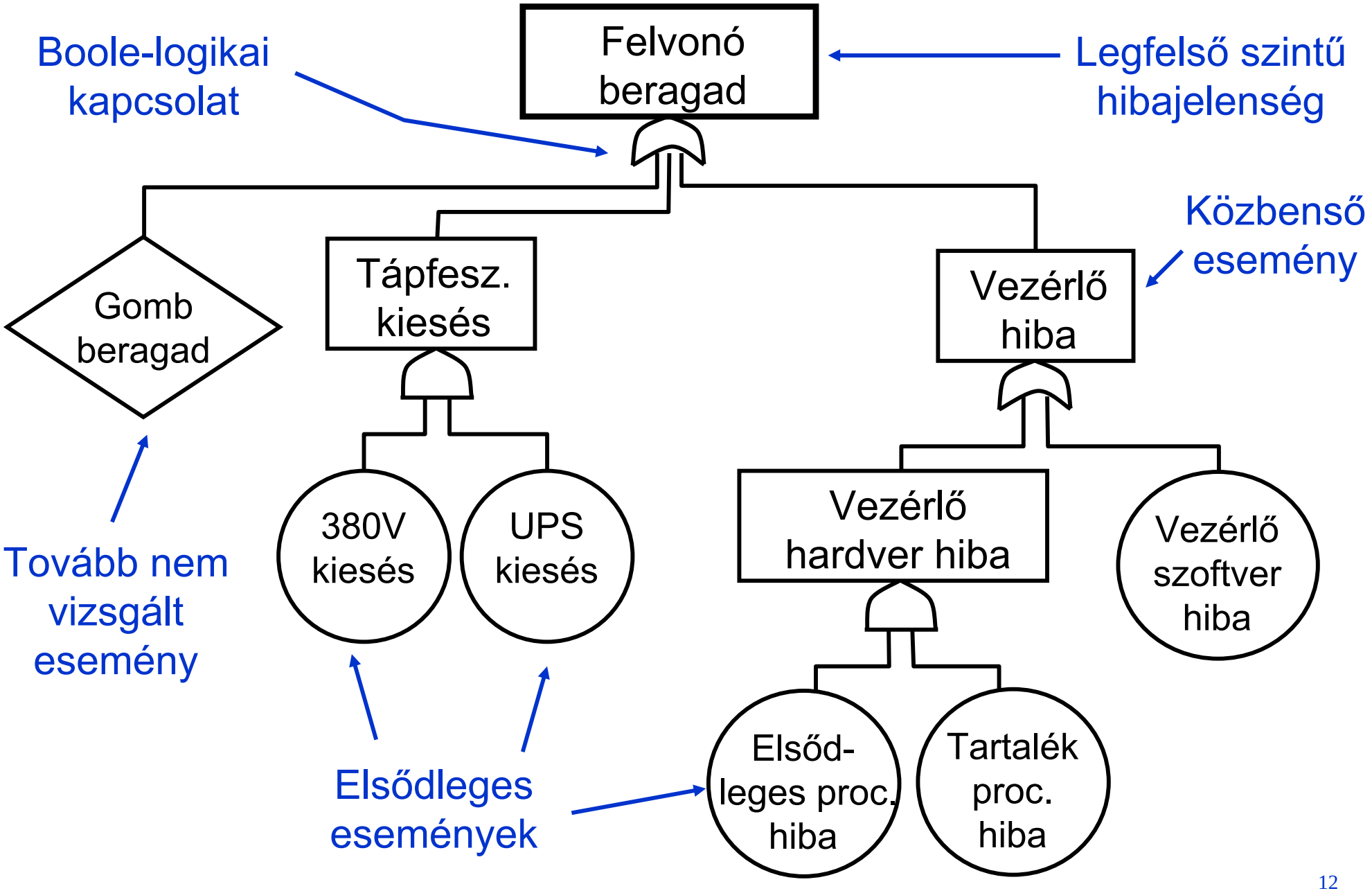


ÉS kapu



VAGY kapu

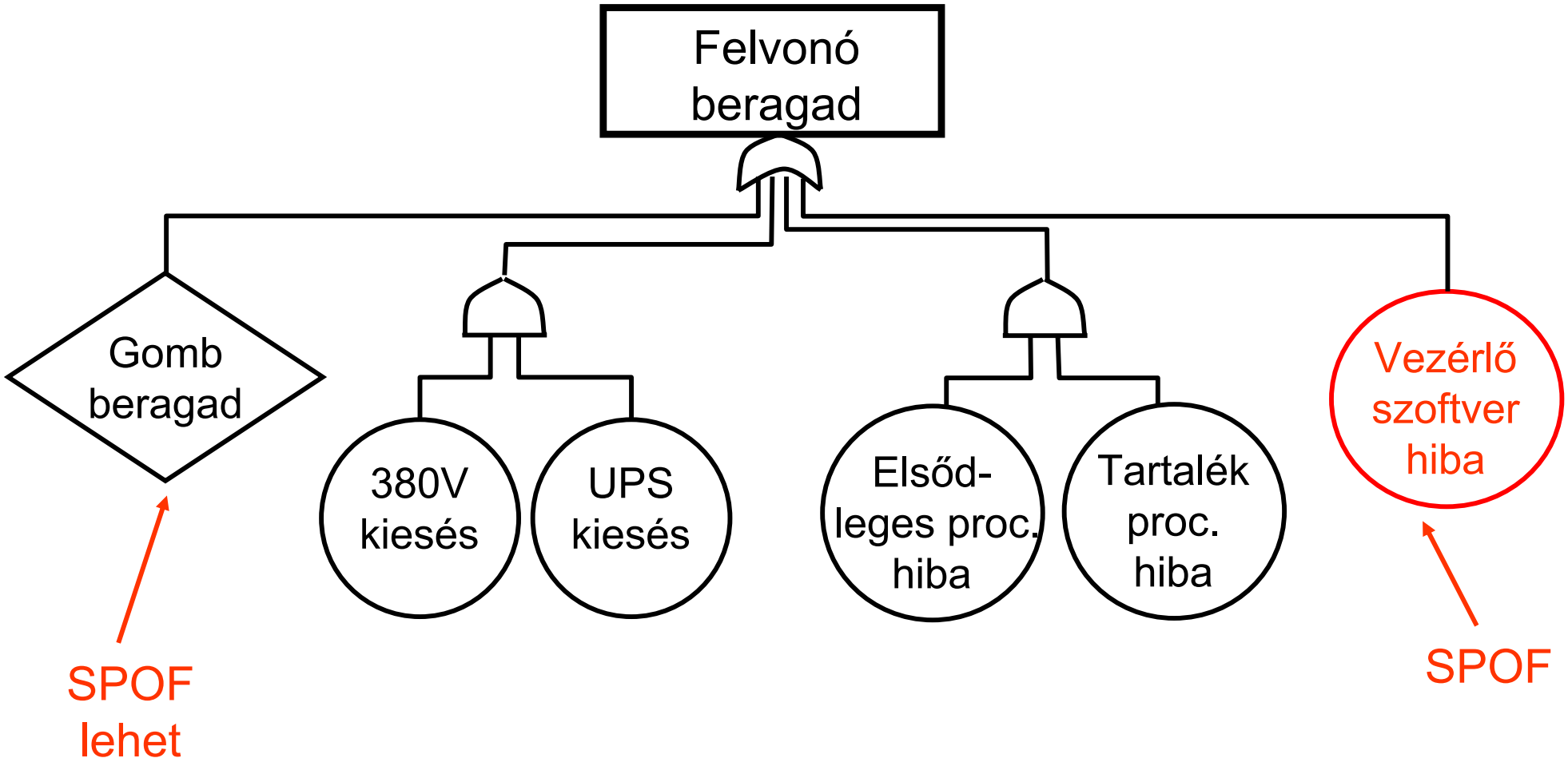
Hibafa példa: Felvonó



Minőségi (kvalitatív) analízis

- Hibafa redukció: Közbenső események és pszeudo-események feloldása
  $\rightarrow$ diszjunktív normál forma (OR a legtetején)
- Vágat:
  AND kapuval összefogott elsődleges események
- Minimális vágathalmaz: Nem redukálható
  - Nincs olyan, aminek részhalmaza is megtalálható
- Azonosítható:
  - Egyszeres hibapont (SPOF)
  - Kritikus esemény (több vágatban is szerepel)

Redukált hibafa példa: Felvonó

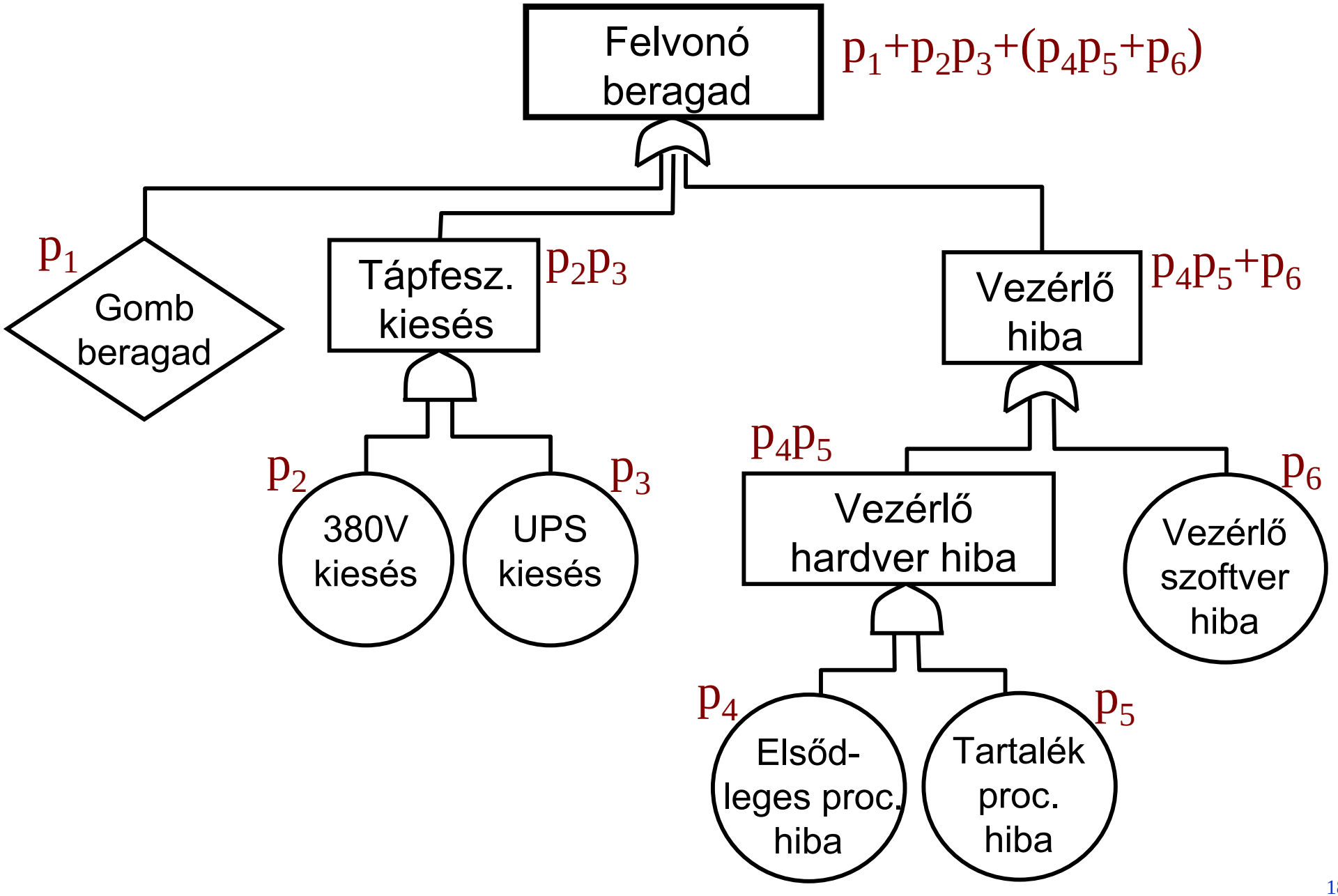


Mennyiségi (kvantitatív) analízis

- Alapszintű eseményekhez rendelt valószínűségek
  - Komponens-adat, tapasztalat, becslés
- Rendszerszintű hibajelenség valószínűségének számítása
  - AND kapu: szorzat (ha független események)
    - Pontos: $P\{A \wedge B\} = P\{A\}\, P\{B|A\}$
  - OR kapu: összegzés (felső becslés)
    - Pontos: $P\{A \vee B\} = P\{A\}+P\{B\}-P\{A \wedge B\} <= P\{A\}+P\{B\}$

- Problémák:
  - Korreláló hibák
  - Időbeli (hiba)szekvenciák kezelése
- Események időtartama figyelembe vehető
  - Időfüggvények manipulációja

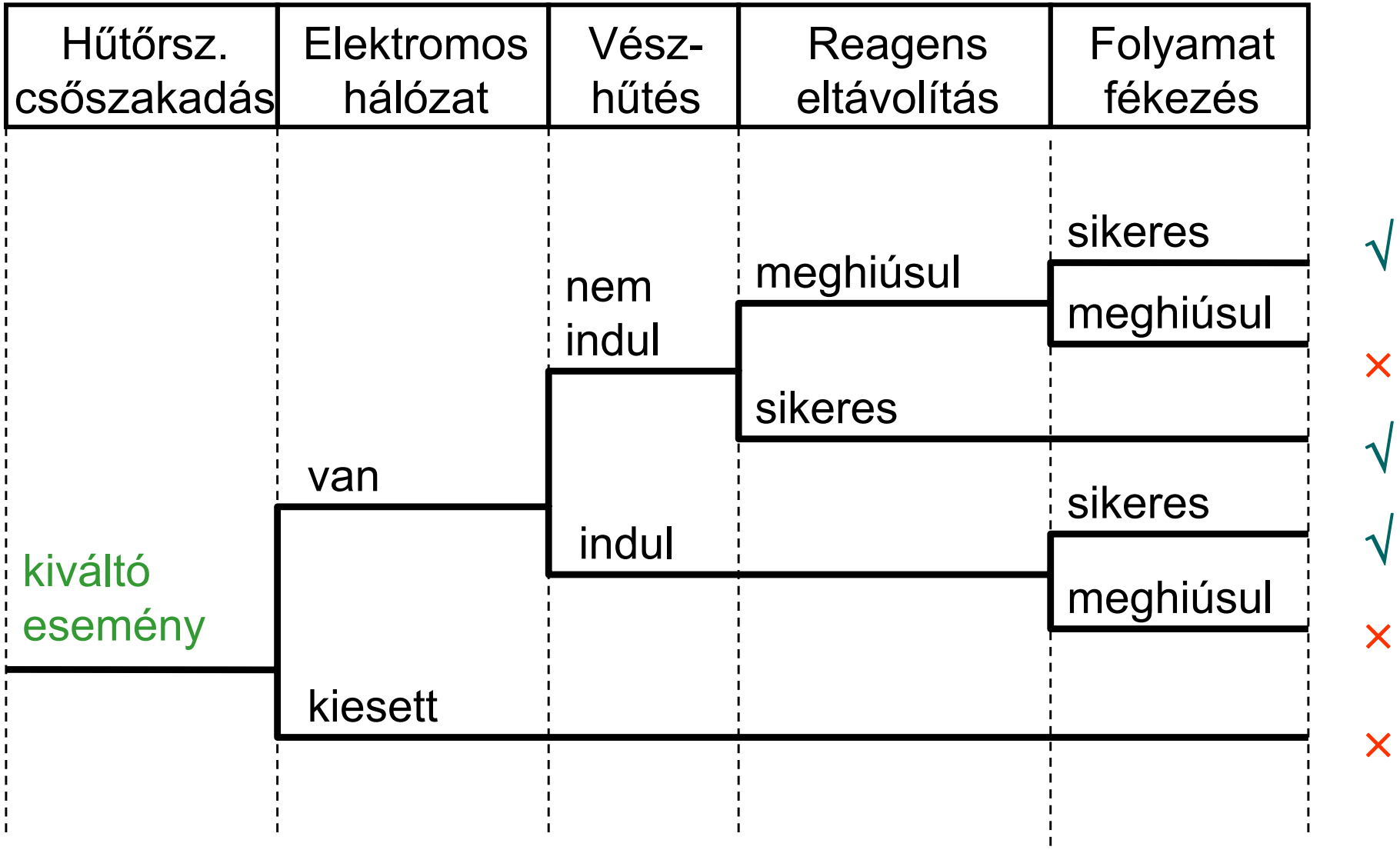
Hibafa példa: Felvonó



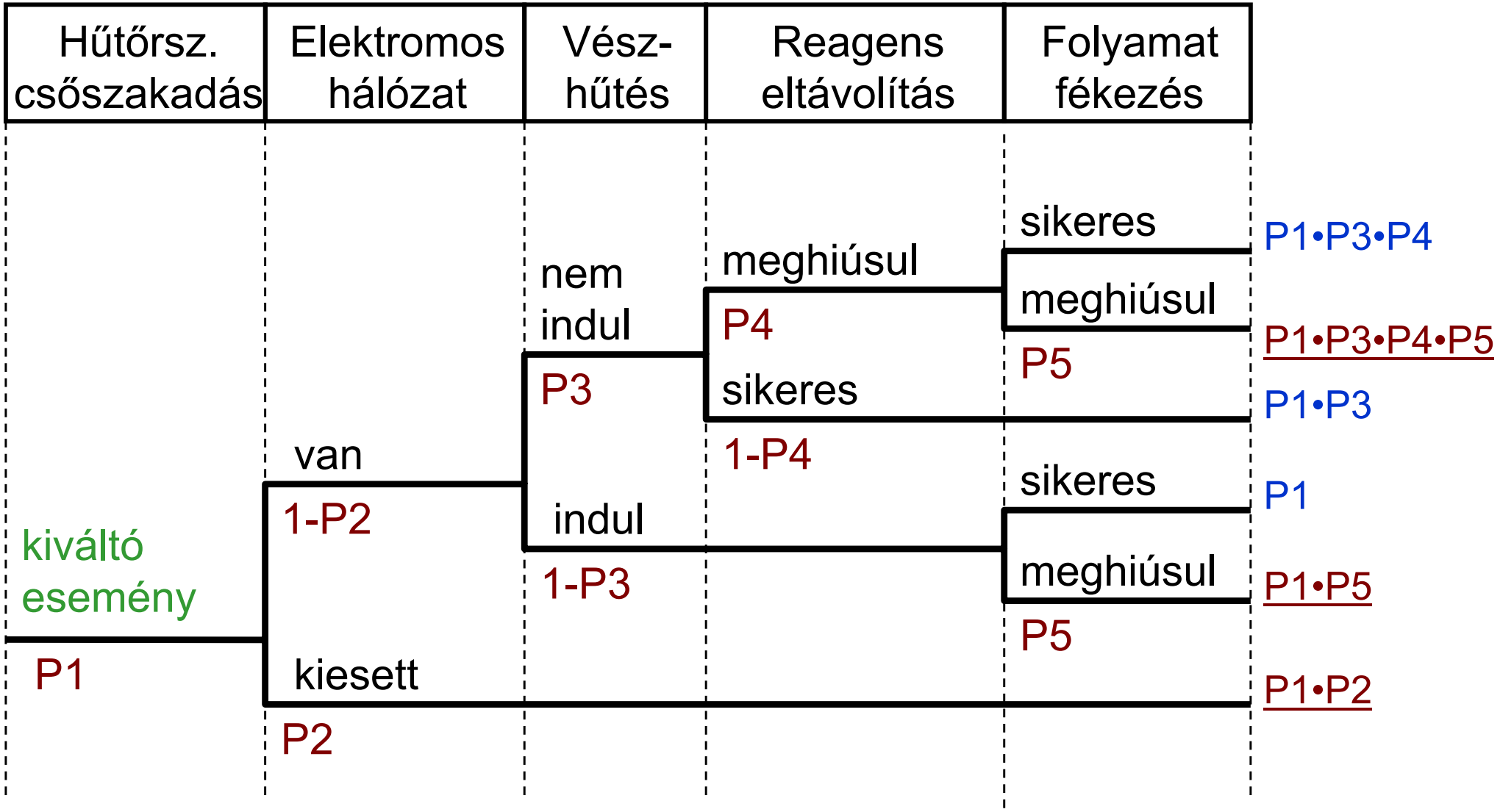
3. Eseményfa analízis

- Előrelépő analízis:
  Elsődleges események következményeit vizsgálja
  - Kiváltó esemény: pl. egy komponens hibája
  - Következmények: más komponensek állapotától függ
  - Sorrendezés: oksági kapcsolat, időbeli viszony
  - Elágazások: események bekövetkezése
- „Forgatókönyvek” vizsgálata
  - Utak valószínűsége (elágazások valószínűsége alapján)
  - Hibatűrés, védelmi rendszerek hatékonysága
- Előnyök: Eseményszekvenciák vizsgálhatók
- Korlátok: Komplexitás, többszörös események

Eseményfa példa: Reaktorhűtés



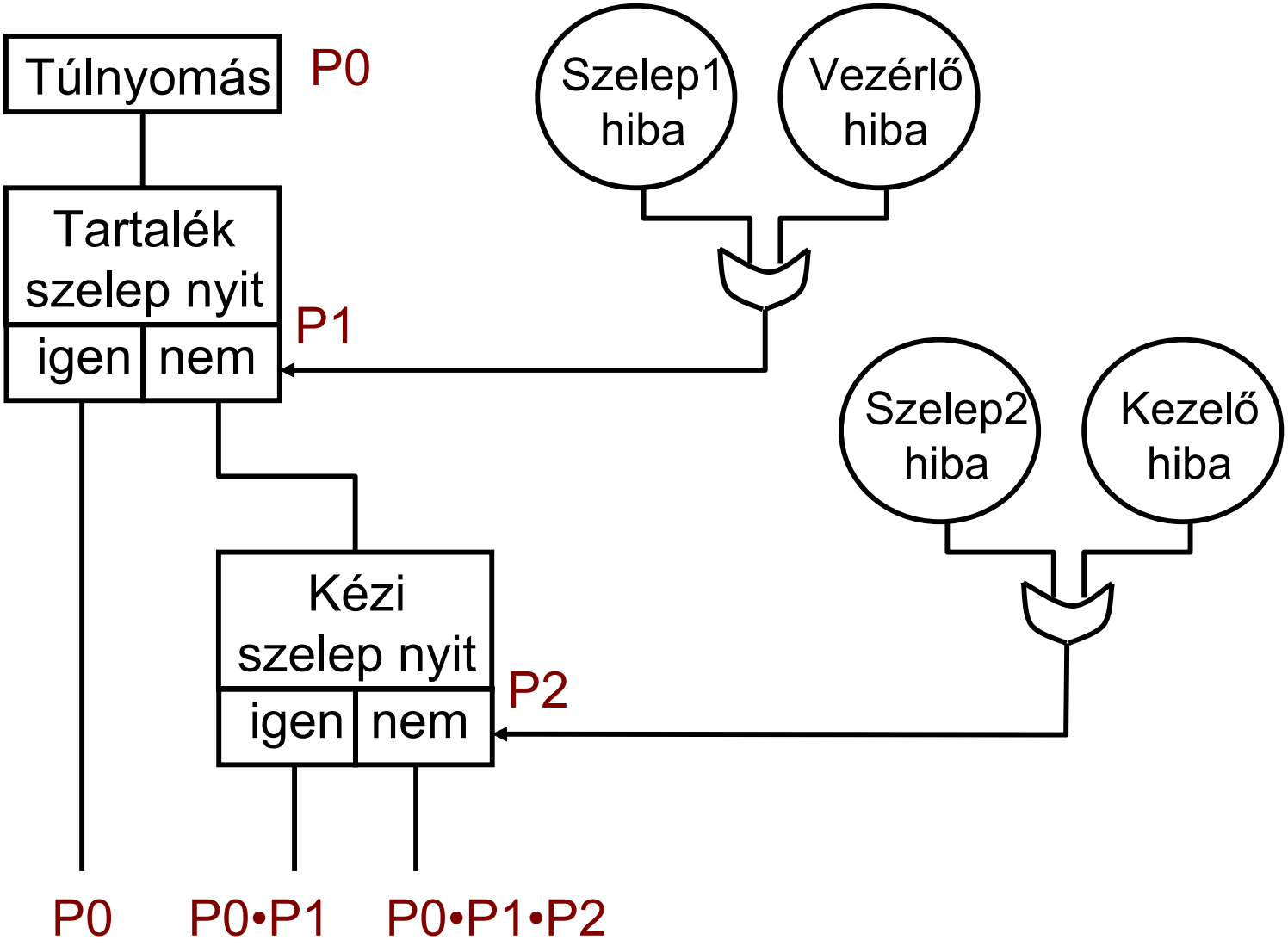
Eseményfa példa: Reaktorhűtés



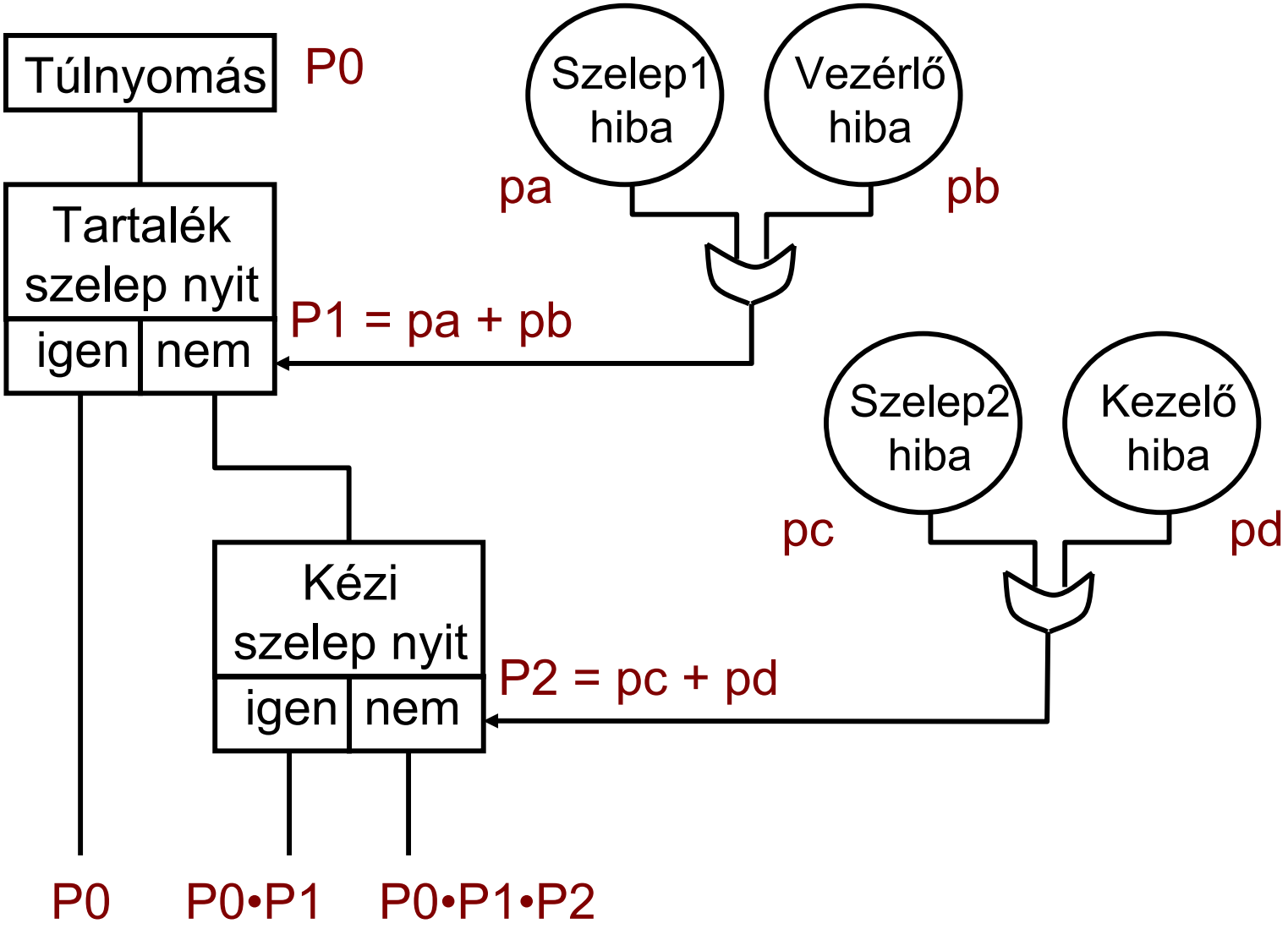
4. Ok-következmény analízis

- Eseményfa és hibafa összekapcsolása
  - Eseményfa: forgatókönyvek (szekvencia)
  - Csatolt hibafa: esemény bekövetkezés okai, rendelkezésre állás számítása
- Előnyök:
  - Szekvenciák (előrelépő analízis) és ok-okozati kapcsolatok (hátralépő analízis) együtt
- Korlátok:
  - Minden kiváltó eseményhez külön diagram szükséges

Példa ok-következmény analízisre



Példa ok-következmény analízisre



5. Veszély és működőképesség analízis

- HAZOP: Hazard and operability analysis
- Elterjedés: Vegyipari folyamatok
  - A tervezettől eltérő anyagáramlás okozza a hibát
  - Hibaszótár használata:
    NO, MORE, LESS, AS WELL AS, PART OF, REVERSE, …
- Informatikai folyamatok:
  - Információáramlásra alkalmazható hibaszótár
  - Lehetséges eltérések szisztematikus felmérése
    (folyamat diagramok, adatfolyam hálózatok alapján)

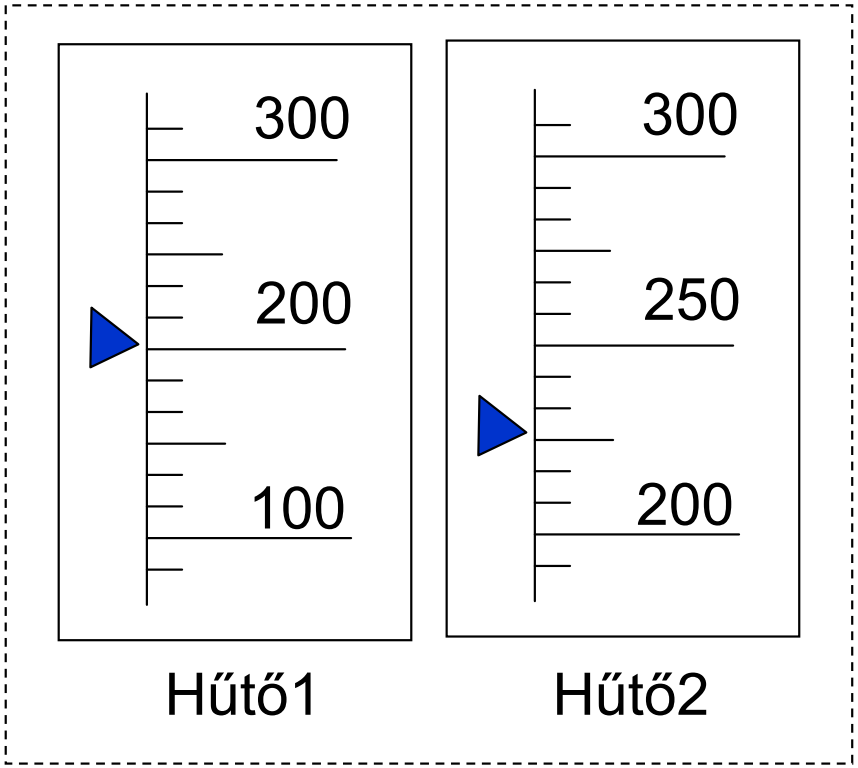
6. Hibamód és hatás analízis

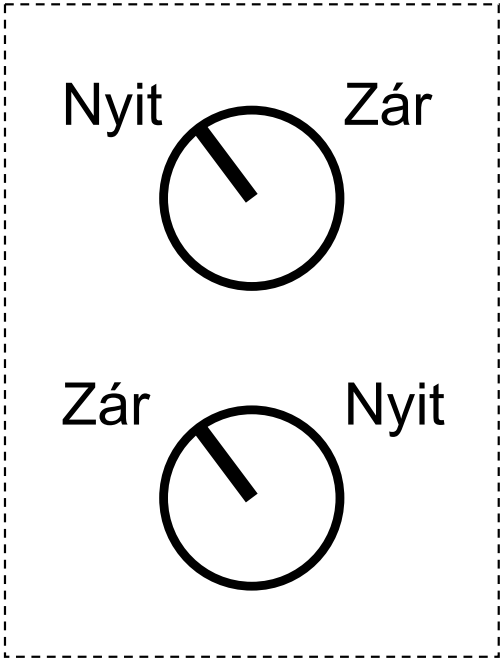
- FMEA: Failure Modes and Effects Analysis
- Hibák és hatásaik szisztematikus áttekintése
- Előny:
  - Rendszerkomponensek ismert hibáinak vizsgálata
  - Redundancia felismerhető (hatás kiküszöbölve)
  - Hiba kritikusságának elemzésével kiegészíthető (FMECA)

Komponens	**Hibamód**	**Valószínűség**	**Hatás**
L határérték-túllépés vizsgálat	> L átmegy ≤ L nem megy át	65% 35%	- túlnyomás - technológiai hiba
...	...	...	...

7. Emberi hibák analízise

- Kvalitatív módszerek (FMEA jellegű táblázat):
  - Művelet – hibázás – hatások – okok – elkerülés
  - Fizikai és mentális elvárások elemzése
  - Hibalehetőségek ← pl. kezelői felület problémái





8. Állapot alapú analízis

- A hibaállapotok felvétele állapot alapú modellben
  - Állapotok, átmenetek, feltételek, trigger események, akciók
  - Hibamódok felvétele
- Kvalitatív analízis: Elérhetőségi analízis
  - Milyen hibaállapot következhet be (adott feltételek mellett)?
    - Veszélyes állapotok a biztonság szempontjából
  - Gyakran visszafelé keresés: Mi vezethet adott állapothoz?
- Gyakori a kvantitatív analízis
  - Kiegészítés az állapotátmenetek valószínűségével, gyakoriságával
  - Részletesen ld. később!