Veszély analízis

Rendszertervezés és -integráció előadás

dr. Majzik István

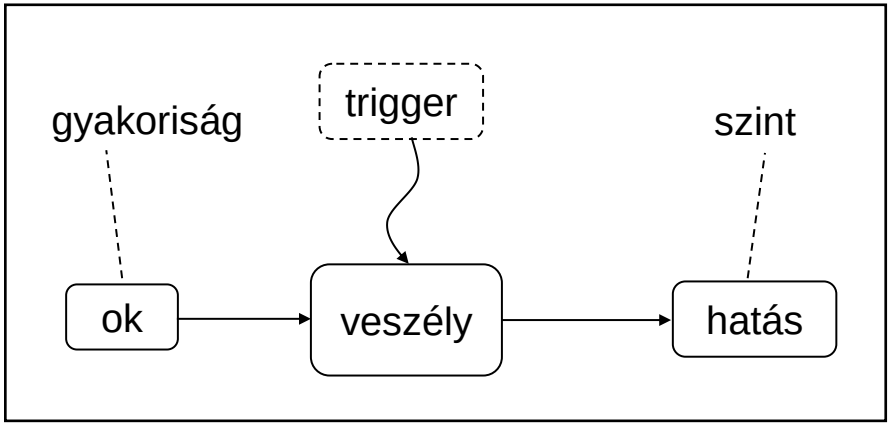
Méréstechnika és
Információs Rendszerek
Tanszék

Célkitűzések

A veszély analízis

- Cél: Hibahatások és veszélyes állapotok kialakulásának felmérése
  - Mi okozhat rendszerszintű veszélyes állapotot?
  - Mit okoz egy komponens szintű hiba?
- Eredmények:
  - Veszély katalógus
  - Veszélyek minősítése
    - Előfordulási gyakoriság
    - Következmények szintje

    → Kockázati mátrix



- Alapot képez a kockázatcsökkentéshez

Cél: Kockázati mátrix elkészítése

- Védelmi szint: Kezelendő kockázatok

Veszély szint /gyakoriság	Elhanyagol-ható	Mérsékelt	Kritikus	Katasztrofális
Gyakori	P2 szelep beragad	.	.	.
Valószínű	.	Pumpa beragad	P3 szelep beragad	J1 jelfogó zárva beragad
Esetenkénti	Motor nem indul	.	.	.
Ritka	.	Tartály ereszt	.	D3 dióda szakadása
Valószínűt-len	Cső repedése	.	R1 szakadt	D3 dióda rövidzára
Lehetetlen	.	.	.	.

Piros tartomány: Kockázat-csökkentés szükséges

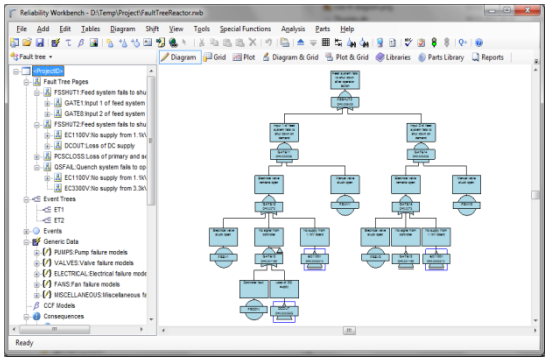
A módszerek csoportosítása

- Ok-okozati szempontból:
  - Előrelépő (induktív): Események hatásainak vizsgálata
  - Visszalépő (deduktív): Veszélyek okainak felderítése
- Rendszerhierarchia szempontból:
  - Alulról felfelé: Komponensek felől rendszerszint felé
  - Felülről lefelé: Rendszerszintről a komponensek felé

Fontos: Szisztematikus módszerek szükségesek

Veszély analízis technikái (áttekintés)

- Informális analízis
  - Ellenőrző listák
- Szisztematikus analízis a veszély okok és következmények vizsgálatára:
  - Hibafa analízis (FTA)
  - Eseményfa analízis (ETA)
  - Ok-következmény analízis (CCA)
  - Hibamód és hatás analízis (FMEA)



Ellenőrző listák

Ellenőrző listák szerepe

- Technika:
  - Tapasztalatok, tipikus hibák rendszerezett gyűjteménye
  - Alkalmazás: Mint „ökölszabályok”
- Biztosítja:
  - Ismert veszélyforrások nem maradnak ki
  - Kipróbált megoldások alkalmazhatók
- Hátrányok:
  - A lista nem teljes és nehezen kezelhető
  - Téves biztonságérzetet ad
  - Más környezetben az alkalmazhatóság kérdéses

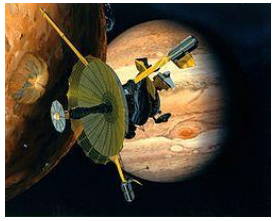
Specifikációk és tervek vizsgálati szempontjai

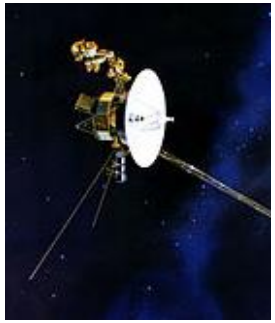
- Teljesség
  - Funkciók, komponensek, eszközök
- Ellentmondás-mentesség
  - Belső és külső (pl. szabványok)
  - Követhetőség
- Megvalósíthatóság
  - Erőforrások rendelkezésre állása
  - Használhatóság
  - Karbantarthatóság
  - Költségbeli, technikai, környezeti kockázatok elkerülése
- Tesztelhetőség
  - Specifikusság
  - Egyértelműség
  - Számszerűsíthetőség

Specifikáció vizsgálata: Motiváció

- Tapasztalat: Sok hiba visszavezethető hiányos vagy ellentmondásos specifikációra
  - Példa: Voyager és Galileo űrszondák szoftver validációja során felfedezett hibák statisztikája

    78% (149/192) specifikációs hiányosság, ebből
    - 23% veszélyes állapotban ragadás (nincs kilépés)
    - 16% időzítési kényszerek megadásának hiánya
    - 12% nincs specifikált reakció külső eseményre
    - 10% bemeneti érték ellenőrzésének hiánya



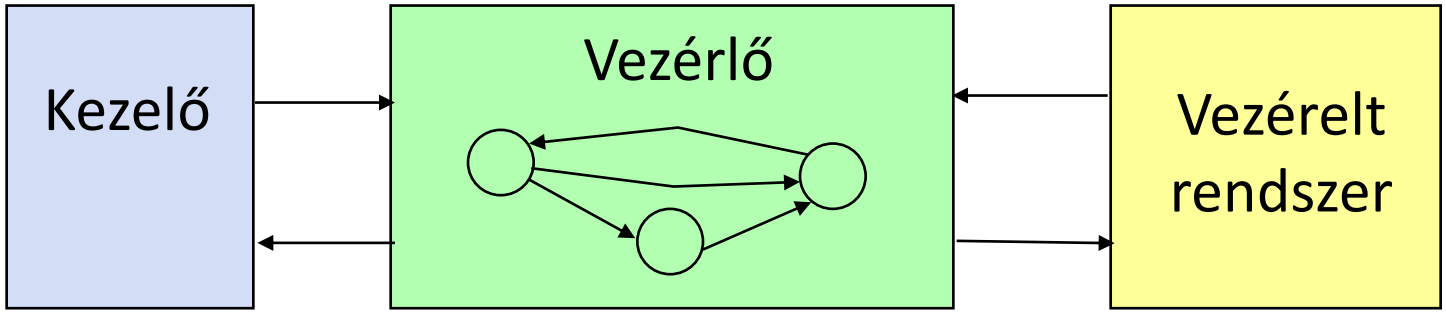


- Megoldás lehet:
  - Szigorú specifikációs nyelv (kötött szintaxis kényszerít)
  - Ellenőrzött tervezési minták használata
  - (Utólagos) ellenőrzés

Példa: Ellenőrző lista állapotgép modellekhez

Teljesség és ellentmondásmentesség:

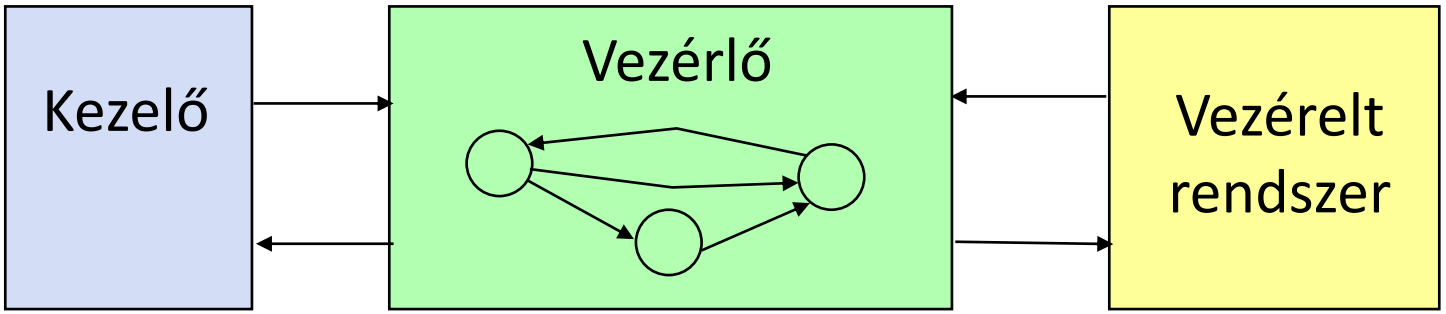
- Állapotdefiníció
- Bemenetek (események)
- Kimenetek
- Kimenetek és trigger kapcsolata
- Állapotátmenetek
- Ember-gép interfész



Példa: Ellenőrző lista állapotgép modellekhez

- Állapotdefiníció
- Bemenetek (
- Kimen
- Kimen
- Állapo
- Ember-gép interfész

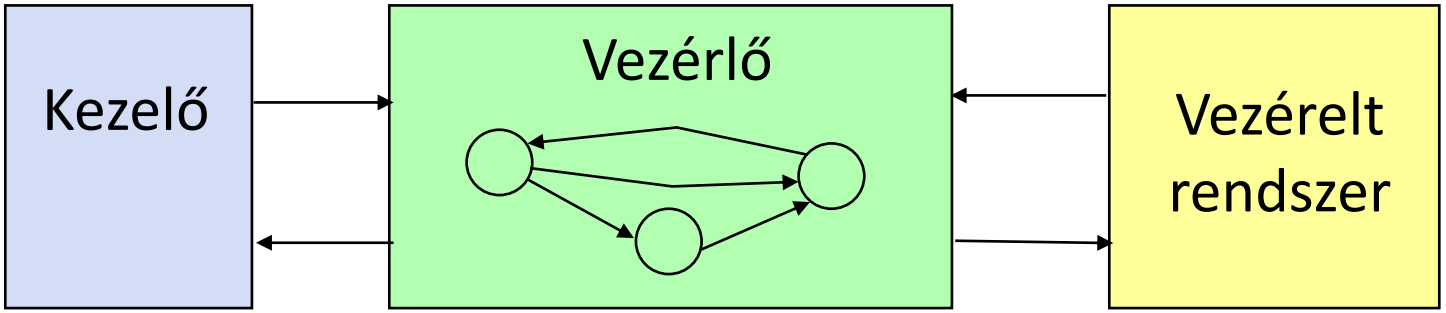
• Biztonságos a kezdőállapot
• Érvénytelen állapot definiált:
kimaradó bemeneti események esetén timeout,
ide lép és nincs a kimeneten akció szinkronizálásig



Példa: Ellenőrző lista állapotgép modellekhez

- Állapotdefiníció
- Bemenetek (események)
- Kimene
- Kimen
- Állapo
- Ember

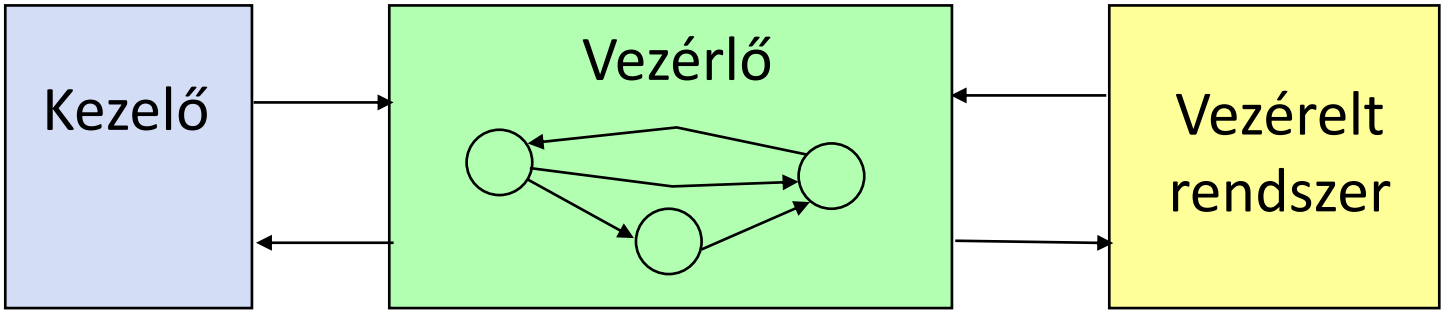
- Minden bemenetre van megadott reakció
- Egyértelmű (determinisztikus) reakciók vannak
- Van bemeneti ellenőrzés (pl. érték, idő)
- Hibás bemenet kezelése megtörténik
- Megszakítások gyakorisága korlátozott



Példa: Ellenőrző lista állapotgép modellekhez

- Állapotdefiníció
- Bemenetek (események)
- Kimenetek
- Kimen
- Állapo
- Ember

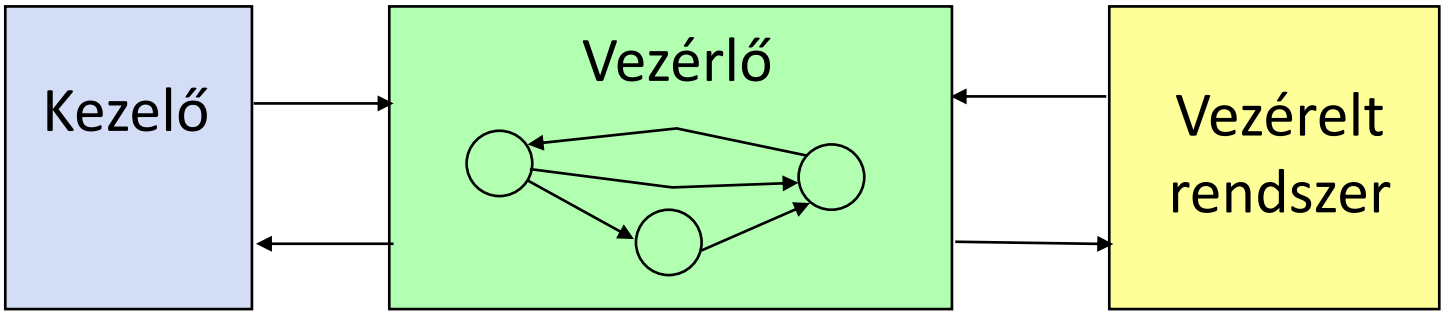
- Hihetőségvizsgálat kritériumai adottak
- Fel nem használt kimenetek ellenőrzöttek
- Környezeti feldolgozó kapacitás betartva



Példa: Ellenőrző lista állapotgép modellekhez

- Állapotdef
- Bemenete
- Kimenetek
- Kimenetek és trigger kapcsolata
- Állapotátmenetek
- Ember-gép interfész

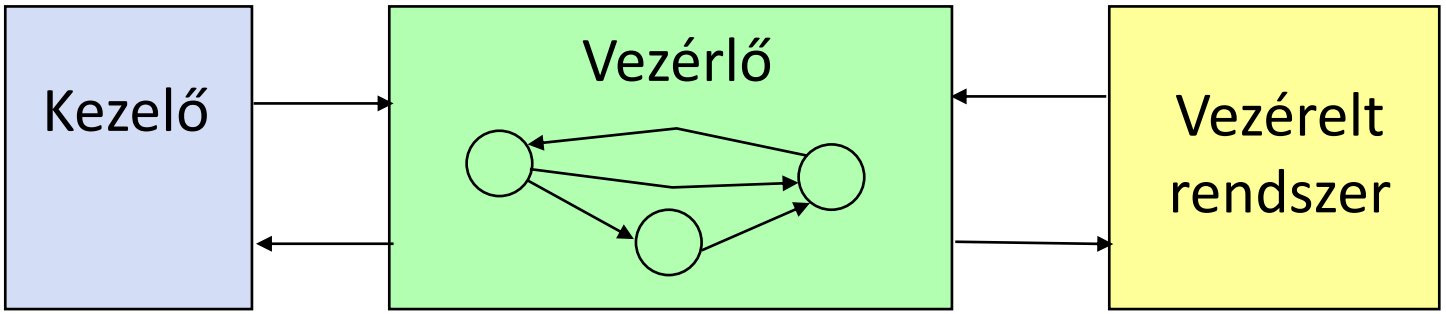
- Kimenetek hatása ellenőrzött a bemeneteken keresztül
- Szabályzási kör stabil



Példa: Ellenőrző lista állapotgép modellekhez

- Állap
- Bem
- Kime
- Kime
- Állapotátmenetek
- Ember-gép interfész

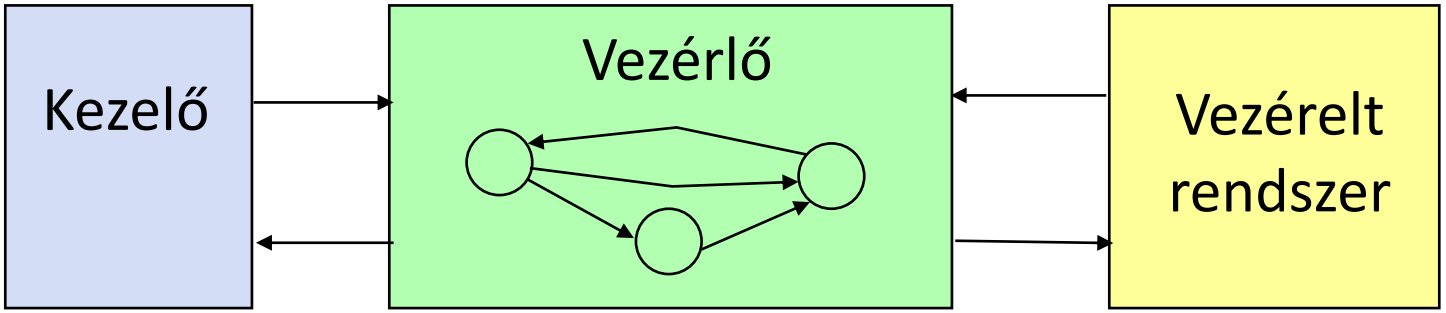
- Minden állapot elérhető statikusan
- Állapotátmenetek visszafordíthatók (út van)
- Több átmenet van veszélyes állapotból biztonságosba
- Megerősített átmenet van biztonságos állapotból veszélyes állapotba



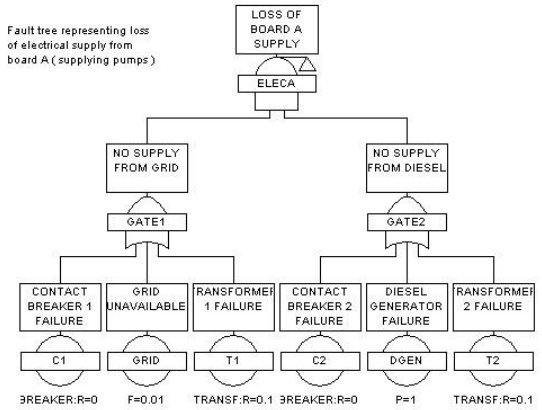
Példa: Ellenőrző lista állapotgép modellekhez

- Állapotdefiníció
- Bem
- Kim
- Kim
- Állapotátm ek
- Ember-gép interfész

- Kijelzett események frissítése definiált
- Kijelzett események gyakorisága korlátozott
  (kezelő túlterhelése elkerülve)
- Kezelő felé kijelzendő események sorrendezettek (prioritás)



Hibafa analízis

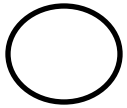


Hibafa konstrukció

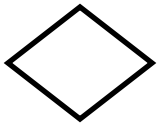
- Rendszerszintű veszély okainak vizsgálata
  - Tipikusan felülről lefelé haladó analízis
  - Felderíti a kezelendő hibaokokat és -kombinációkat
- Hibafa konstrukció:
  1. Rendszerszintű veszély, veszélyes állapot azonosítása: környezet, követelmények, szabványok
  2. Közbenső események, pszeudo-események: veszélyhez vezetnek, alacsonyabb szintű események Boole-logikai kombinációi (AND, OR)
  3. Elsődleges (alapszintű) események: további felbontás nincs

Hibafa grafikus elemkészlet

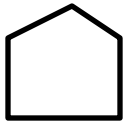
Legfelső szintű vagy közbenső esemény



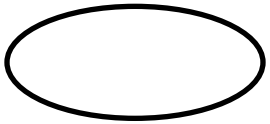
Elsődleges (alapszintű) esemény



Tovább nem vizsgált esemény



Normál esemény (nem hiba vagy veszély)

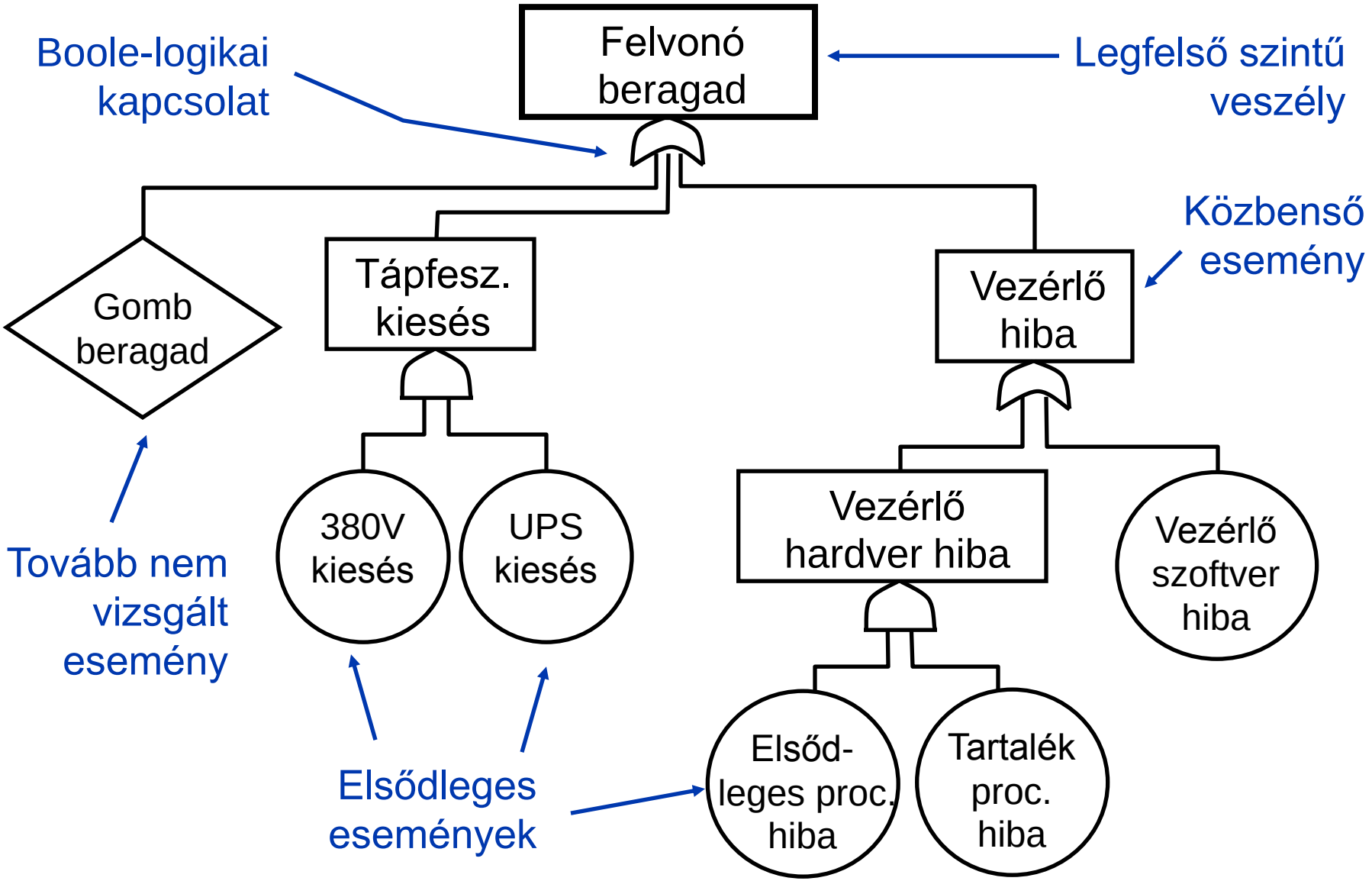


Feltétel egy összetett esemény bekövetkezéséhez

Logikai ÉS (AND) kapu

Logikai VAGY (OR) kapu

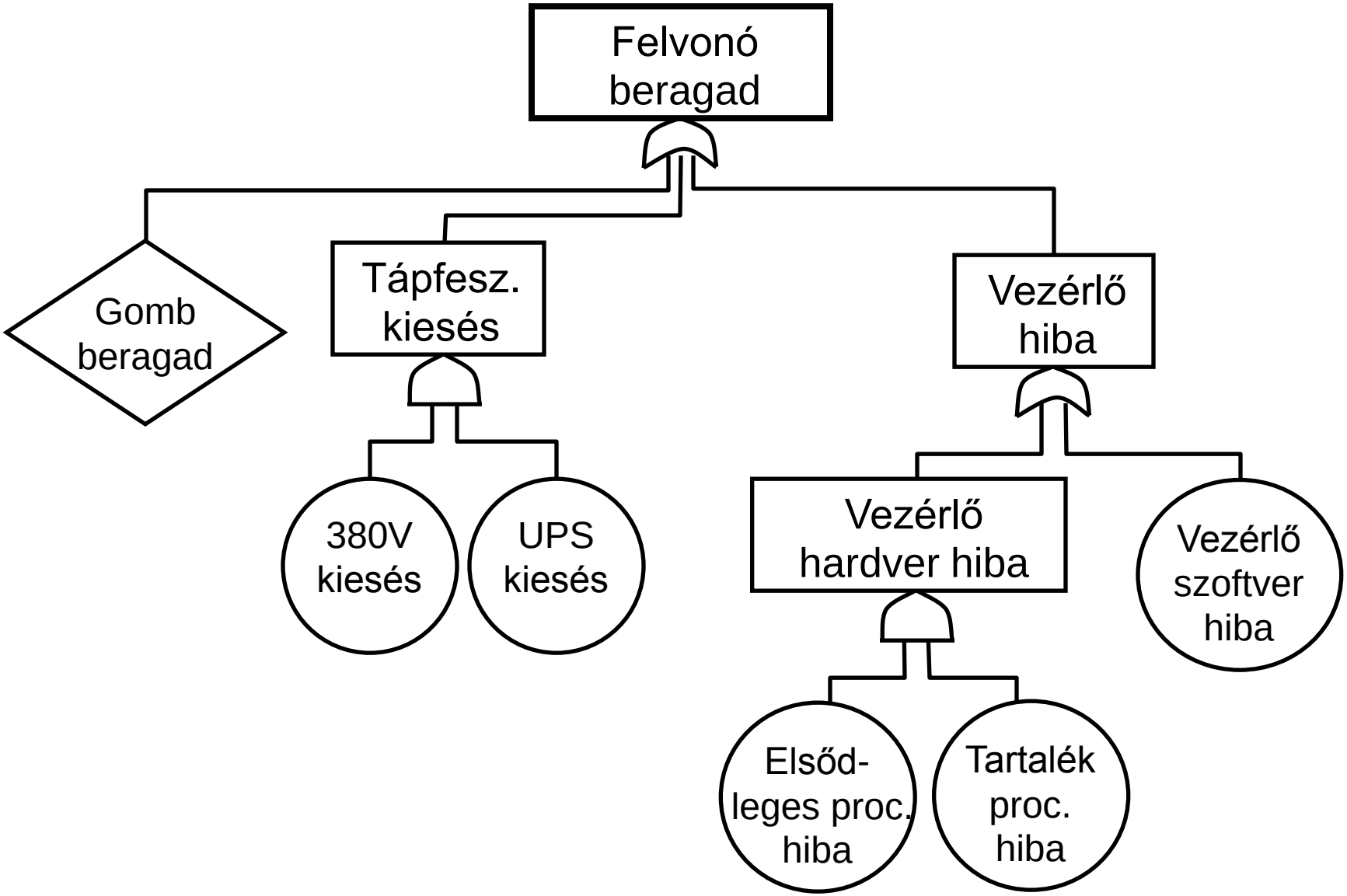
Hibafa példa: Felvonó



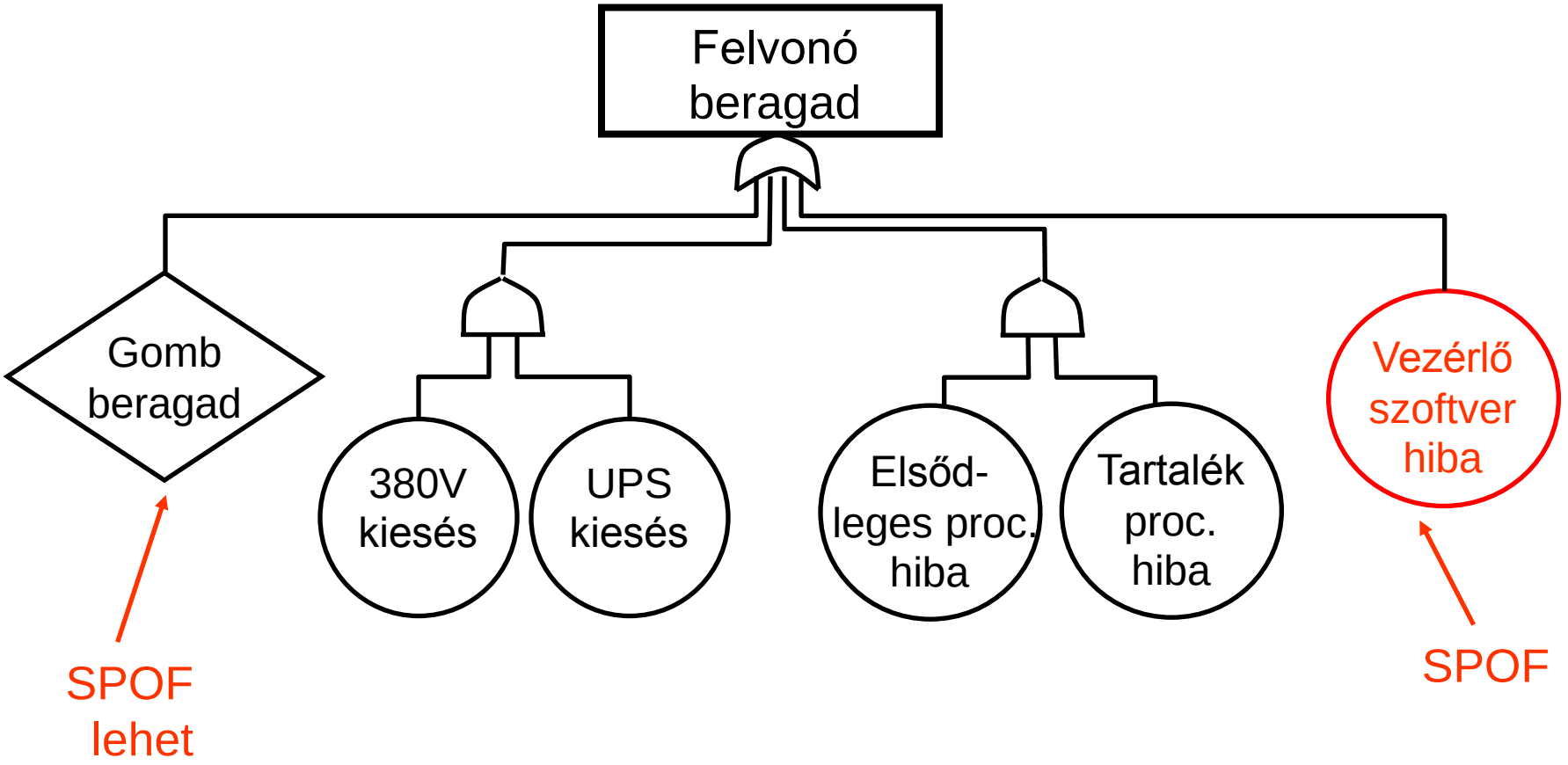
Minőségi (kvalitatív) analízis

- Hibafa redukció: Közbenső események és pszeudo-események feloldása
  → diszjunktív normál forma (OR a legtetején, AND ágakkal)
- Vágat:
  AND kapuval összefogott elsődleges események
- Minimális vágathalmaz: Nem redukálható
  - Nincs olyan vágat, aminek részhalmaza is megtalálható
- Azonosítható:
  - Egyszeres hibapont (SPOF)
  - Több vágatban is szereplő (kritikus) esemény

Hibafa példa: Felvonó



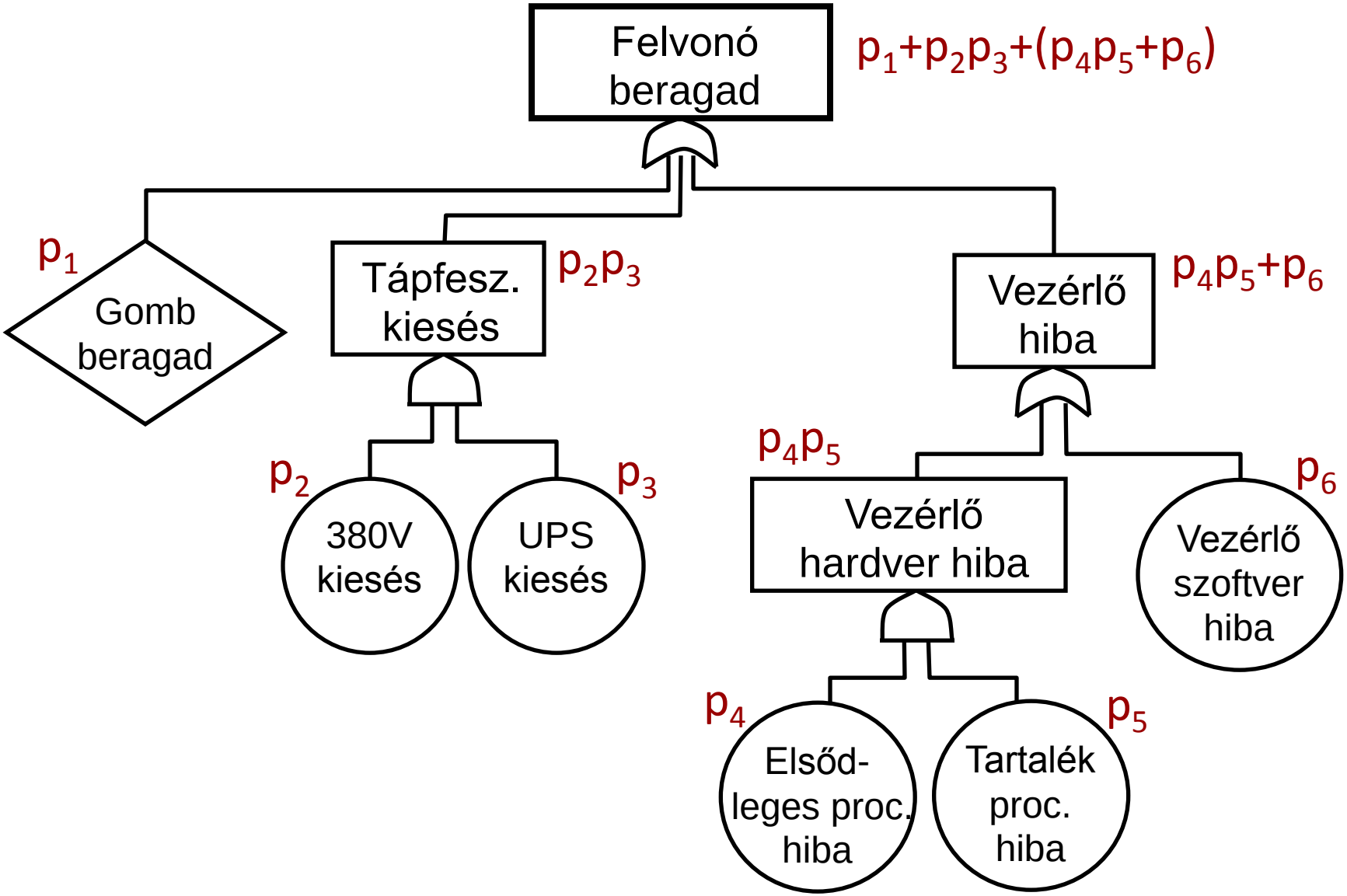
Redukált hibafa példa: Felvonó



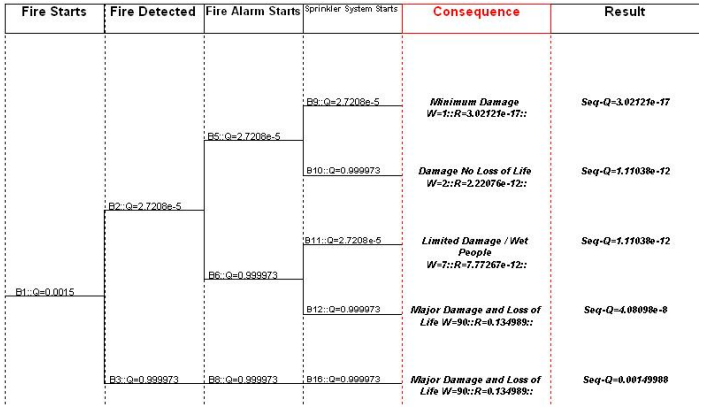
Mennyiségi (kvantitatív) analízis

- Alapszintű eseményekhez rendelt valószínűségek
  - Komponens-adat, tapasztalat, becslés
- Rendszerszintű veszély valószínűség számítása
  - AND kapu: szorzat (ha független események)
    - Pontos: P{A és B} = P{A} · P{B|A}
  - OR kapu: összegzés (felső becslés)
    - Pontos: P{A vagy B} = P{A}+P{B}-P{A és B} <= P{A}+P{B}
- Problémák:
  - Korreláló hibák
  - Időbeli (hiba)szekvenciák kezelése

Hibafa példa: Kvantitatív analízis



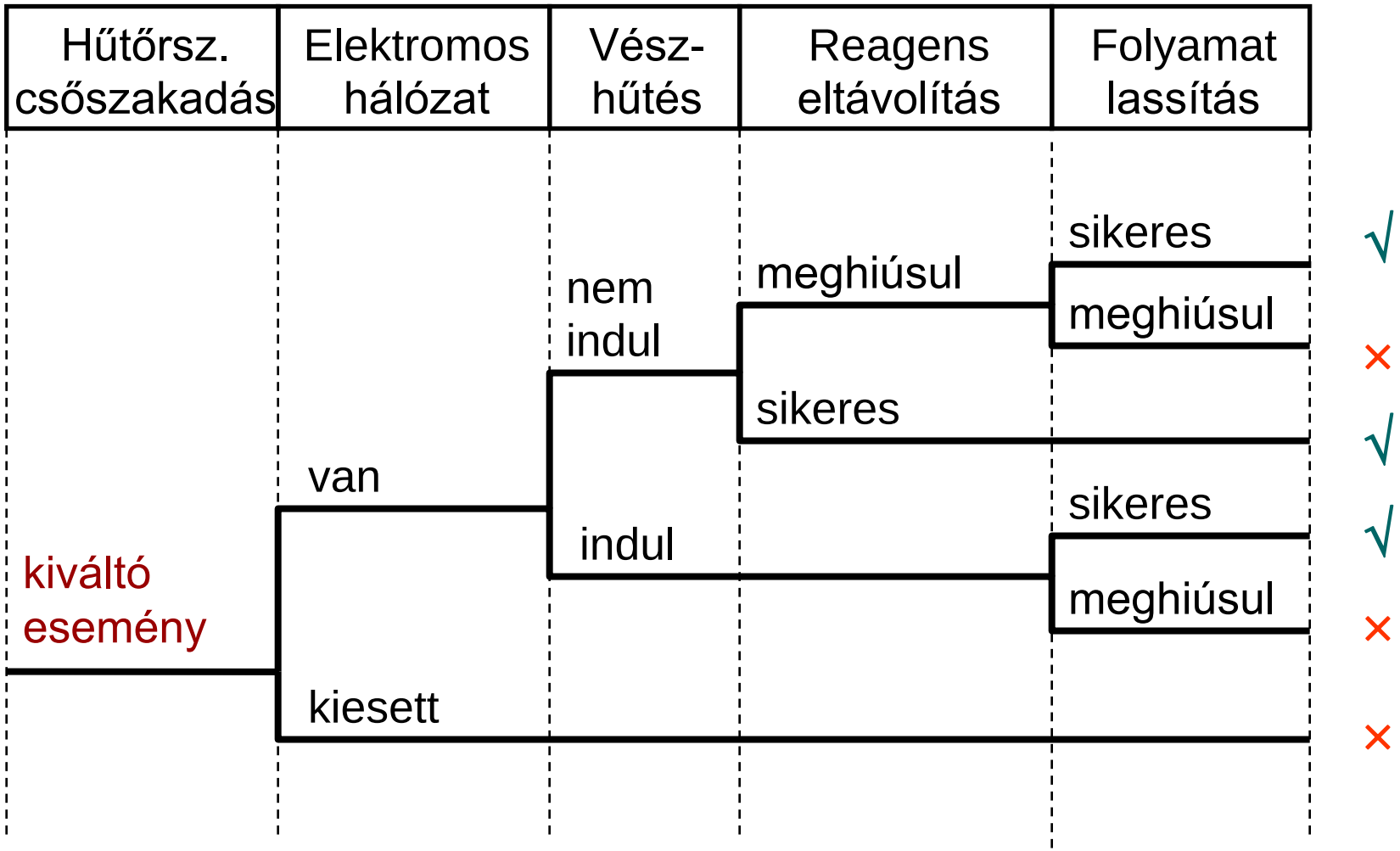
Eseményfa analízis



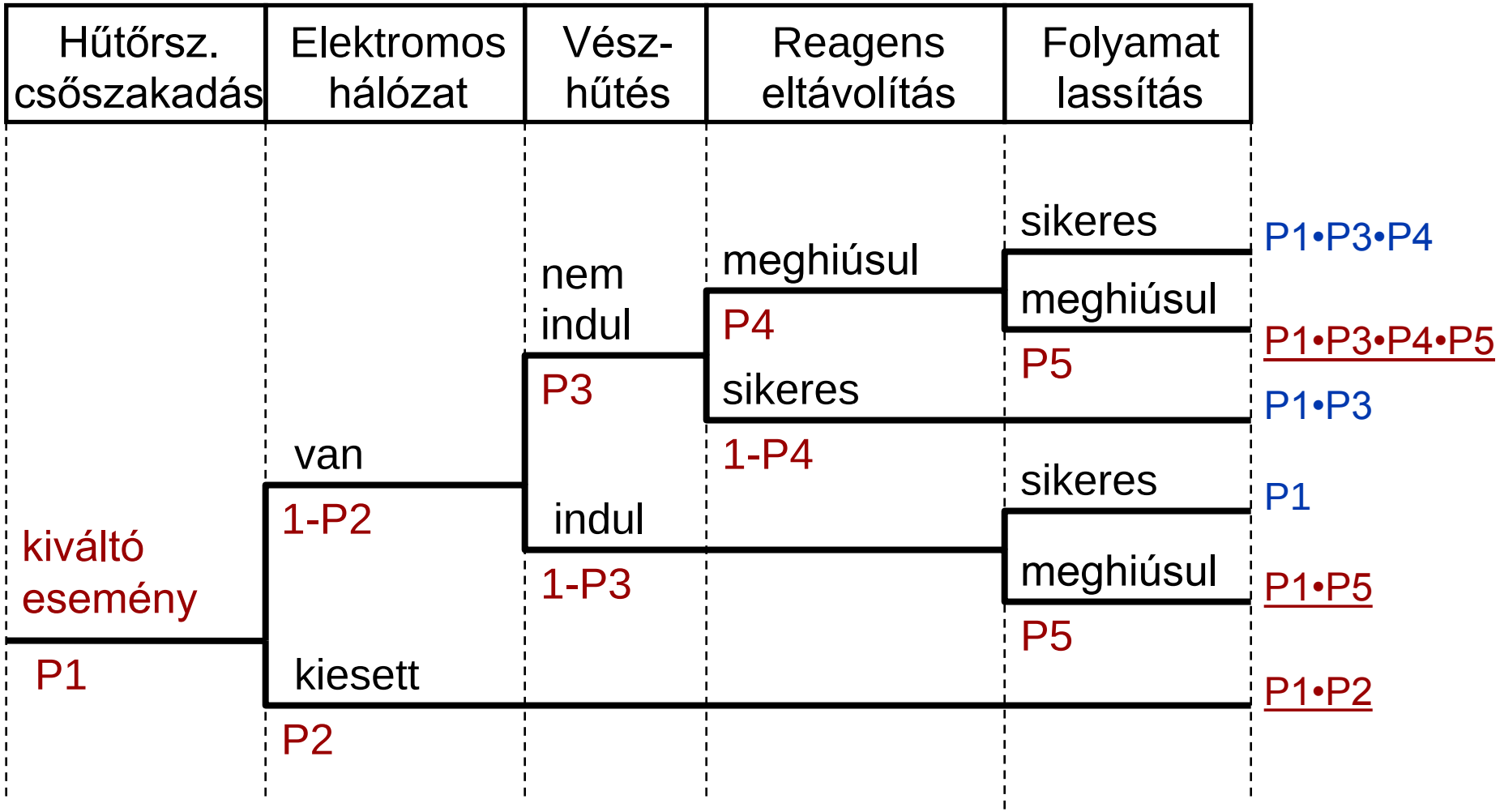
Eseményfa konstrukció

- 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
- Baleset / veszély „forgatókönyvek” vizsgálata
  - Utak valószínűsége (elágazások valószínűsége alapján)
  - Védelmi rendszerek hatékonysága
- Előnyök: Eseményszekvenciák vizsgálhatók
- Korlátok: Komplexitás, többszörös események

Eseményfa példa: Reaktorhűtés



Eseményfa példa: Reaktorhűtés

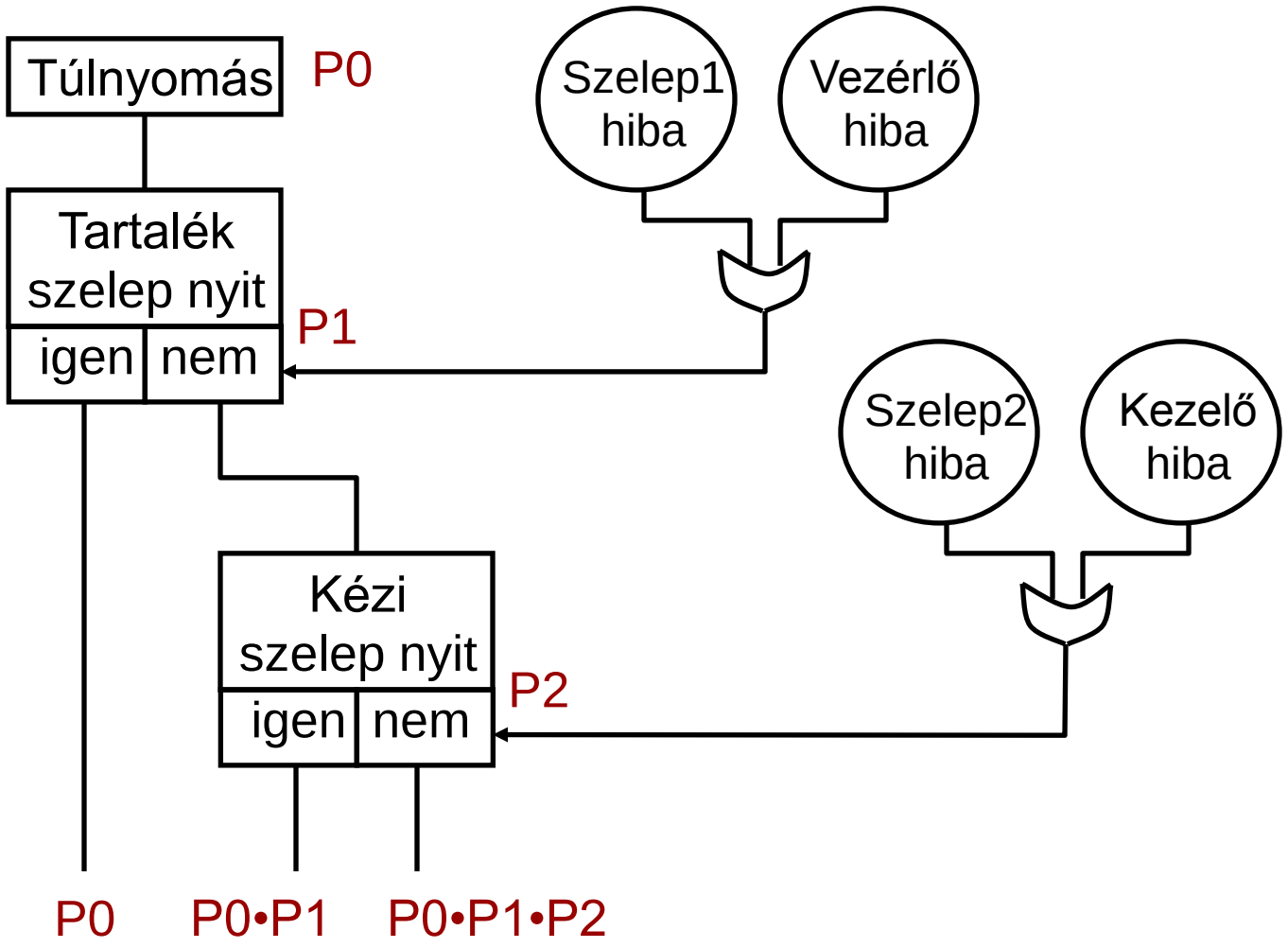


Ok-következmény analízis

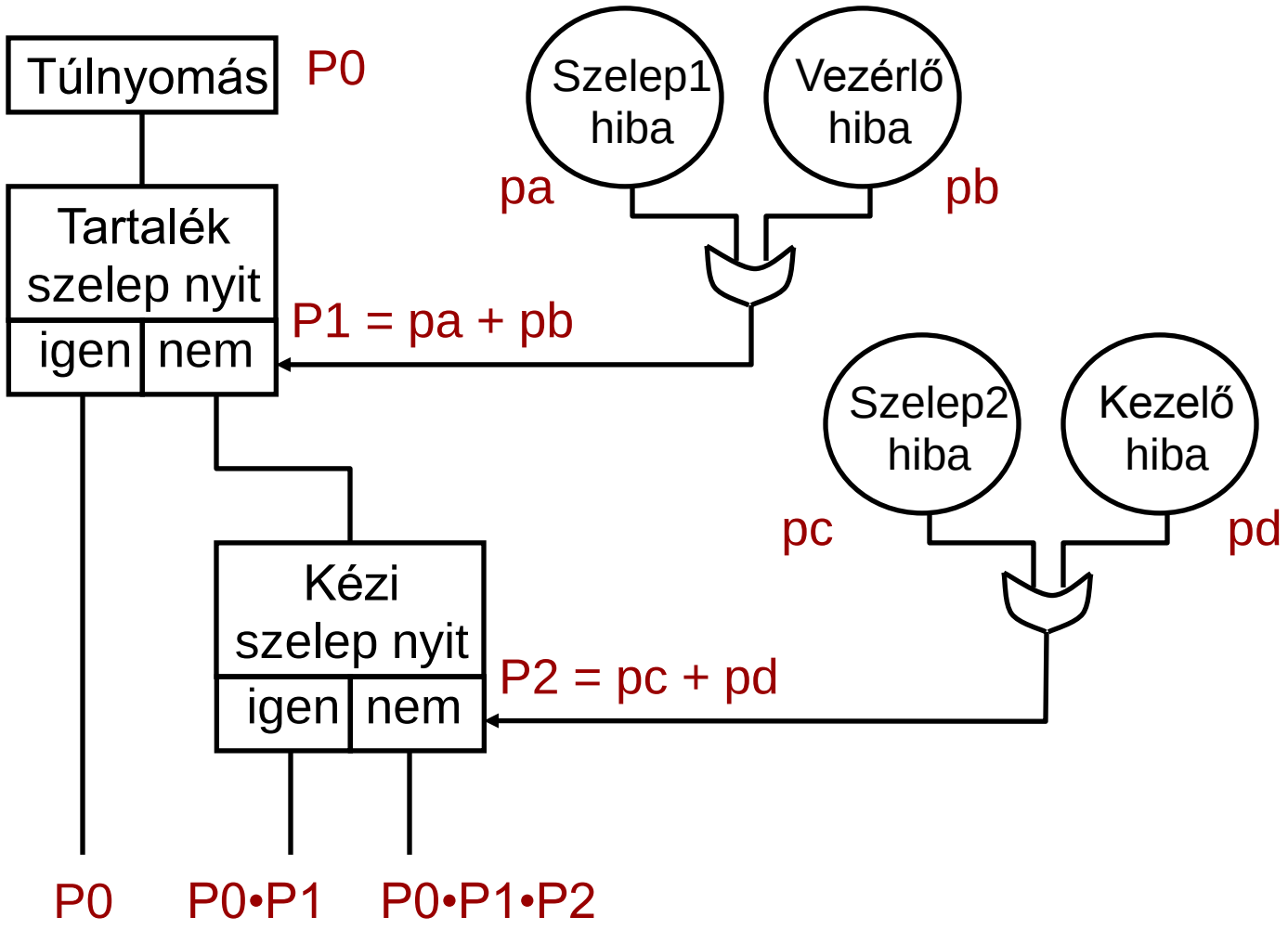
Ok-következmény diagram konstrukció

- Eseményfa és hibafa összekapcsolása
  - Eseményfa: Esemény forgatókönyvek (szekvenciák)
  - Csatolt hibafák: Adott események bekövetkezési okainak analízise
- Előnyök:
  - Szekvenciák (előrelépő analízis) és ok-okozati kapcsolatok (hátralépő analízis) együtt
- Hátrányok:
  - Minden kiváltó eseményhez külön diagram szükséges
  - Komplex diagramok

Példa ok-következmény analízisre



Példa ok-következmény analízisre



Hibamód és hatás analízis

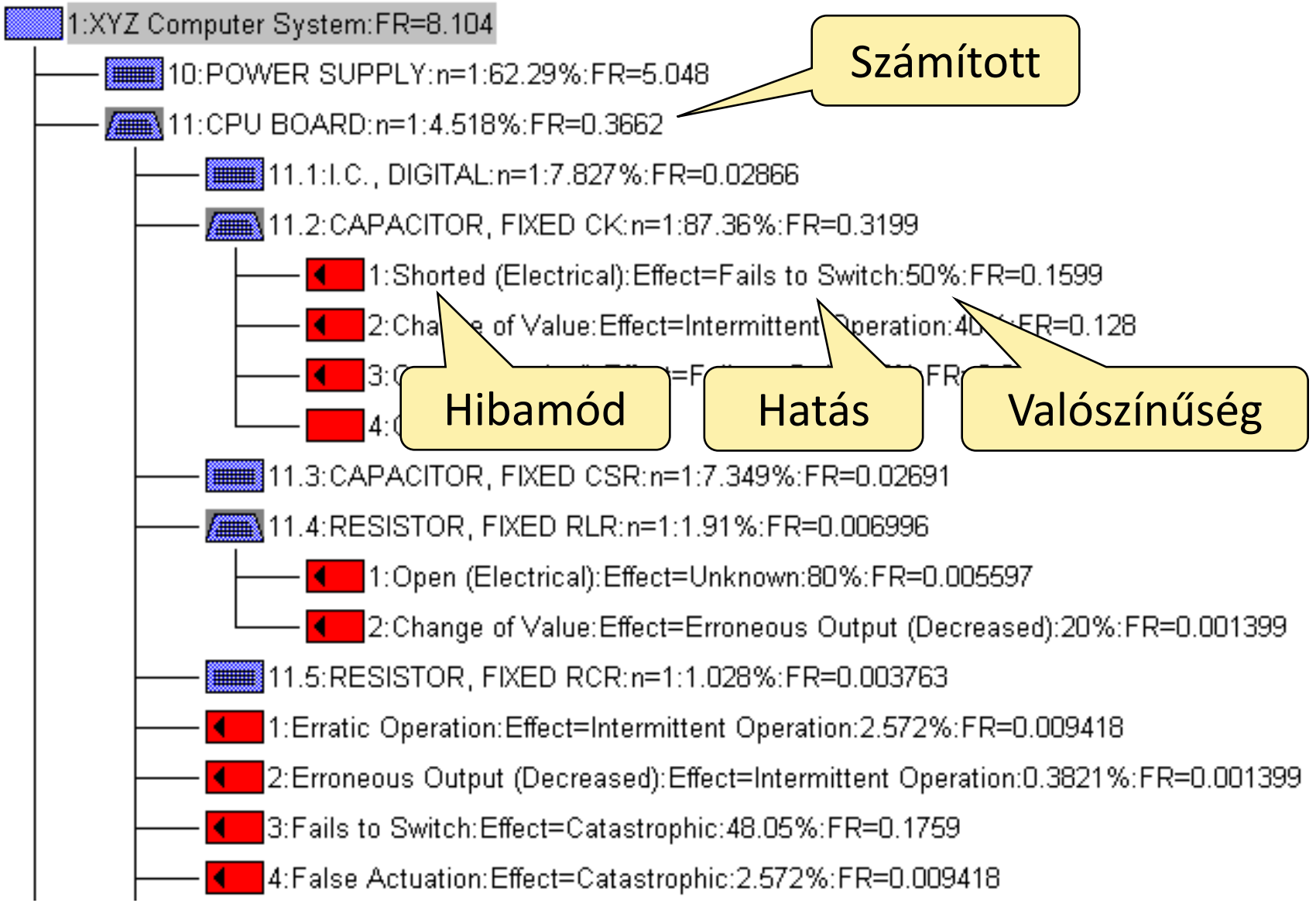
Item and (% chance of failure)	Failure mode		Effect of failure mode		Criticality of effect by severity type x 10^6			
	Description	Chance	Description	Chance	V.Hi	High	Med	Low
Main stack (0.2%)	Corruption	15%	Data loss	24%	180			
			System crash	66%		495		
	Overflow	60%	Shutdown	90%			2700	
			System crash	10%		300		
	Underflow	25%	Warning	98%				1225
Total					180	795	2700	1225

Hibamód és hatás analízis (FMEA) táblázat

- Hibák és hatásaik szisztematikus áttekintése
- Előnyök:
  - Rendszerkomponensek ismert hibáinak teljes vizsgálata
  - Redundancia felismerése

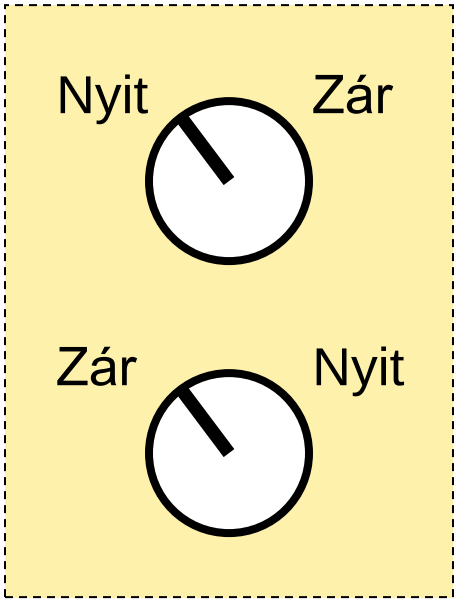
Komponens	**Hibamód**	**Valószínűség**	**Hatás**
D1 dióda	szakadás rövidzár	65% 35%	- túlnyomás - technológiai hiba
...	...	...	...

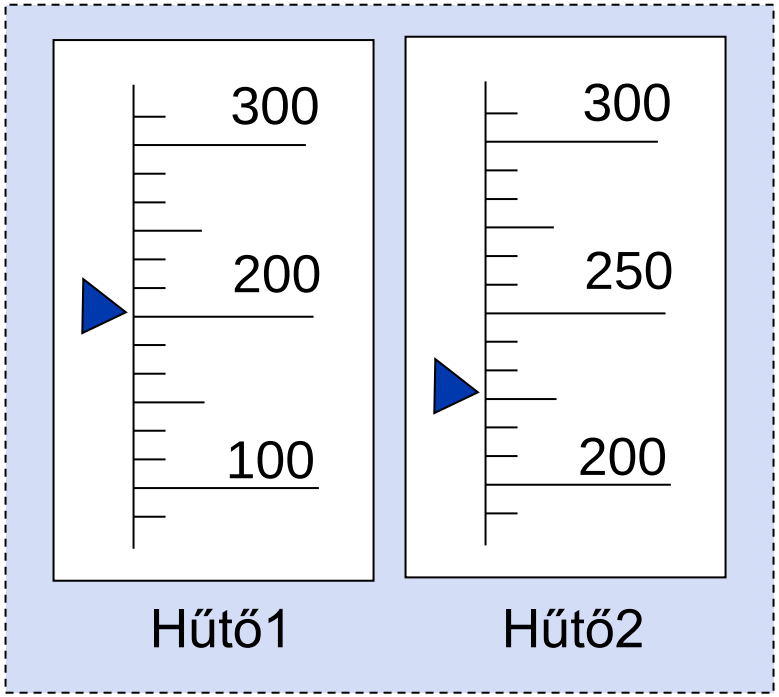
Példa: Vezérlő elektronika



Emberi hibák analízise

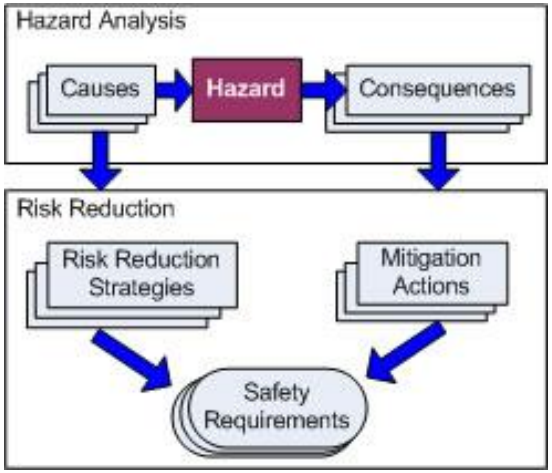
- Kvalitatív módszerek:
  - Művelet – veszély – hatások – okok – elkerülés
  - Fizikai és mentális elvárások elemzése
  - Hibalehetőségek ← pl. kezelői felület problémái





Kockázati mátrix és kockázatcsökkentés

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High



Veszély katalógus

- Veszély analízis alapján a veszélyek besorolása (pl. MIL-STD-822b, NASA szabványok):
  - Veszély szint:
    katasztrofális, kritikus, mérsékelt, elhanyagolható
  - Veszély időtartam/gyakoriság:
    gyakori, valószínű, esetenkénti, ritka, valószínűtlen, lehetetlen
- Veszély katalógus formája:
  - Kockázati mátrix
  - Védelmi szint bejelölése: A kezelendő kockázatok

Kockázati mátrix és védelmi szint

- Védelmi szint: Kezelendő kockázatok

Veszély szint /gyakoriság	Elhanyagol-ható	Mérsékelt	Kritikus	Katasztrofális
Gyakori	P2 szelep beragad	.	.	.
Valószínű	.	Pumpa beragad	P3 szelep beragad	J1 jelfogó zárva beragad
Esetenkénti	Motor nem indul	.	.	.
Ritka	.	Tartály ereszt	.	D3 dióda szakadása
Valószínűt-len	Cső repedése	.	R1 szakadt	D3 dióda rövidzára
Lehetetlen	.	.	.	.

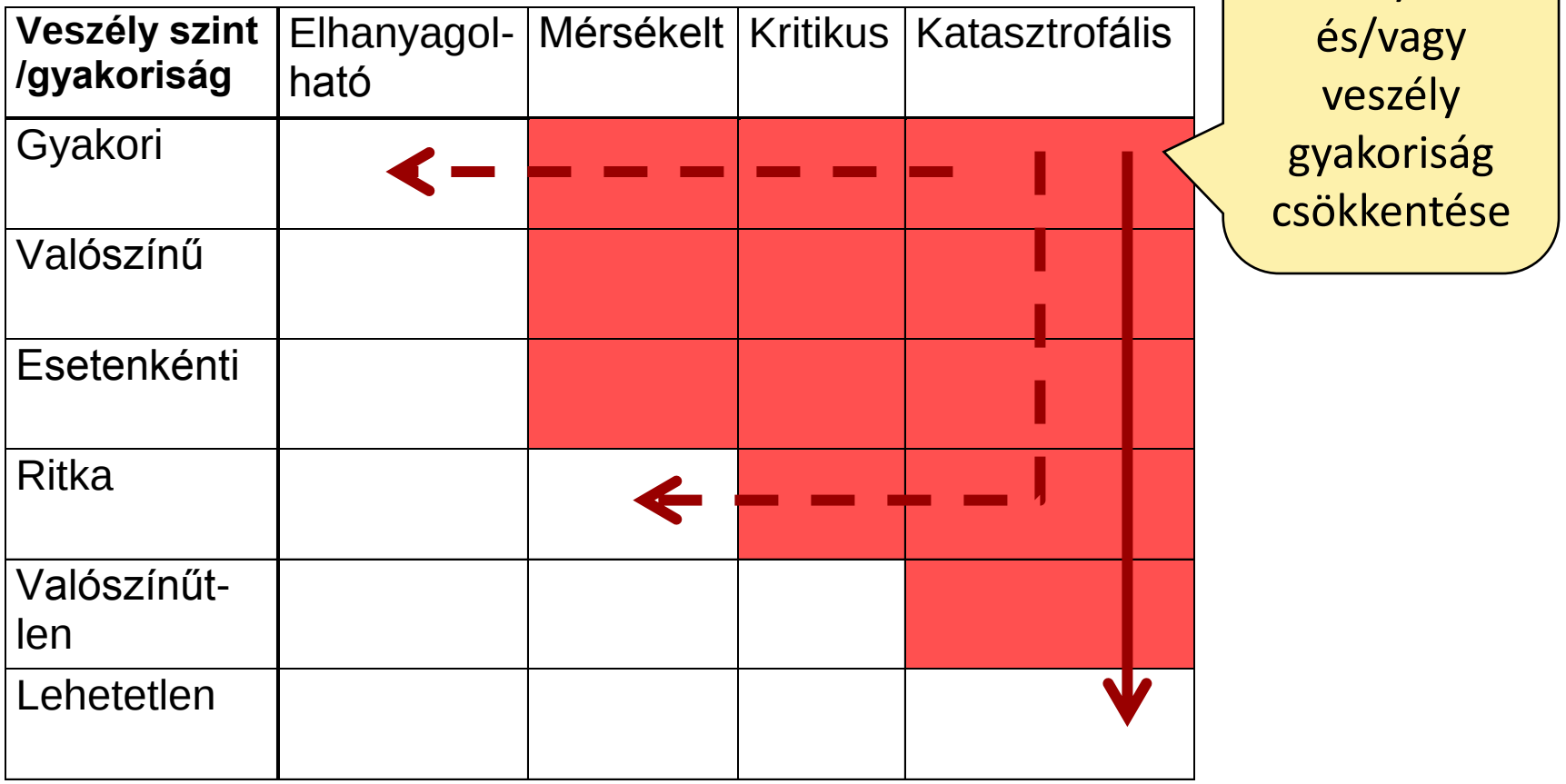
Piros tartomány: Kockázat-csökkentés szükséges

Kockázati mátrix példa (vasúti alkalmazások)

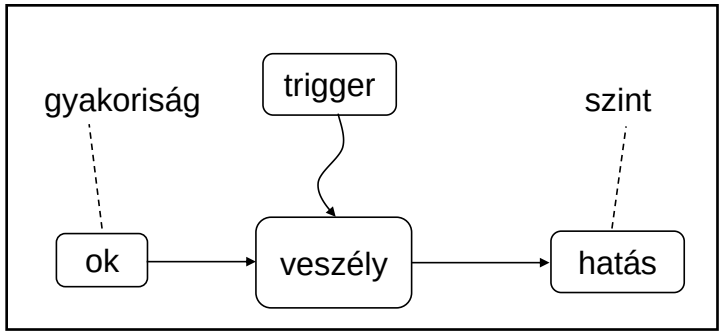
	Frequency of Occurrence of a Hazardous Event	RISK LEVELS			
Daily to monthly	**FREQUENT (FRE)**	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)	Intolerable (INT)
Monthly to yearly	**PROBABLE (PRO)**	Tolerable (TOL)	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)
Between once a year and once per 10 years	**OCCASIONAL (OCC)**	Tolerable (TOL)	Undesirable (UND)	Undesirable (UND)	Intolerable (INT)
Between once per 10 years and once per 100 years	**REMOTE (REM)**	Negligible (NEG)	Tolerable (TOL)	Undesirable (UND)	Undesirable (UND)
Less than once per 100 years	**IMPROBABLE (IMP)**	Negligible (NEG)	Negligible (NEG)	Tolerable (TOL)	Tolerable (TOL)
	INCREDIBLE (INC)	Negligible (NEG)	Negligible (NEG)	Negligible (NEG)	Negligible (NEG)
		INSIGNIFICANT (INS)	**MARGINAL (MAR)**	**CRITICAL (CRI)**	**CATASTROPHIC (CAT)**
		Severity Levels of Hazard Consequence			

Kockázati mátrix és védelmi szint

- Védelmi szint: Kezelendő kockázatok

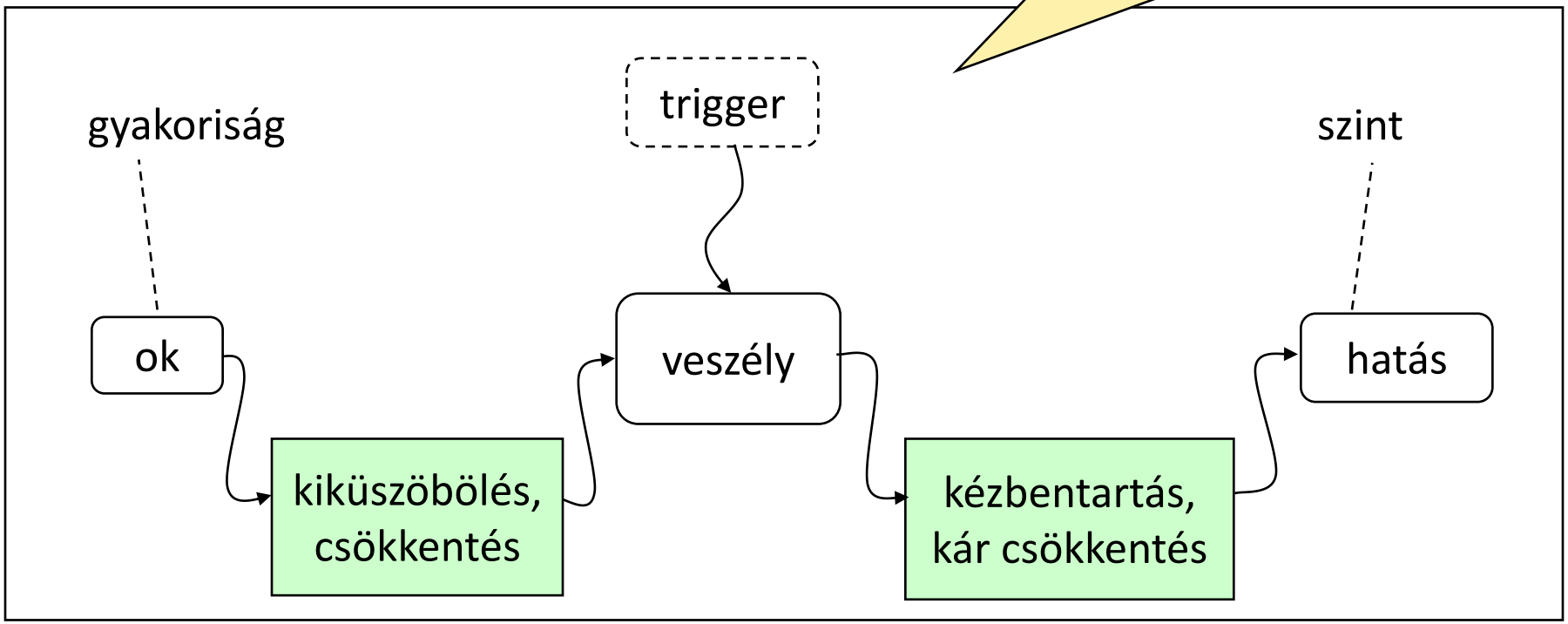


Kockázatcsökkentés alapelvei



Veszély okai és hatásai

Beavatkozási lehetőségek



Kockázatcsökkentés (áttekintés)

- Veszély kiküszöbölés: elkerülni a veszélyt
  - Helyettesítés: kevésbé veszélyes alkatrész, programnyelv
  - Egyszerűsítés: determinisztikus, statikus struktúra
  - Szétcsatolás: modularizálás, jogosultságok kezelése
- Veszély csökkentés:
  - Vezérelhetőség: inkrementális vezérlés, monitorozás
  - Határolók: kizárás (jogosultság), bezárás (bemenet vizsgálat), közrezárás (végrehajtási szekvencia vizsgálat)
  - Hiba minimalizálás: biztonsági tartomány
- Veszély kézbentartás:
  - Időtartam csökkentés, elszigetelés, védőrendszerek
- Kár csökkentés:
  - Menekülés, riadó tervek

Összefoglalás

- Veszély- és kockázati analízis
  - Ellenőrző listák (statikus analízis)
  - Hibafa
  - Eseményfa
  - Ok-következmény analízis
  - Hibamód és hatás analízis (FMEA)
- Kockázati mátrix
  - Védelmi szint
- Kockázatcsökkentési módszerek