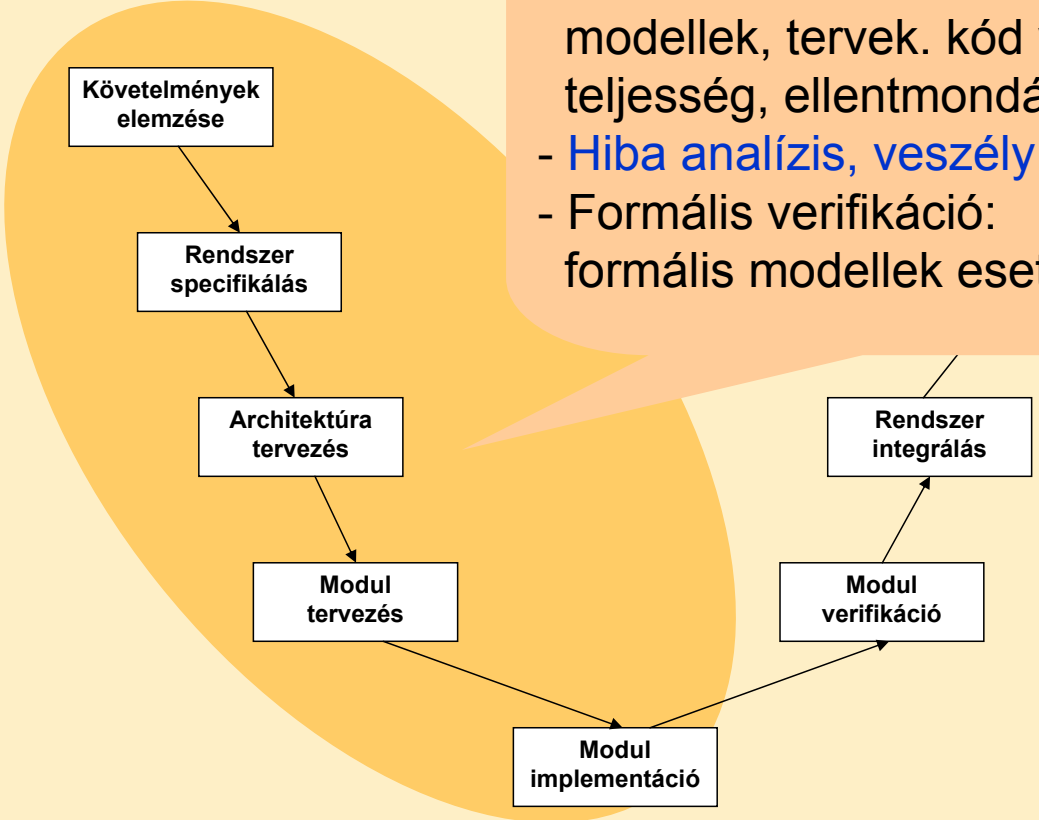
A szolgáltatásbiztonság kvalitatív analízise

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

Ellenőrzések a tervezési fázisban

- Statikus analízis:
  modellek, tervek. kód vizsgálata
  teljesség, ellentmondás-mentesség
- Hiba analízis, veszély analízis
- Formális verifikáció:
  formális modellek esetén



Hibahatások analízise

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

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. Állapot alapú analízis
8. Emberi hibák analízise

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

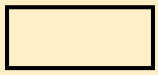
Rendszerszintű hibajelenség okainak vizsgálata

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

Hibafa konstrukció:

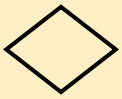
1. Rendszerszintű hibajelenség azonosítása:
   környezet, követelmények, szabványok
2. Közbenső események, pszeudo-események:
   hibajelenséghez vezetnek,
   alacsonyabb szintű események Boole-logikai kombinációi
   (AND, OR)
3. Elsődleges (alapszintű) események:
   további felbontás nincs

Hibafa grafikus elemkészlet



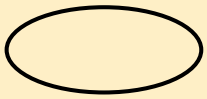
Legfelső szintű vagy közbenső esemény

Elsődleges (alapszintű) esemény



Tovább nem vizsgált esemény

Normál esemény (nem hiba vagy veszély)

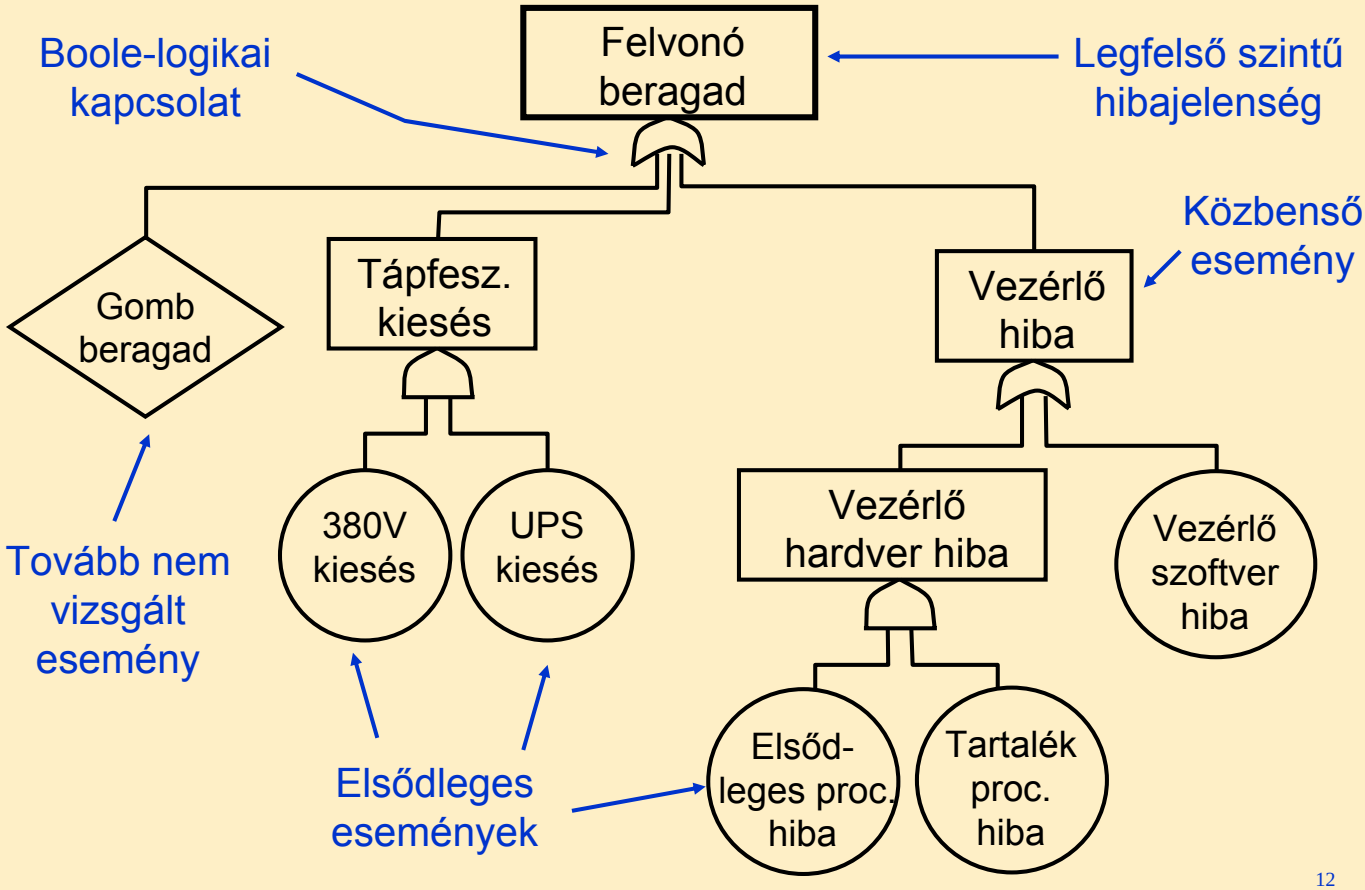


Feltétel egy összetett esemény bekövetkezéséhez

ÉS kapu

VAGY kapu

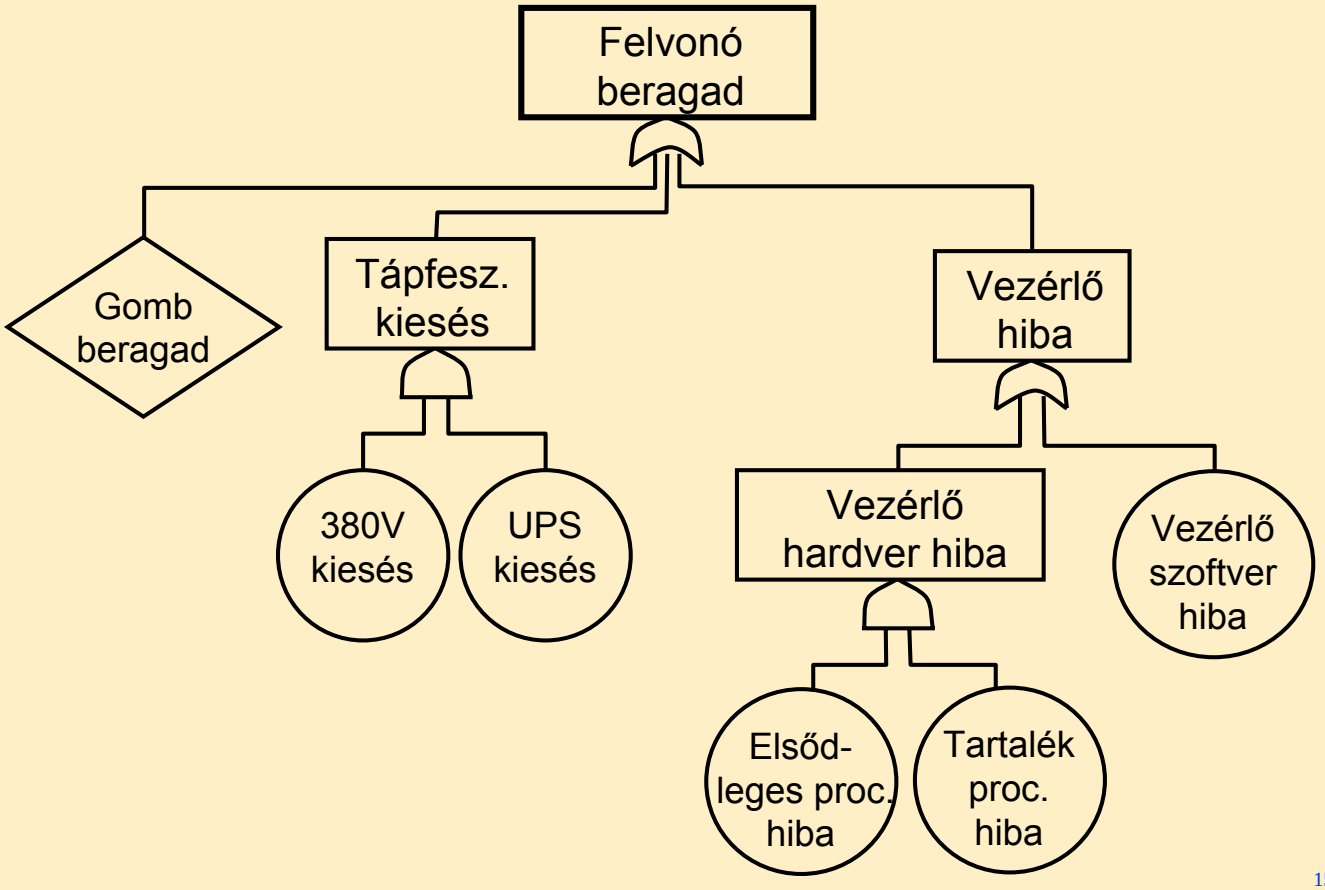
Hibafa példa: Felvonó



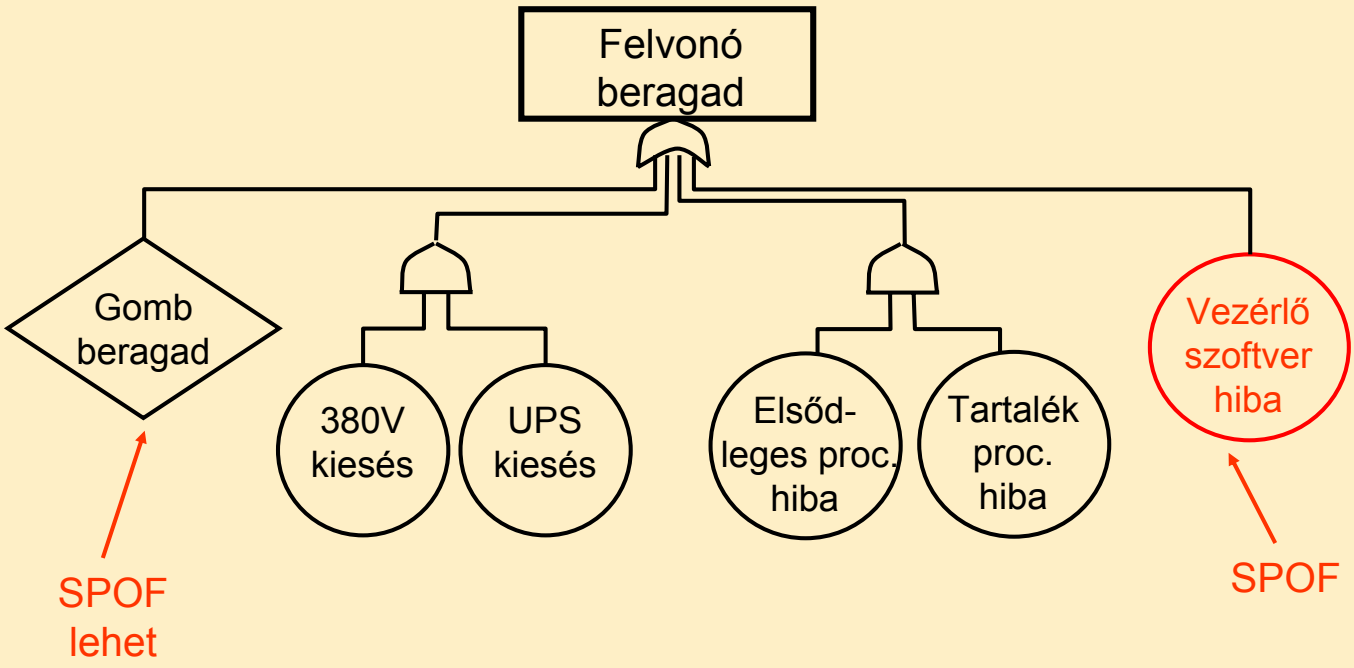
Minőségi (kvalitatív) analízis

- Hibafa redukció: Közbenső események és pszeudo-események feloldása
  → 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)

Hibafa példa: Felvonó



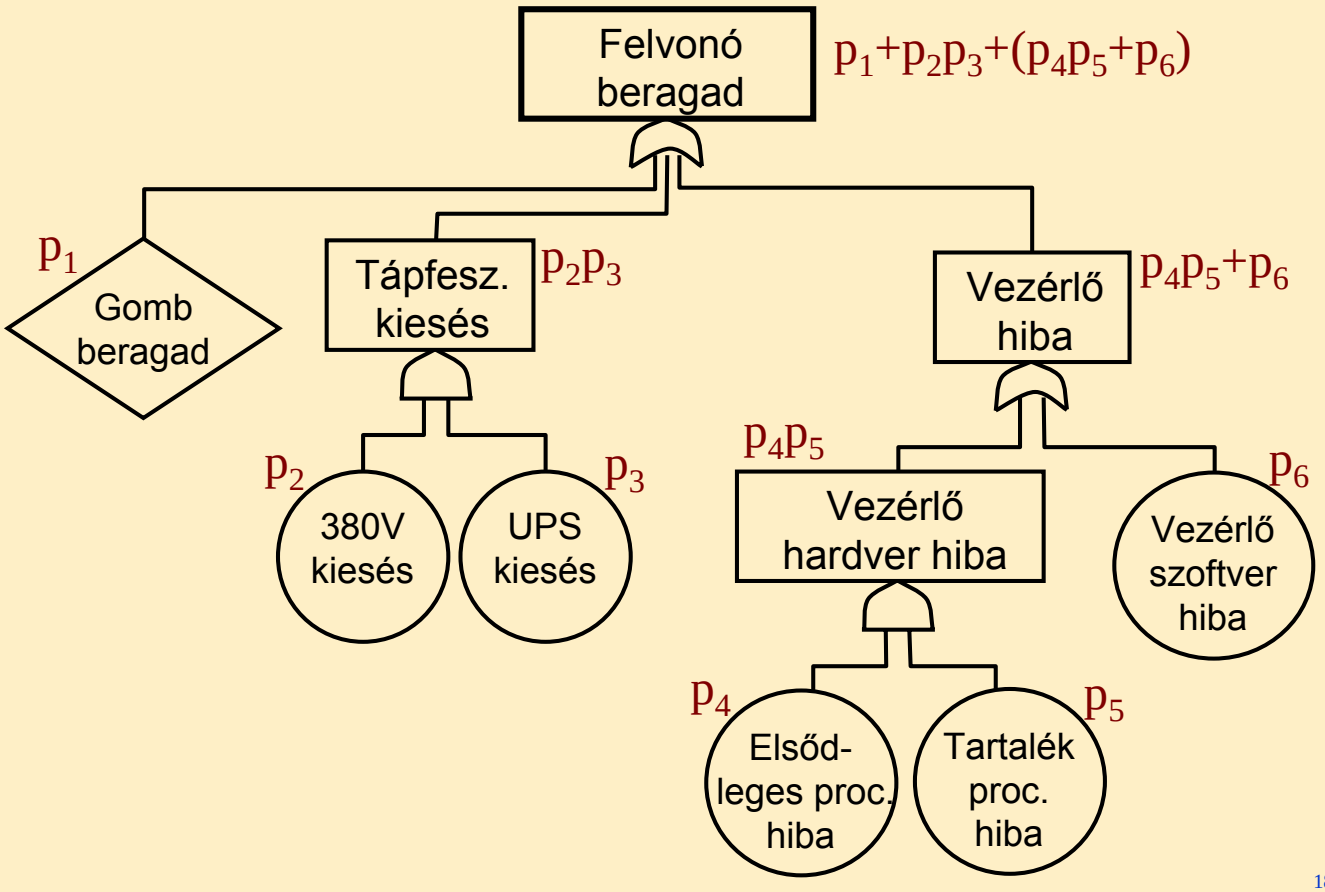
Redukált hibafa példa: Felvonó



Mennyiségi (kvantitatív) analízis

- Alapszintű eseményekhez rendelt valószínűségek
  - Komponens-adat, tapasztalat, becslés
- Rendszerszintű veszély valószínűség számítása
  - AND kapu: szorzat (ha független események)
    - Pontos: $P\{A \wedge B\} = P\{A\}\, P\{B|A\}$
  - 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

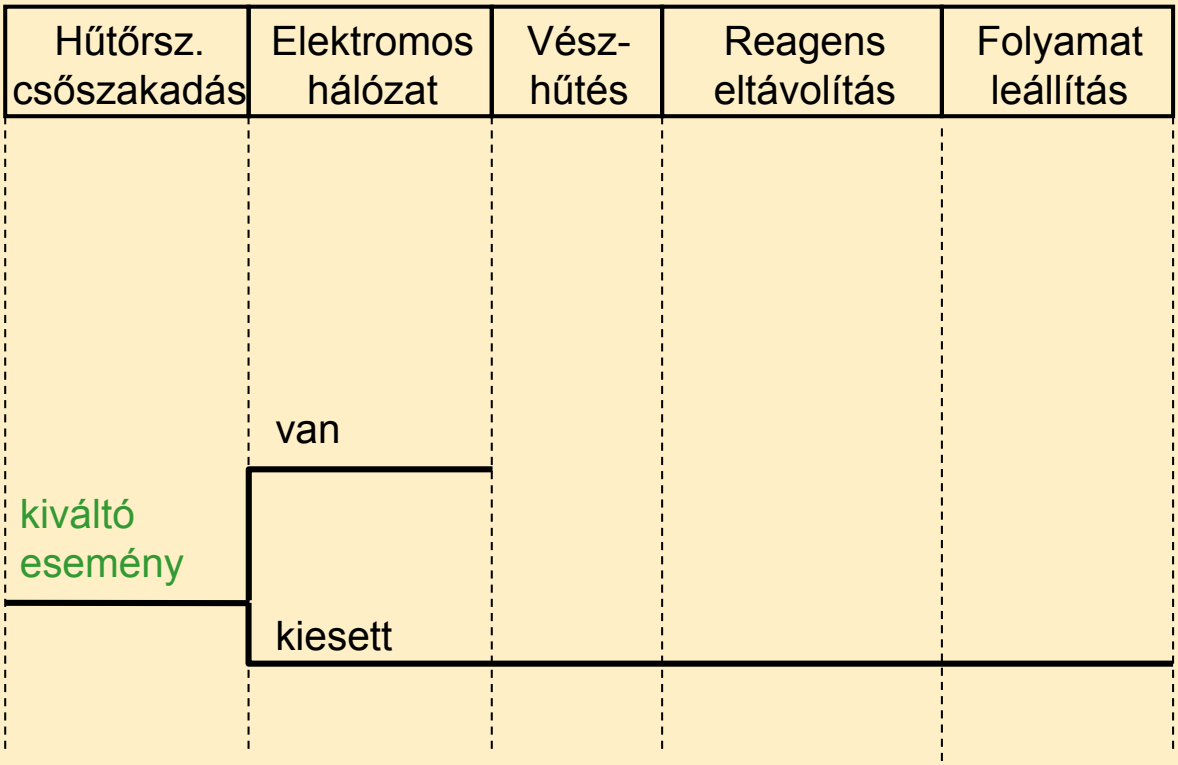
Hibafa példa: Felvonó



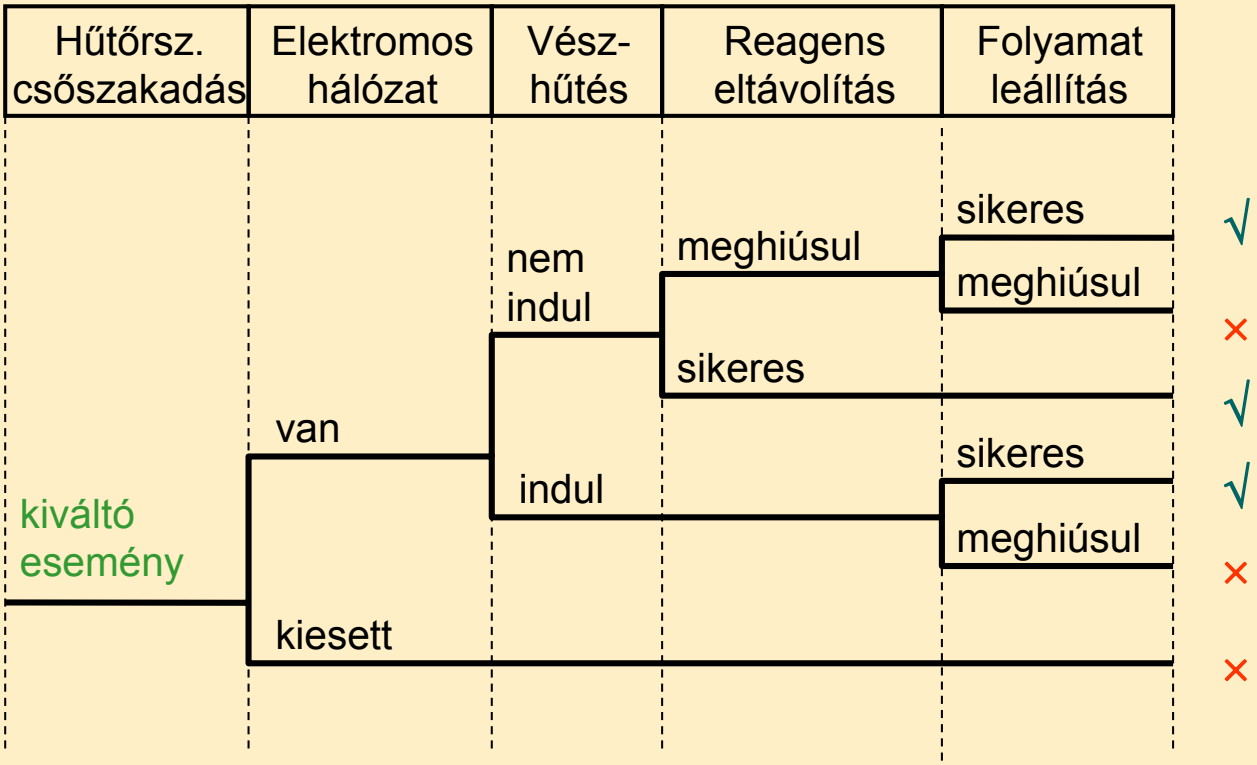
3. Eseményfa analízis

- 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

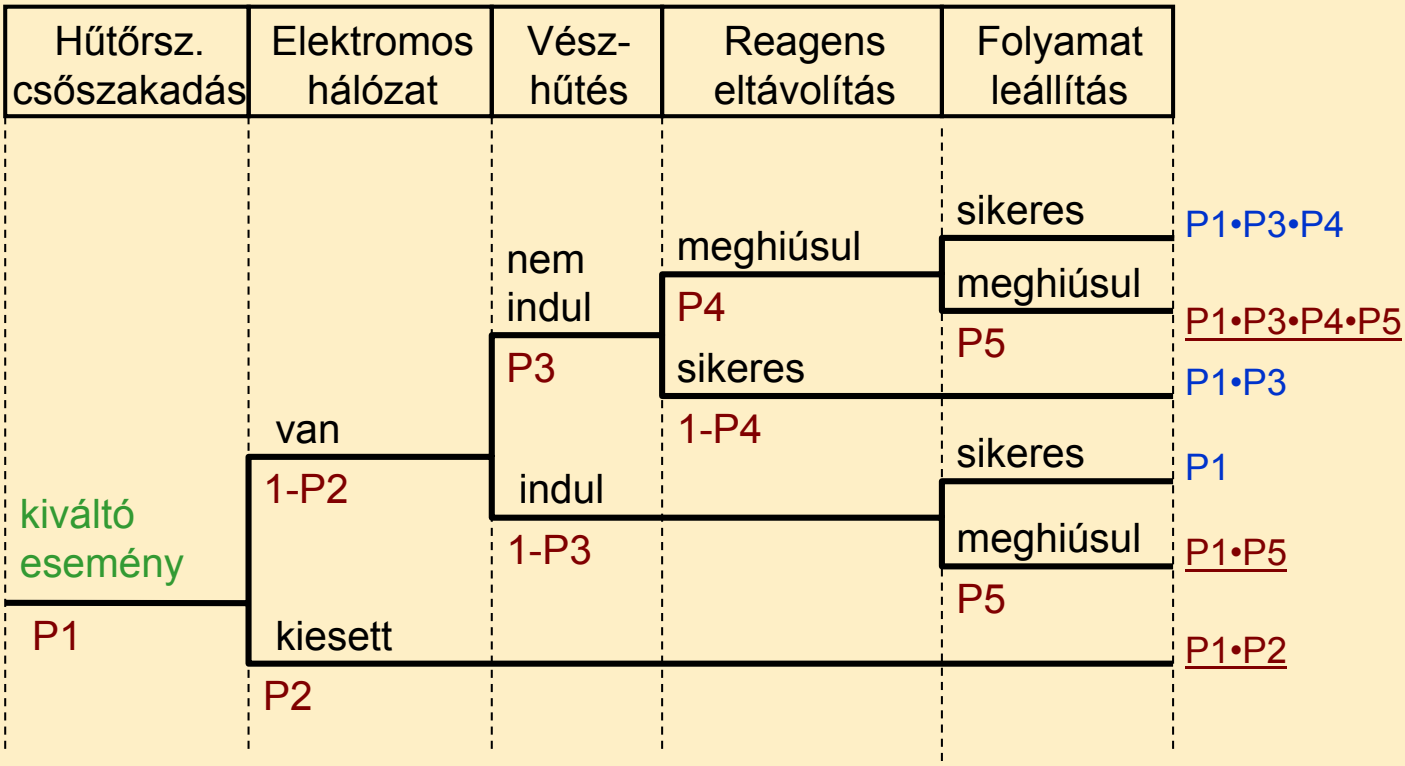
Eseményfa példa: Reaktorhűtés



Eseményfa példa: Reaktorhűtés



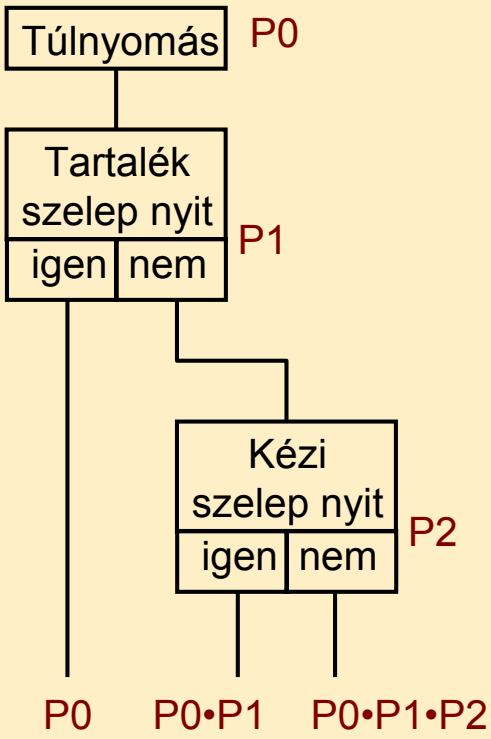
Eseményfa példa: Reaktorhűtés



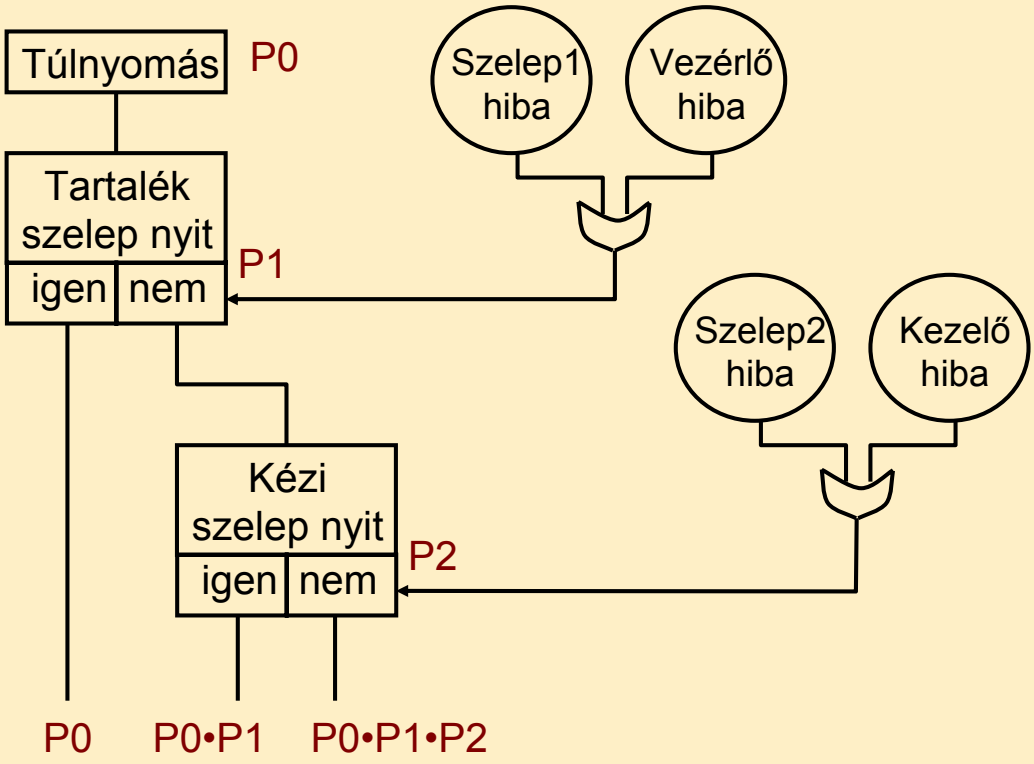
4. Ok-következmény analízis

- 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

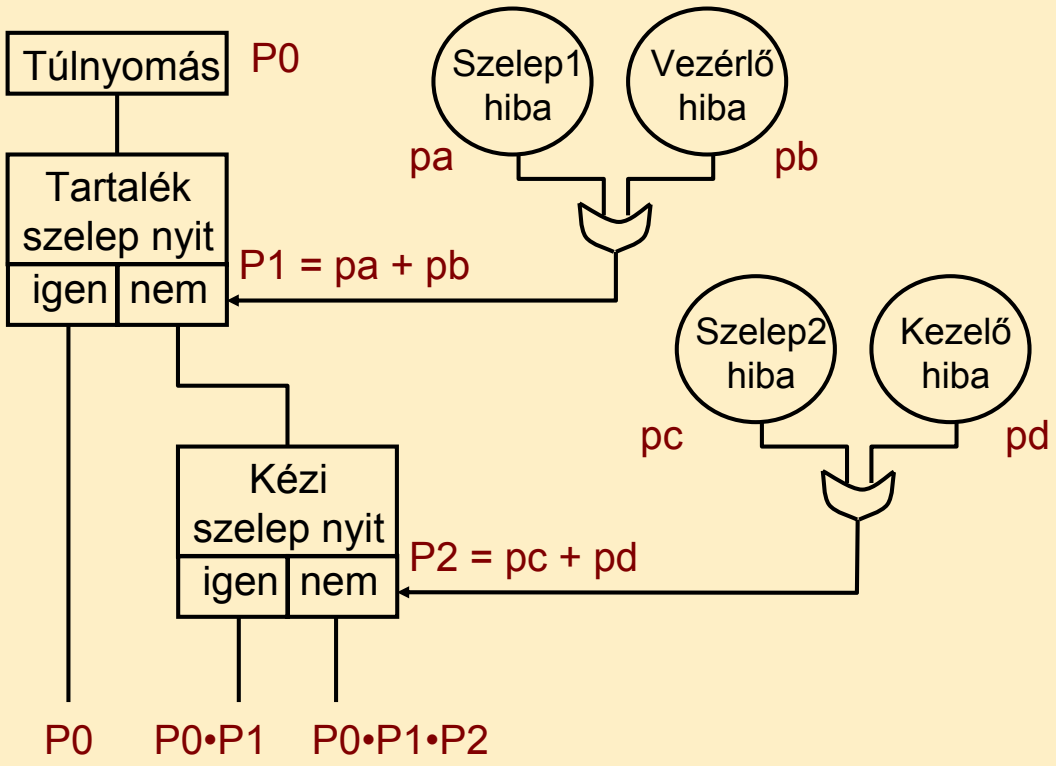
Példa ok-következmény analízisre



Példa ok-következmény analízisre



Példa ok-következmény analízisre



5. Veszély és működőképesség analízis

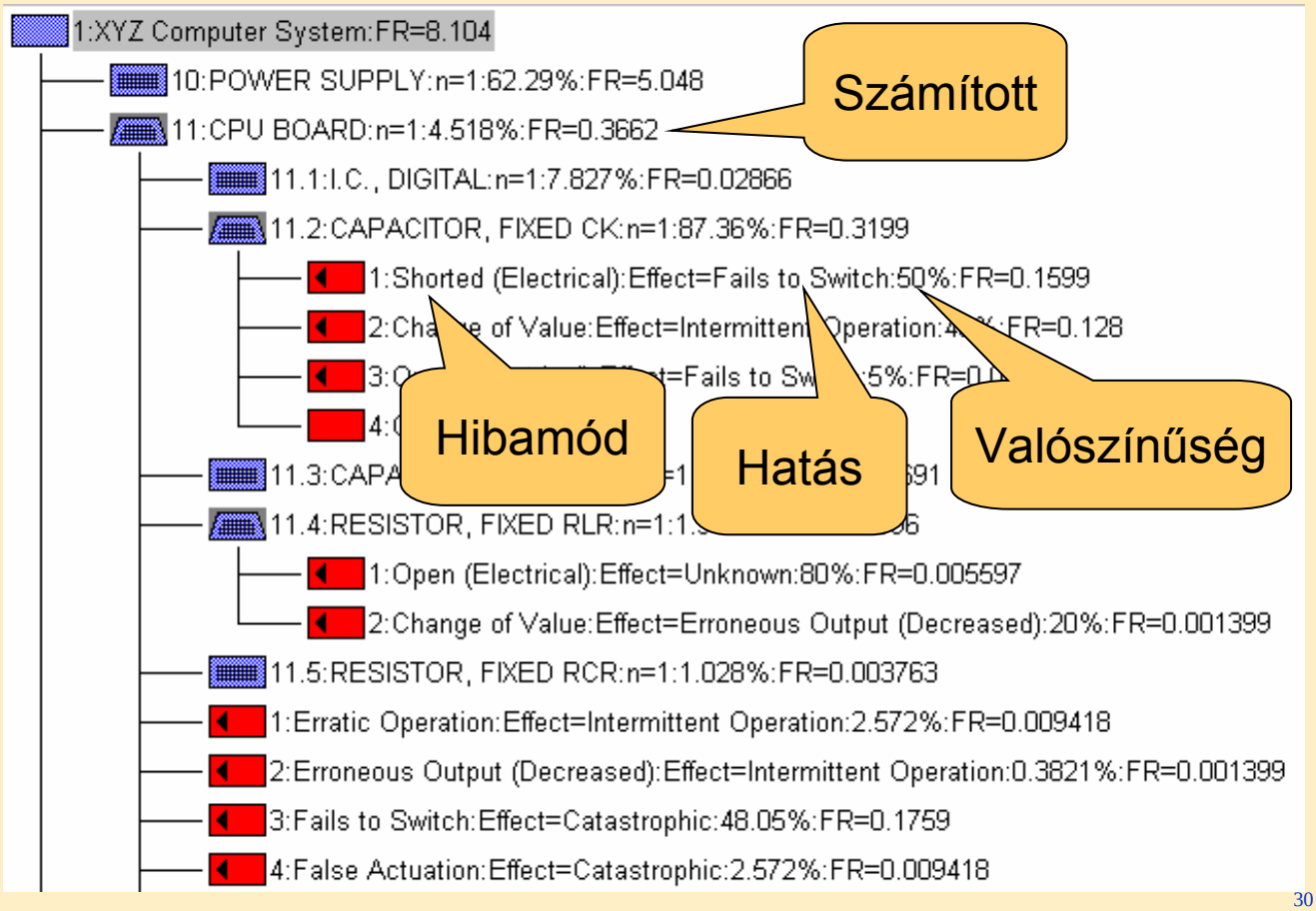
- HAZOP: Hazard and operability analysis
- Elterjedés: Vegyipari folyamatok
  - A tervezettől eltérő anyagáramlás okozza a hibát
  - Hibaszótár használata:
    NO, MORE, LESS, AS WELL AS, PART OF, REVERSE, …
- Informatikai folyamatok:
  - Információáramlásra alkalmazható hibaszótár
  - Lehetséges eltérések 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
…	…	…	…

Példa: Vezérlő elektronika

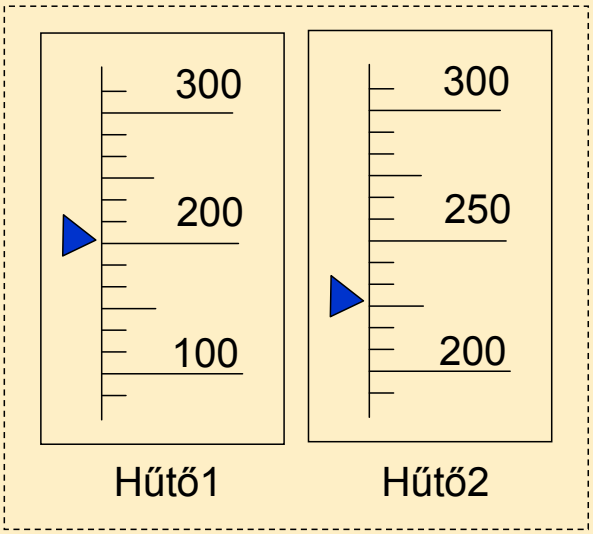


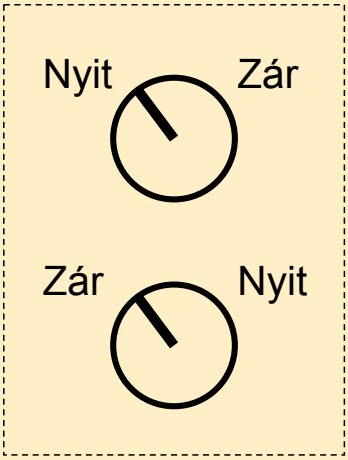
7. Állapot alapú analízis

- 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!

8. Emberi hibák analízise

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





Veszély analízis biztonságkritikus rendszerekben

Specifikus terminológia

- Baleset (*accident*):
  Nemkívánatos, be nem tervezett veszteség, sérülés
- Veszély (*hazard*), veszélyes állapot:
  Olyan állapot, amely adott környezeti feltételek mellett balesethez vezet
- Kockázat (*risk*):
  Veszély következmény szintje + gyakorisága
- Biztonság(osság) (*safety*):
  Balesetektől való mentesség (ideális)
  → Elfogadhatatlan kockázattól való mentesség
- Biztonságkritikus számítógépes rendszer (szoftver):
  Veszélyes állapotokkal kapcsolatba hozható a rendszer (szoftver) hibamentes / hibás / hiányzó végrehajtása

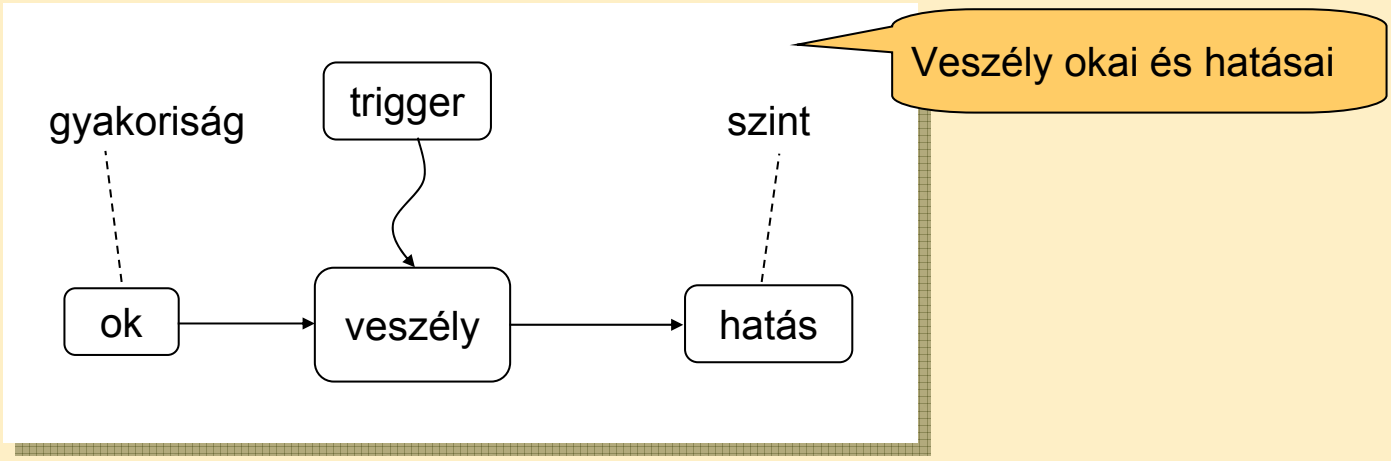
Veszély és meghibásodás

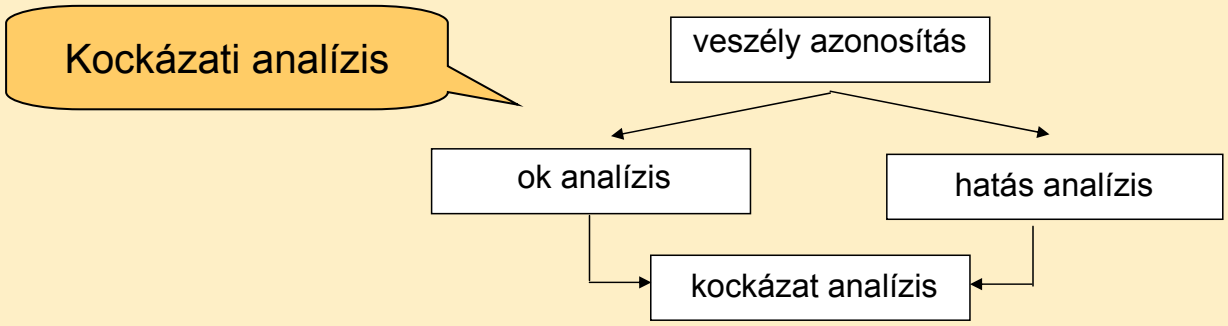
- Balesetek jellegzetességei
  - Kialakulás: Tipikusan a tervezési fázisban előre nem látott eseményszekvencia
- Veszély és meghibásodás nem azonos
  - Előfordulhat veszély hibátlan működés esetén is
  - A detektálatlan hiba tipikusan veszélyt jelent
- Biztonság a rendszer egészének tulajdonsága
  - Tervezési folyamat során kell figyelembe venni
  - Folyamatos analízis a fontos:
    új alkalmazások, technológiák, új környezet

Veszély analízis - analógia

Módszerek	Eredmények	Beavatkozás
- Ellenőrző lista - Hibafa - Eseményfa - Ok-következmény analízis	Hiba analízis: - Hibalehetőségek - Hibaterjedés - Tesztelhetőség	Hibákra: - Hiba elkerülés - Hiba eltávolítás - Hibatűrés
- Veszély- és műveleti analízis - FMEA, FMECA - Állapot-alapú analízis	Veszély analízis: - Azonosítás - Okok - Hatások	Veszélyekre: - Kockázat-csökkentés

Veszély analízis





Kockázati mátrix és védelmi szint

- Veszély analízis alapján a veszélyek besorolása (pl. MIL-STD-822b, NASA szabványok):
  - Veszély szint: katasztrofális, kritikus, mérsékelt, elhanyagolható
  - Veszély gyakoriság: gyakori, valószínű, esetenkénti, ritka, valószínűtlen, lehetetlen

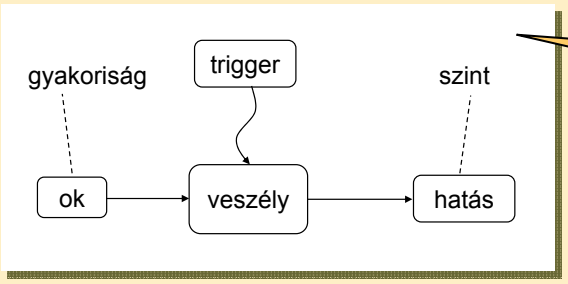
Veszély szint /gyakoriság	Elhanyagolható	Mérsékelt	Kritikus	Katasztrofális
Gyakori	.	.	.	.
Valószínű	.	.	.	.
Esetenkénti	.	.	.	.
Ritka	.	.	.	.
Valószínűt-len	.	.	.	.
Lehetetlen	.	.	.	.

Kockázat-csökkentés szükséges

Kockázati mátrix példa

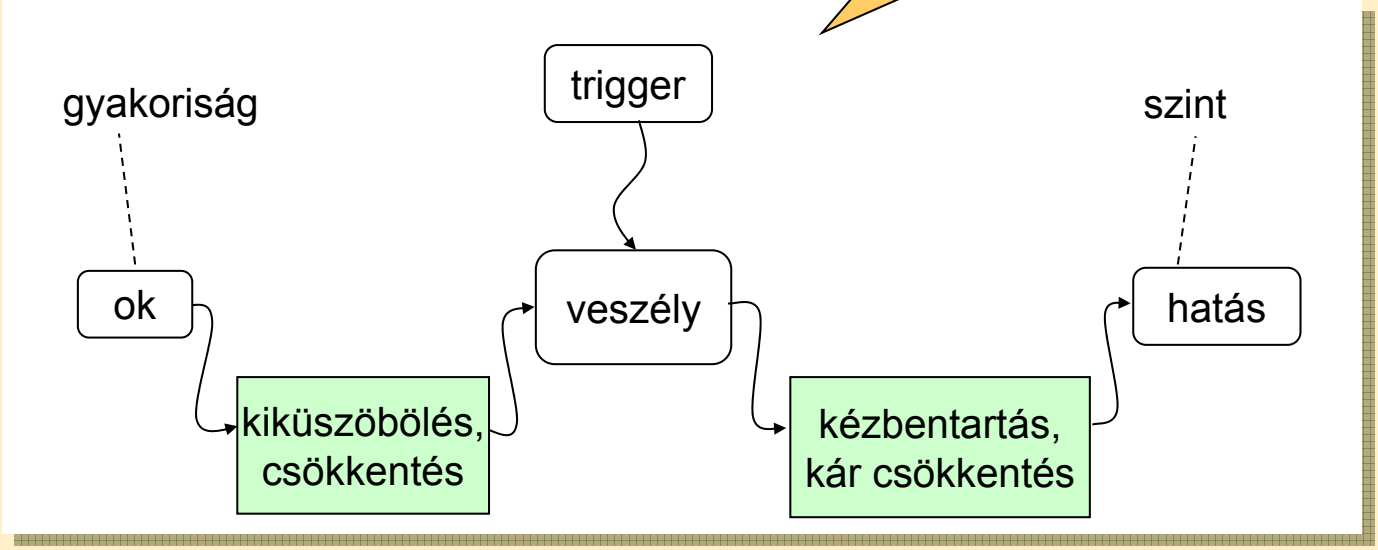
	Frequency of Occurrence of a Hazardous Event	RISK LEVELS			
Daily to monthly	**FREQUENT (FRE)**	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)	Intolerable (INT)
Monthly to yearly	**PROBABLE (PRO)**	Tolerable (TOL)	Undesirable (UND)	Intolerable (INT)	Intolerable (INT)
Between once a year and once 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			

Kockázatcsökkentés alapelvei



Veszély okai és hatásai

Beavatkozási lehetőségek



Kockázatcsökkentés

- 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

- Analízis technikák
  - Ellenőrző listák
  - Hibafa
  - Eseményfa
  - Ok-következmény analízis
  - Veszély és működőképesség analízis
  - Hibamód és hatás analízis (FMEA, FMECA)
  - Állapot alapú analízis
  - Emberi hibák analízise
- Veszély analízis biztonságkritikus rendszerekben
  - Analógia és különbségek
  - Kockázati mátrix
  - Kockázatcsökkentés