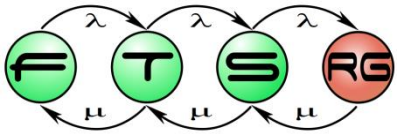
Informatikai rendszertervezés

Budapesti Műszaki és Gazdaságtudományi Egyetem
Hibatűrő Rendszerek Kutatócsoport



A tárgy kontextusa

Előzmények

- Rendszermodellezés

Rendszertervezés BSc specializáció

- Informatikai Rendszertervezés
- Ipari informatika

MSc szakirány

- Modell alapú rendszertervezés
- Szoftver- és rendszerellenőrzés
- Kiber-fizikai rendszerek

A tárgy előadói

- Előadók
  - Horváth Ákos
  - Majzik István
  - Micskei Zoltán
  - (Varró Dániel)
  - + meghívott előadók
- Gyakorlatok és segítők:
  - Búr Márton
  - Debreceni Csaba
  - Nagy András Szabolcs
  - Molnár Vince








Tárgykövetelmények

- Házi feladat: *“Kollaboratív tervezői munka”*
  - Rendszertervezési feladat 3 fős csapatoknak
  - 50%-al beleszámít a jegybe
  - További pluszpontok szerezhetők
- Kötelező részvétel gyakorlatokon
- Írásbeli vizsga

Tárgy struktúrája

- 2 hetes blokkok
  - 2 előadás
  - 1 gyakorlat
  - 1 tutorial
- Összesen 6 nagyobb blokk, minden blokk része a HF-nek
  - Követelmény analízis, komponens tervezés, biztonságra tervezés, viselkedés modellezése, architektúra tervezés és verifikáci/validáció
  - +1 Automatizálási technikák

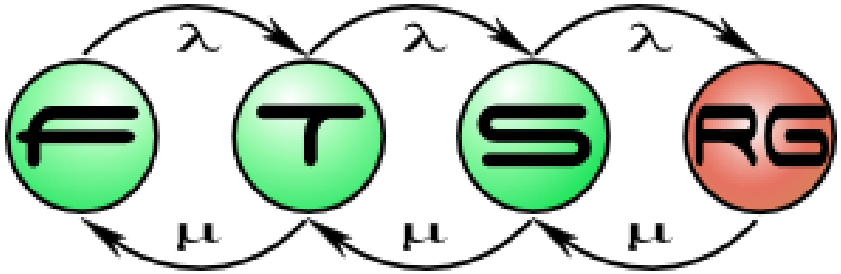
Határidők, fontosabb dátumok

- Házi feladat fontosabb dátumai
  - szerdáig álljanak össze a 3 fős csapatok
    - https://docs.google.com/forms/d/e/1FAIpQLScGe_I8e5owOoJZ_ih64e_15MkiDmU3jqcLDKL-Z0sJWY1gng/viewform
  - Kiadási és beadási dátumok
    - Minden beadáshoz 1 felelős csapatonként

HF1 kiadása 09.16-án	**HF3 kiadása** 10.12-én	**HF5 kiadása** 11.09-én
HF2 kiadása 09.28-án	**HF4 kiadása** 10.24-én	**HF6 kiadása** 11.23-án
HF1-2 beszedés 10.09-én 20:00	**HF3-4 beszedés** 11.06-án 20:00	**HF5-6 beszedés** 12.04-én 20:00

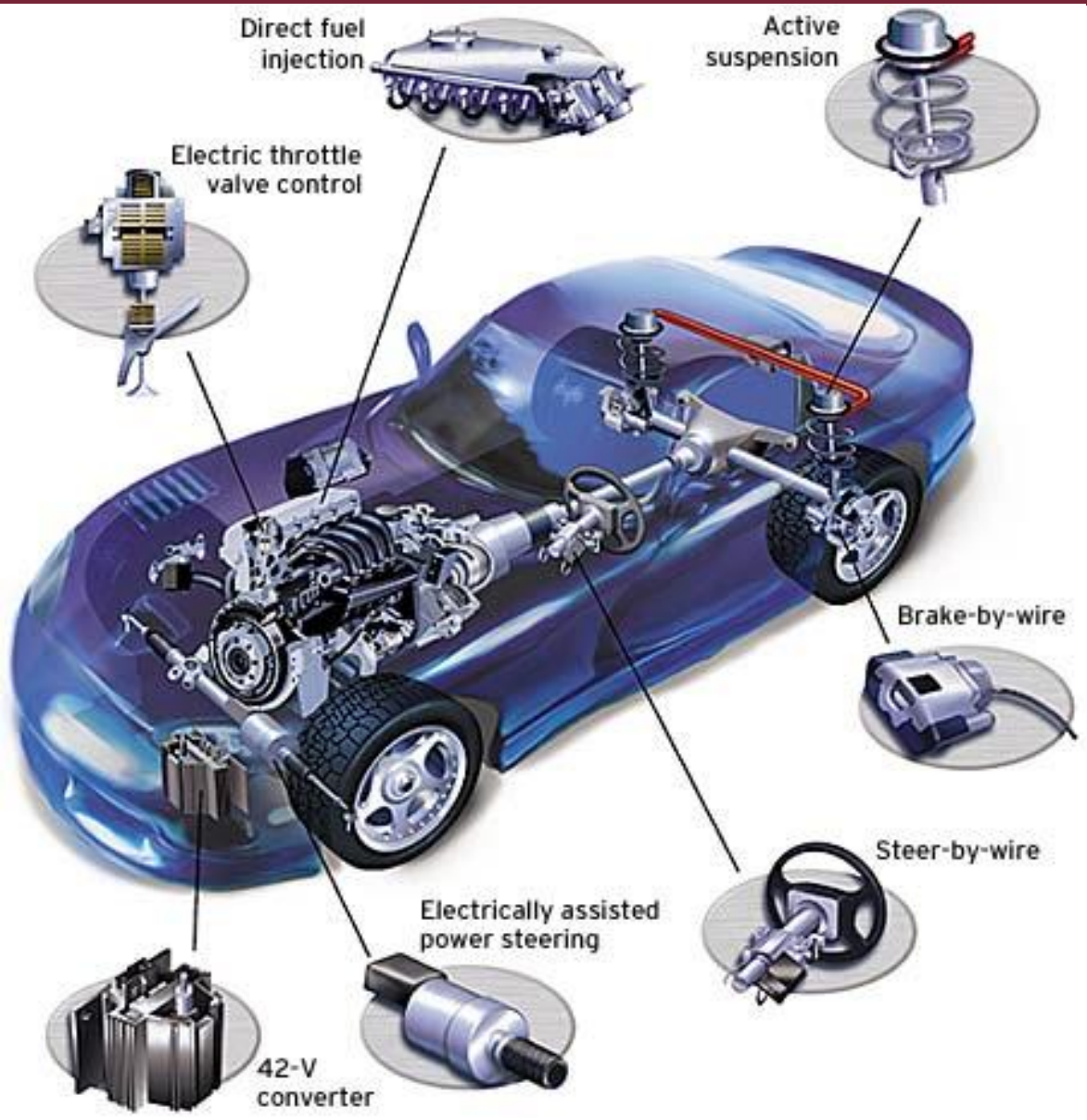
Összefoglaló

- Weboldal
  - Fóliák és kiadandó anyagok
    - http://inf.mit.bme.hu/edu/courses/rete
  - Kérdések
    - http://q2a.inf.mit.bme.hu/questions/rendszertervez%C3%A9s
- Órák:
  - Hétfő, QBF09., 12:15-14:00
  - Szerda, QBF09. 8:15-10:00
  - Kérem mindenki időben jelenjen meg!



MOTIVÁCIÓ

Egy mai modern autóban…



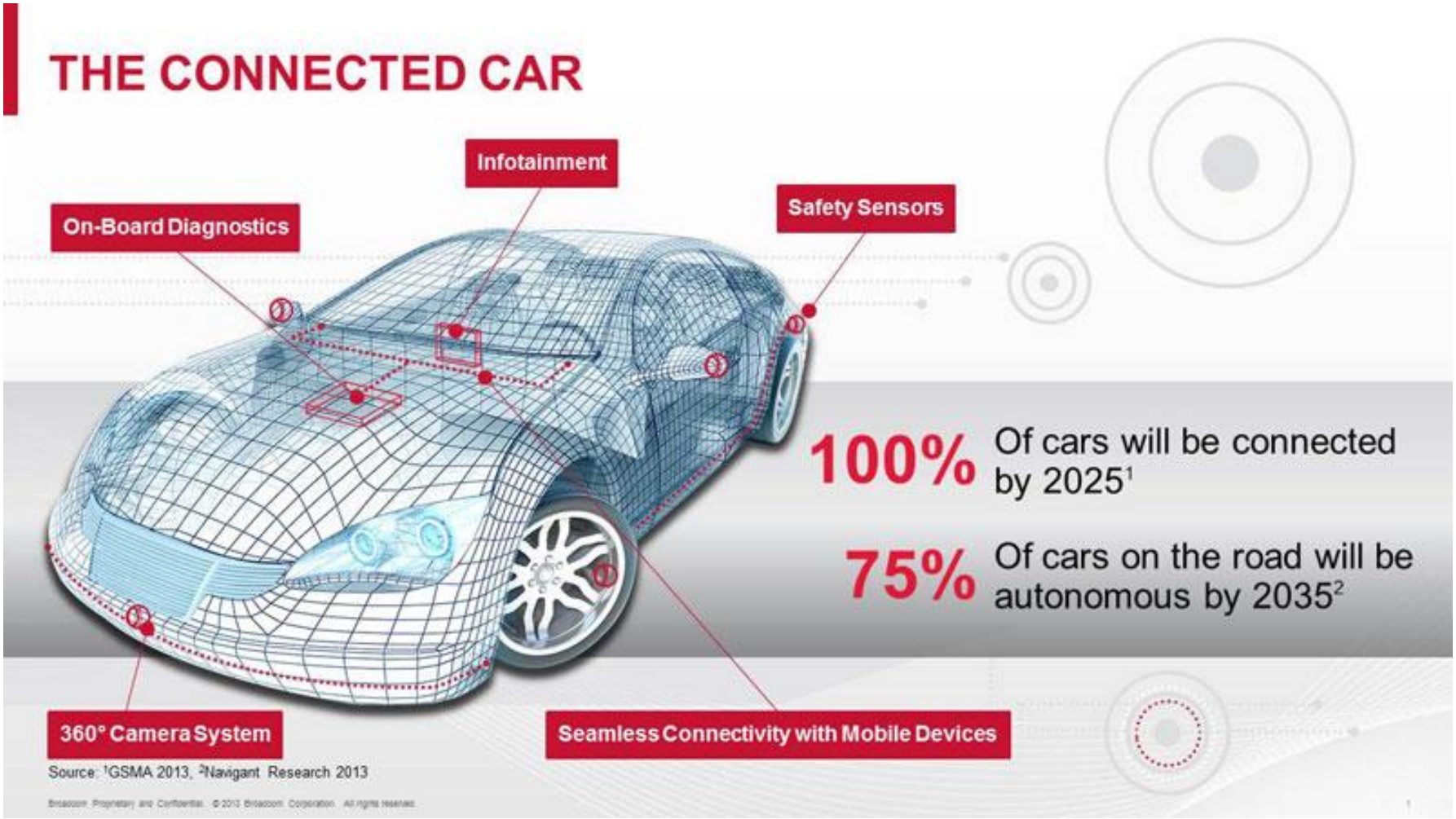
Drive-by-wire: Nincs mechanikus kapcsolat

- Kormánykerék ⇔ kormányzott kerék
- Fékpedál ⇔ fékbetétek
- Gázpedál ⇔ motor

Van viszont helyette

- 50-100 vezérlőegység (ECU)
- 5-7 busz
- 100 millió sornyi forráskód
- 17 millió autó/év (EUR)

… és a jövő autójában



Kiber-fizikai rendszerek

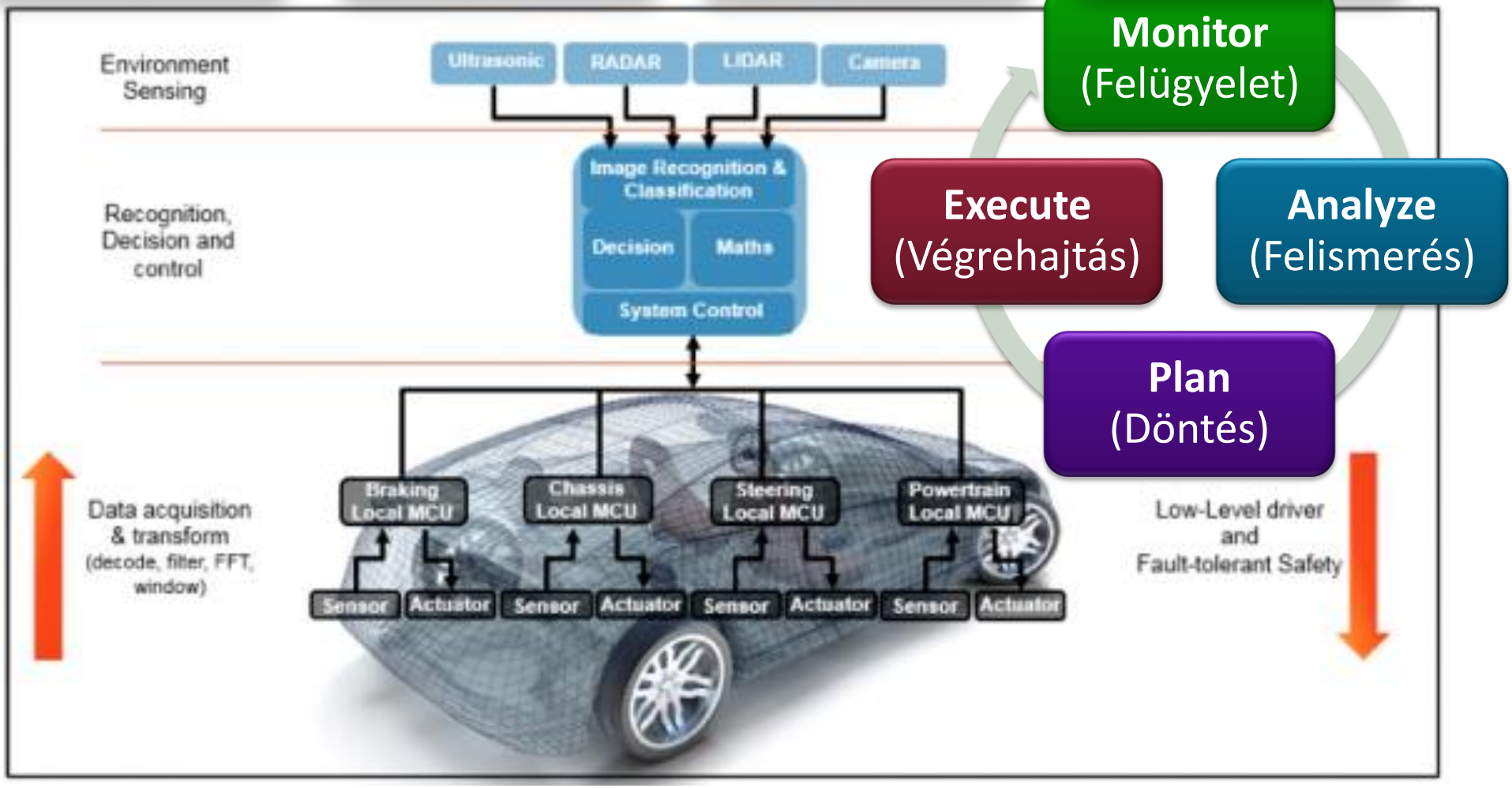
… és a jövő autójában

Változó fizikai környezet

Hálózatba kapcsolt

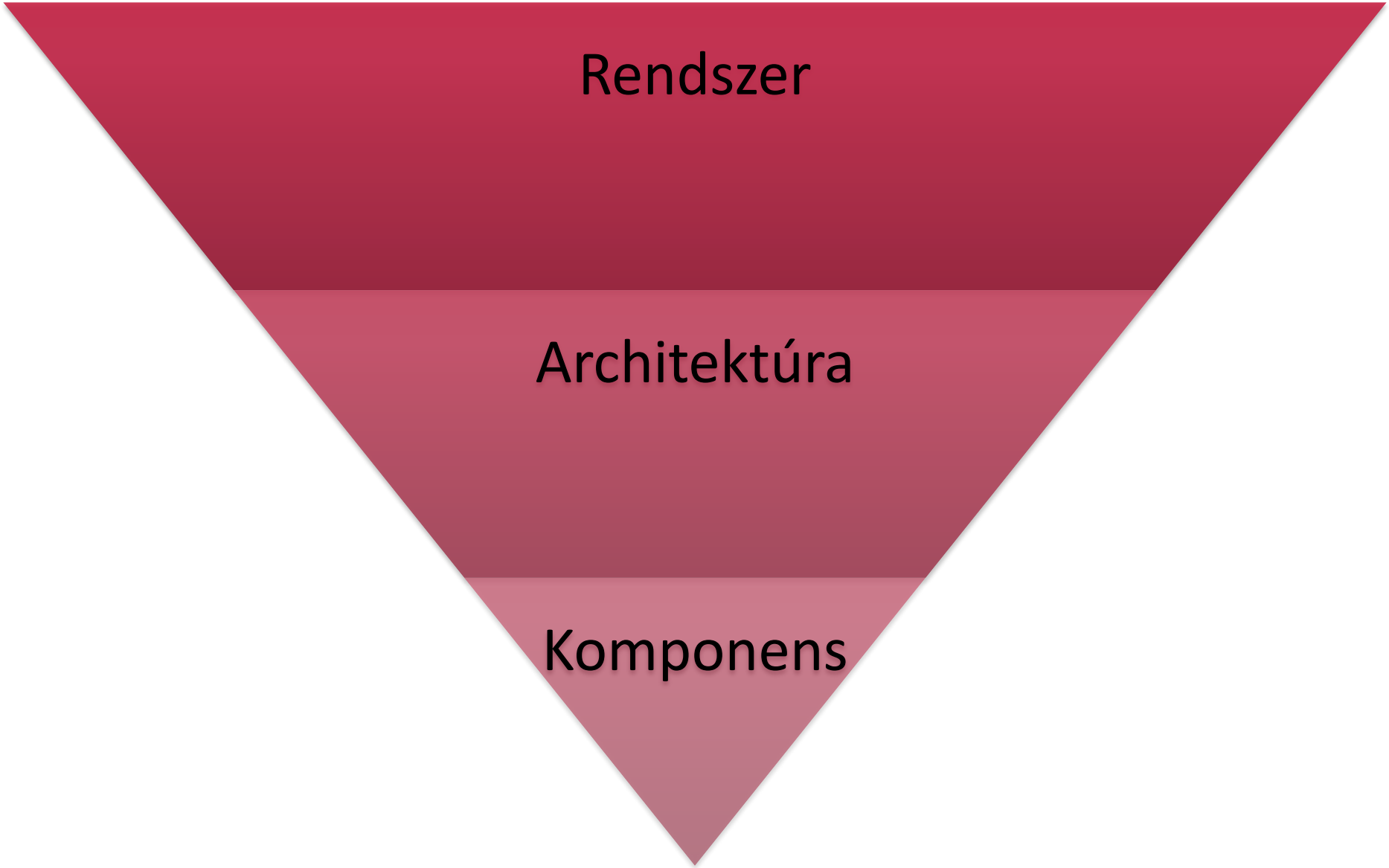
Dinamikus nyílt rendszer

Biztonságos működés?

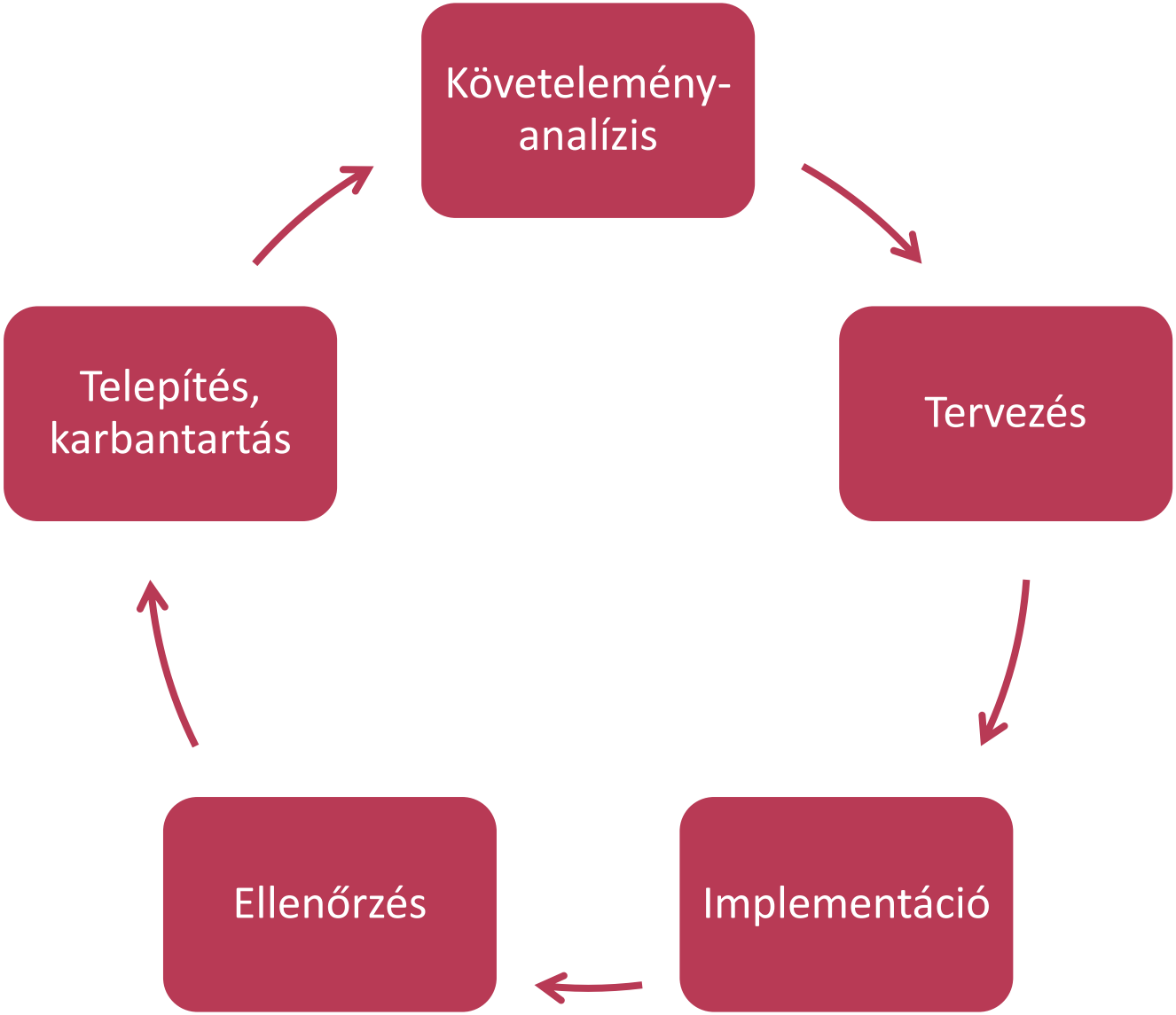


MODELLEK A RENDSZERTERVEZÉSBEN

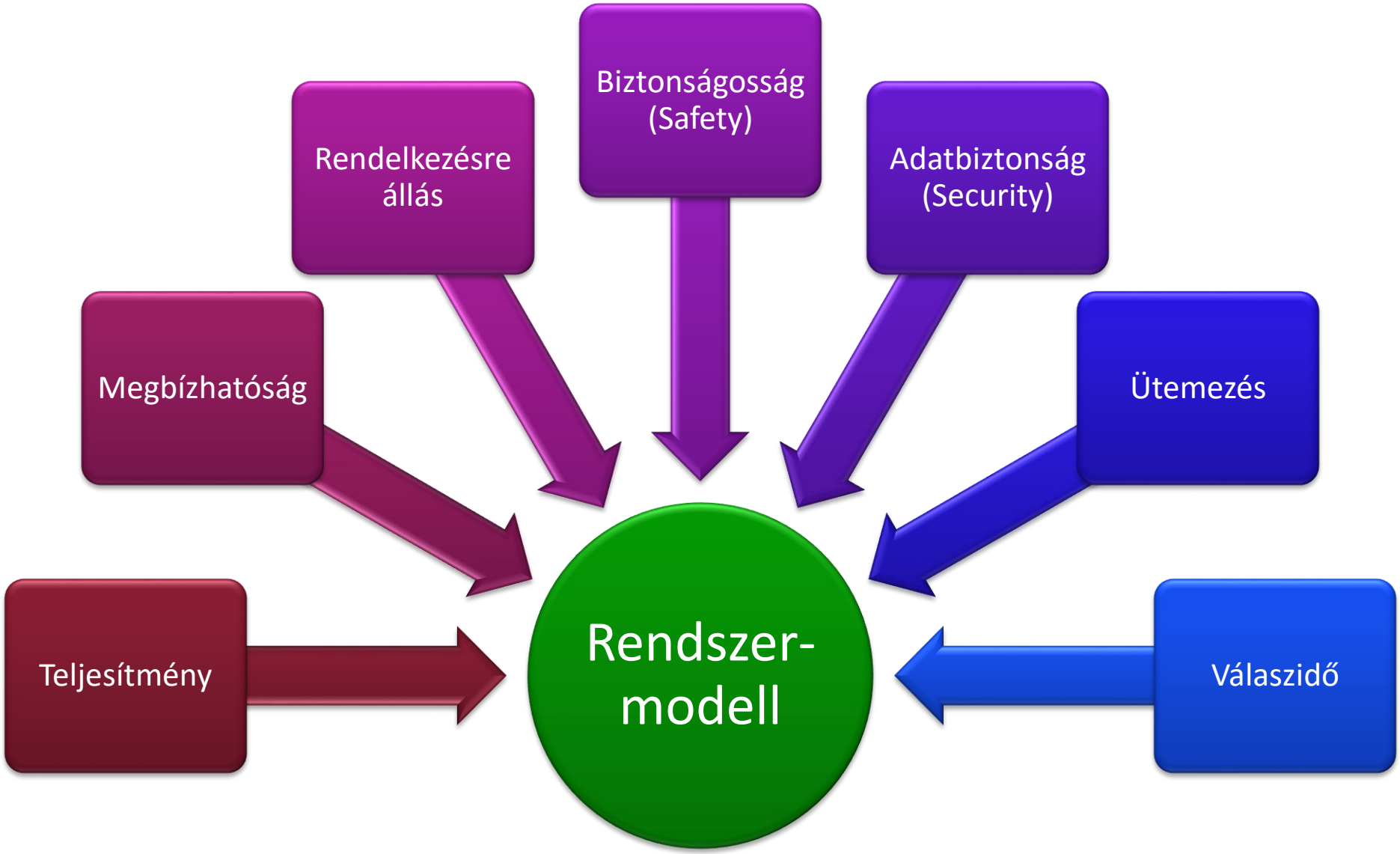
Különböző absztrakciós szinteken…



Különböző tervezési fázisokban…



Többféle nézőpontból…

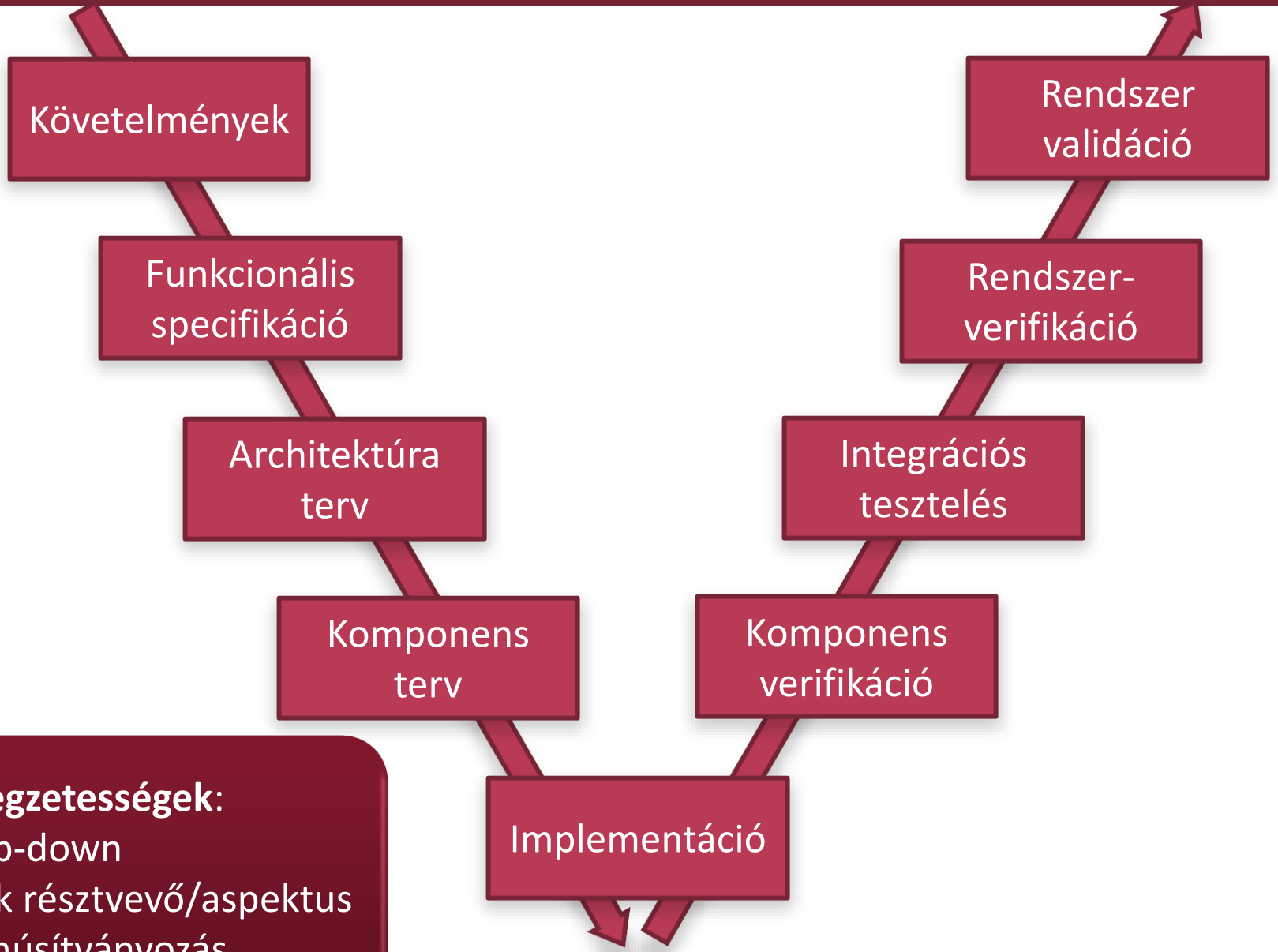


Többféle célból…

Statikus modellezés	Dinamikus modellezés	Tervezési folyamat	Tervezésitér-bejárás, Optimalizáció
Architektúra-tervezés	Platform-modellezés	Allokáció, Telepítés	Tesztelés, V&V
Szimuláció	Kódgenerálás	Dokumentáció-generálás	Fizikai és mérnöki modellek

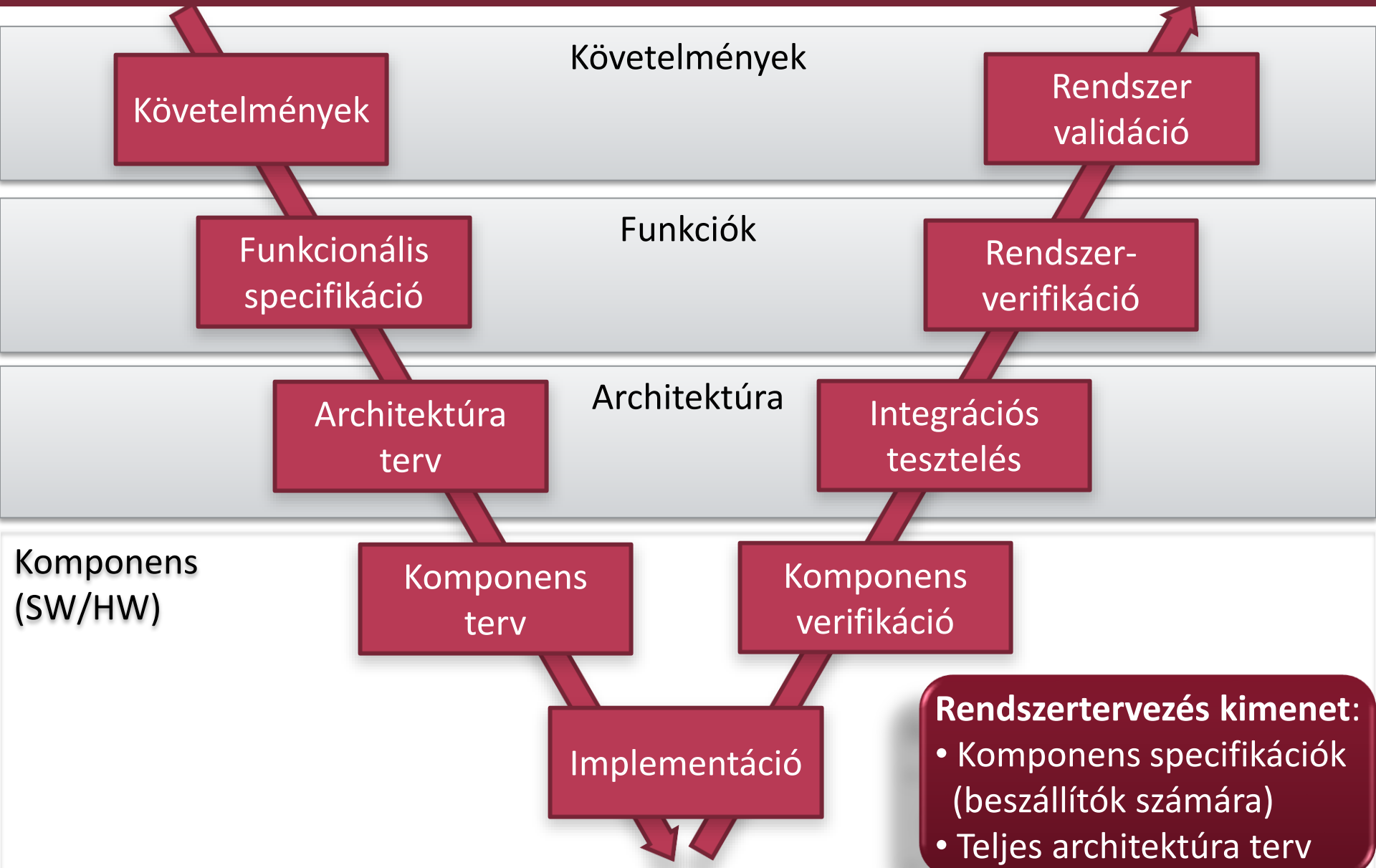
A RENDSZERTERVEZÉSI FOLYAMATA

V-modell: Kritikus rendszerek



Jellegzetességek:
- Top-down
- Sok résztvevő/aspektus
- Tanúsítványozás

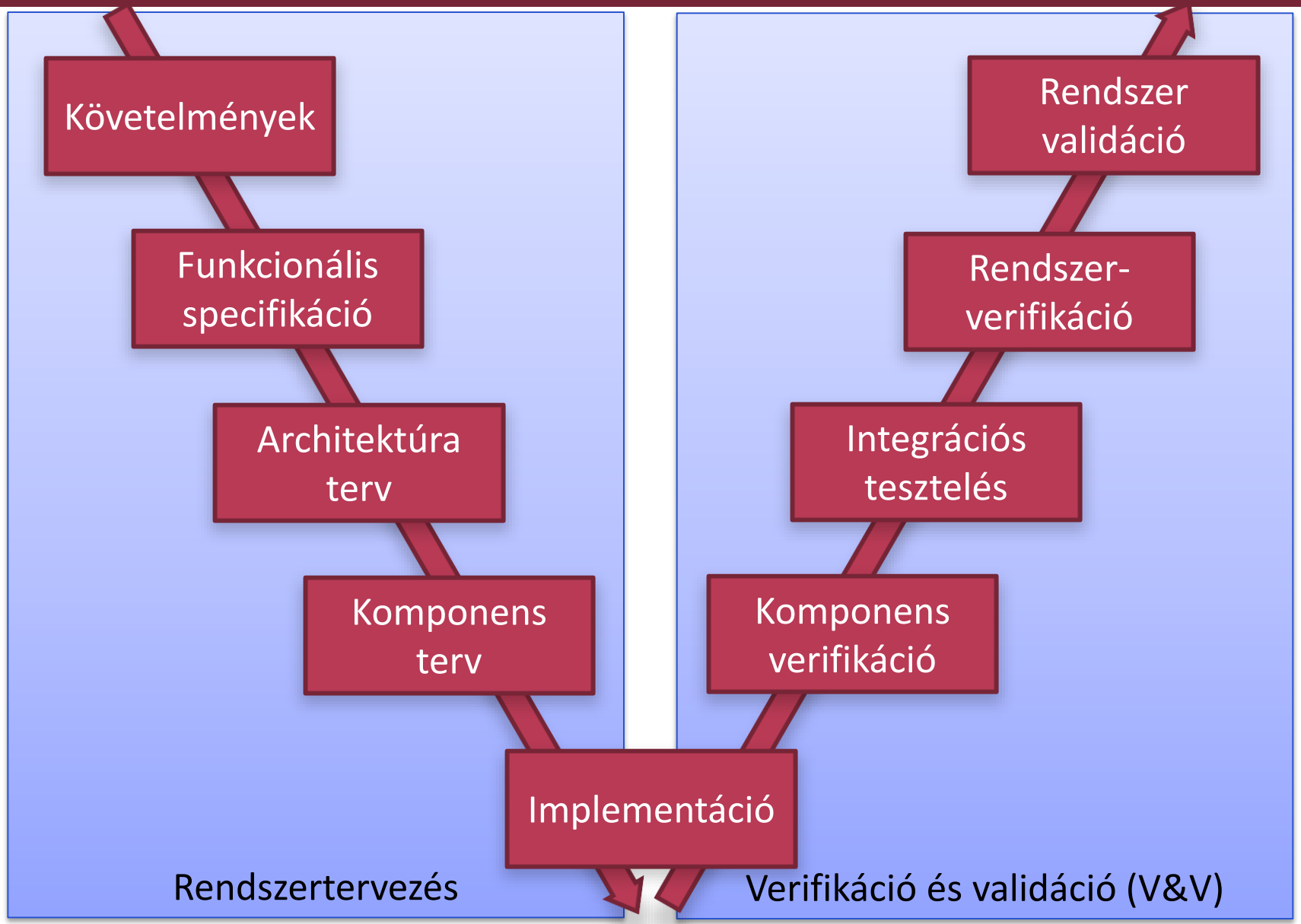
A rendszertervezés feladata



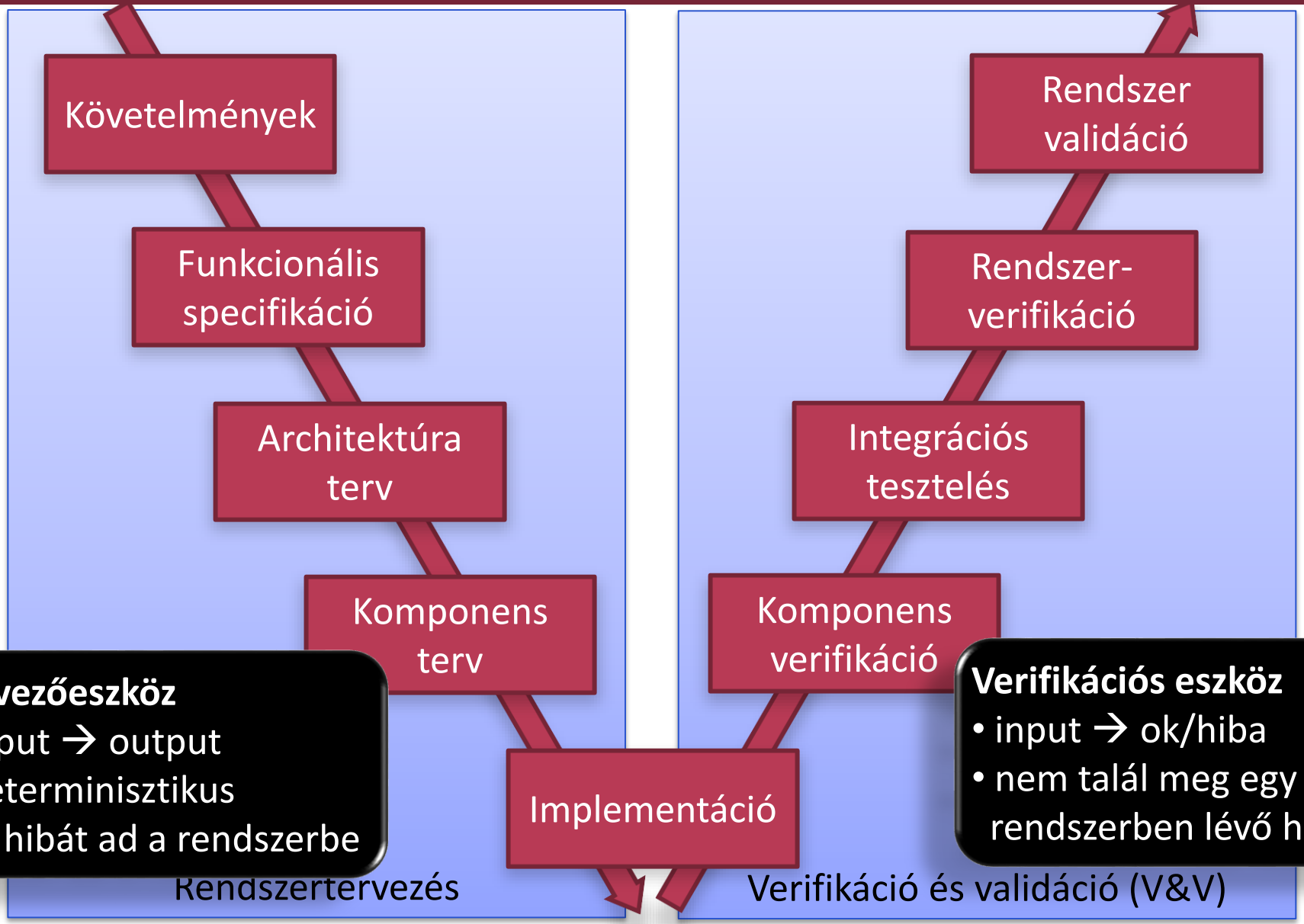
Rendszertervezés kimenet:

- Komponens specifikációk (beszállítók számára)
- Teljes architektúra terv

Rendszertervezés vs. -verifikáció



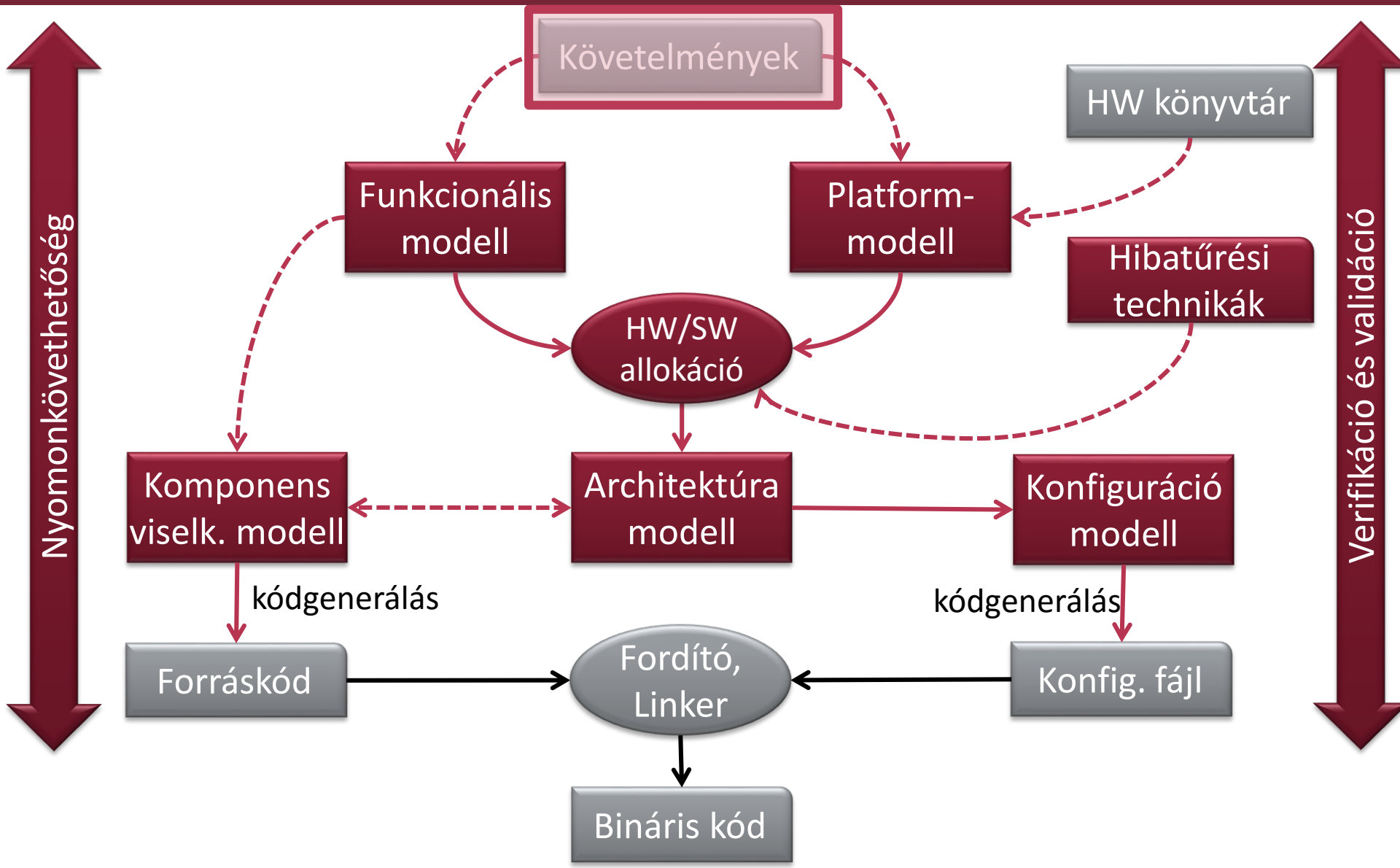
Tervezőeszköz vs. verifikációs eszköz



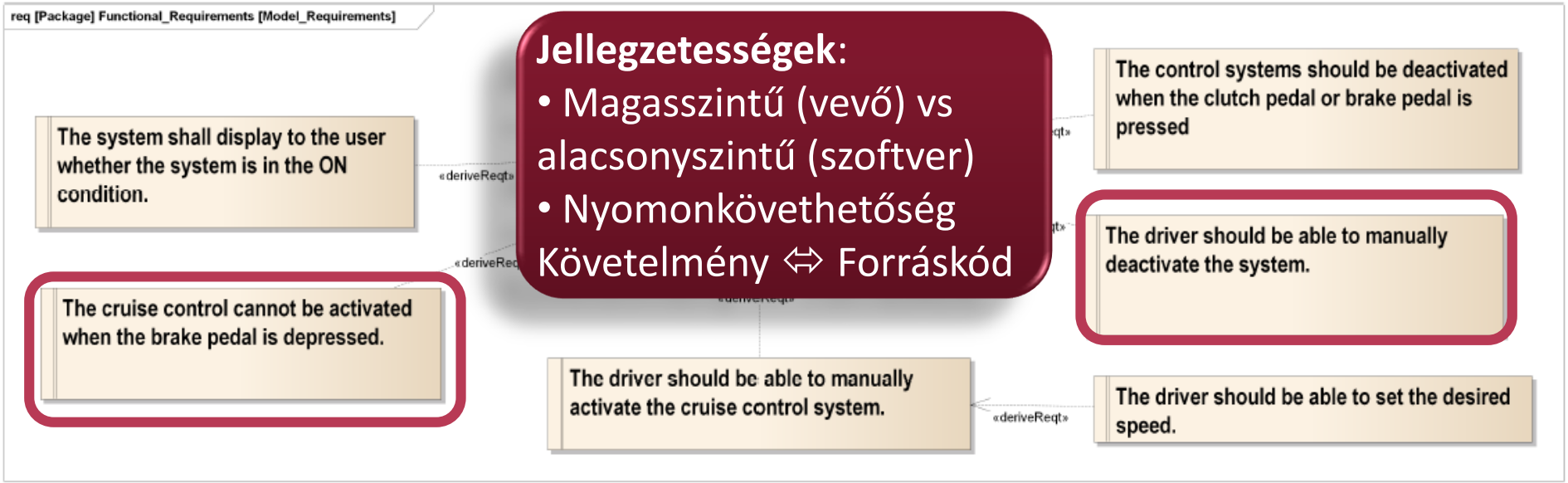
Tervezőeszköz
- input → output
- determinisztikus
- új hibát ad a rendszerbe

Verifikációs eszköz
- input → ok/hiba
- nem talál meg egy rendszerben lévő hibát

Platform-alapú rendszertervezés



Követelmények



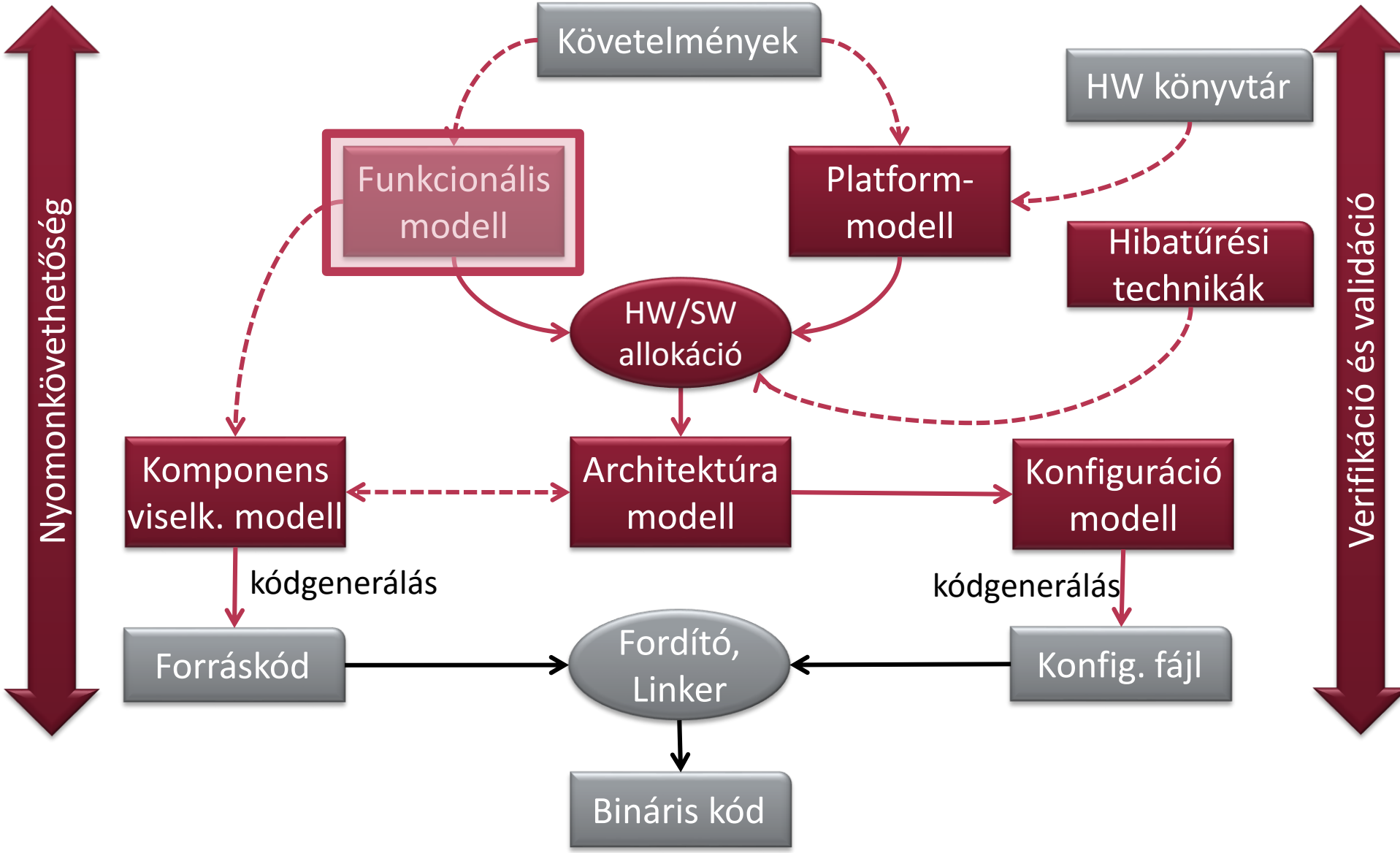
Példa

- A vezető kézzel kikapcsolhatja a tempomatot
- A tempomat nem aktiválható, ha fékpedál le van nyomva

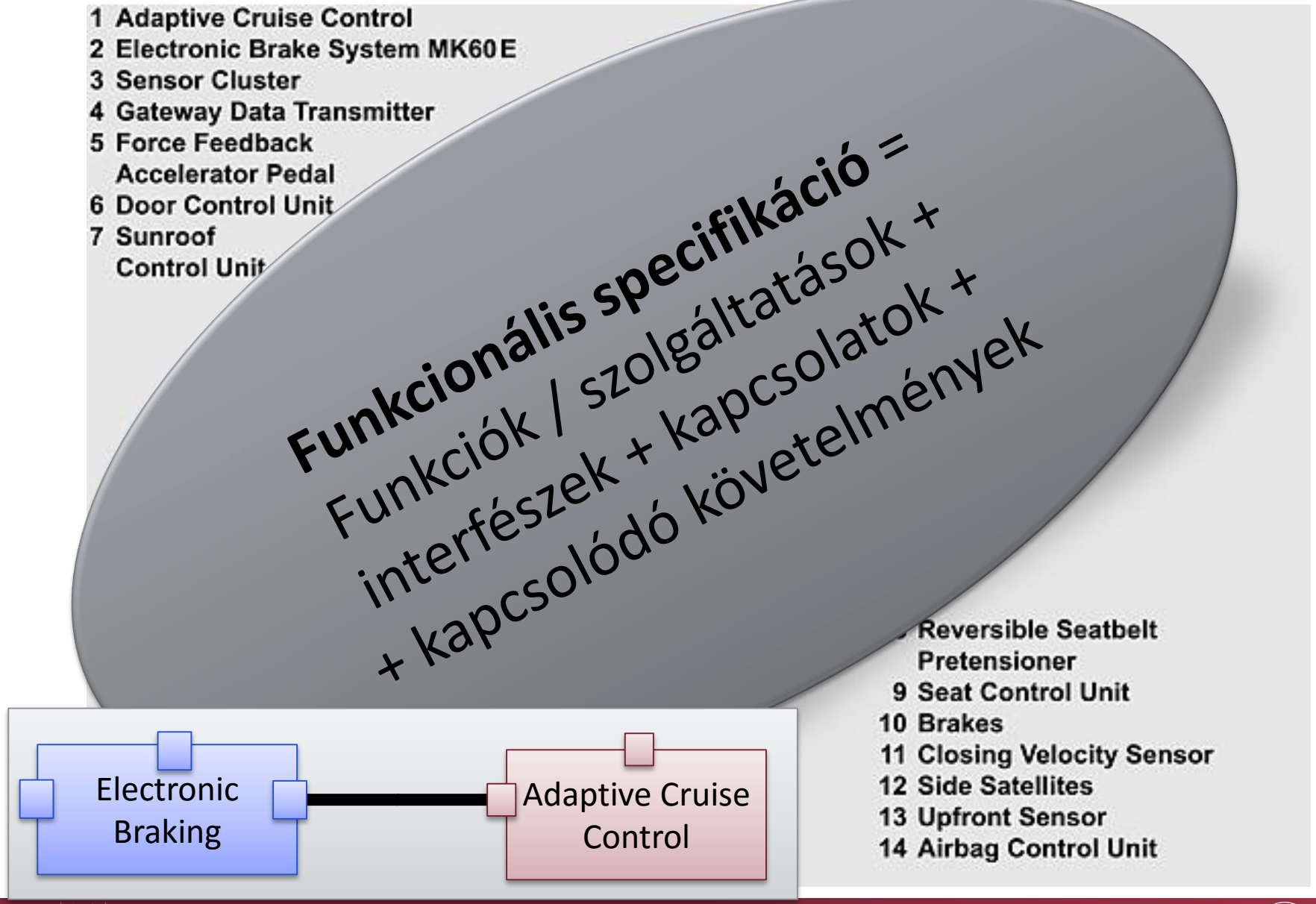
- REMO:
  - Követelmények modellezése
  - Funkcionális / nemfunkcionális
  - Finomítás / Konfliktus
- RETE (UML / SysML):
  - Requirements diagram
  - Use case diagram

Kép forrás: A.V. Varadarajan et al: Development and Validation of Functional Model of a Cruise Control System. Proc. FESCA 2016, pp. 45-58

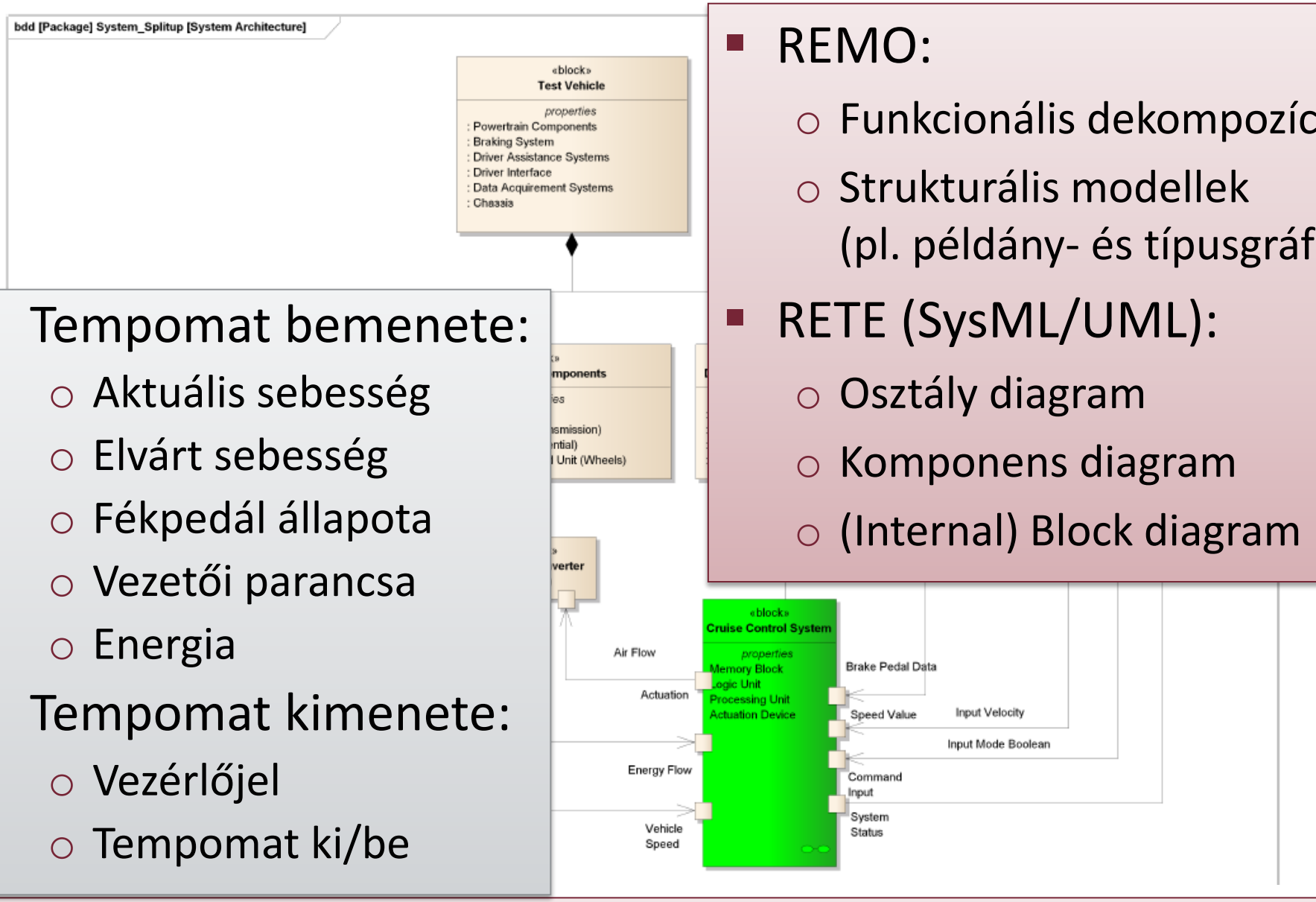
Platform-alapú rendszertervezés



Funkcionális specifikáció



Példa: Funkcionális specifikáció

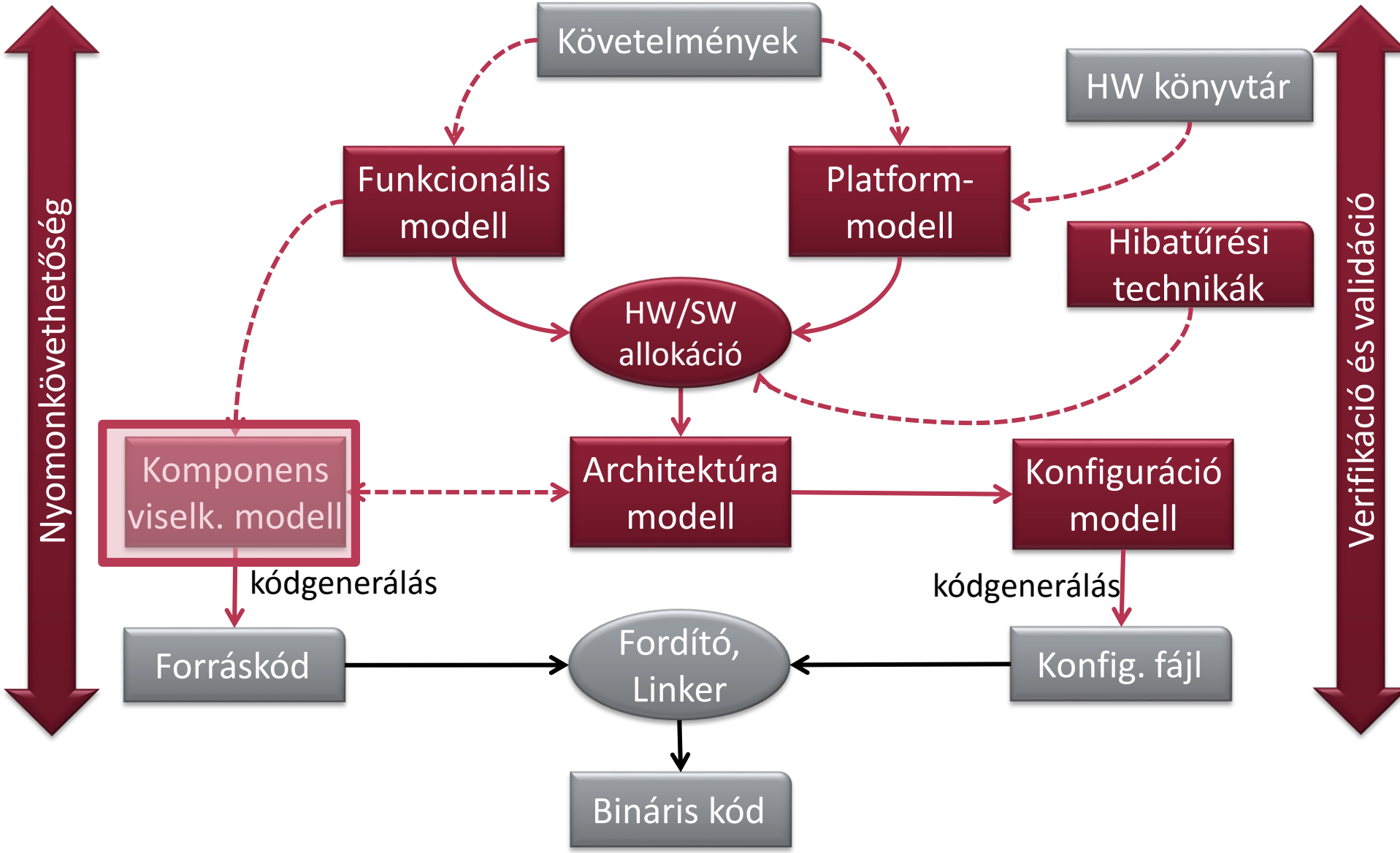


- Tempomat bemenete:
  - Aktuális sebesség
  - Elvárt sebesség
  - Fékpedál állapota
  - Vezetői parancsa
  - Energia
- Tempomat kimenete:
  - Vezérlőjel
  - Tempomat ki/be

- REMO:
  - Funkcionális dekompozíció
  - Strukturális modellek (pl. példány- és típusgráf)
- RETE (SysML/UML):
  - Osztály diagram
  - Komponens diagram
  - (Internal) Block diagram

Kép forrás: A.V. Varadarajan et al: Development and Validation of Functional Model of a Cruise Control System. Proc. FESCA 2016, pp. 45-58

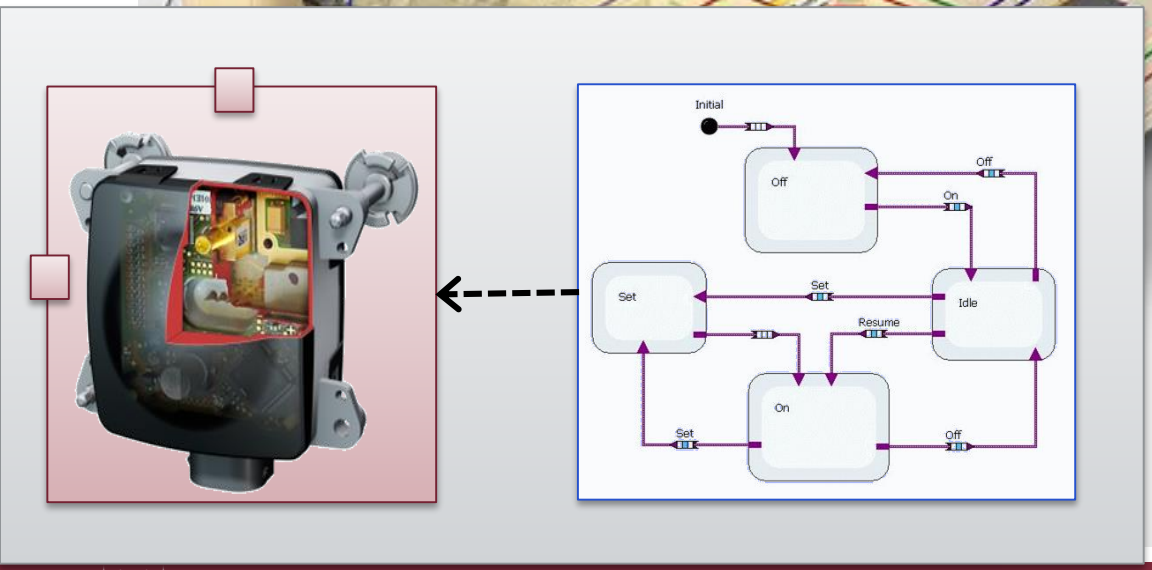
Platform-alapú rendszertervezés



Komponens terv

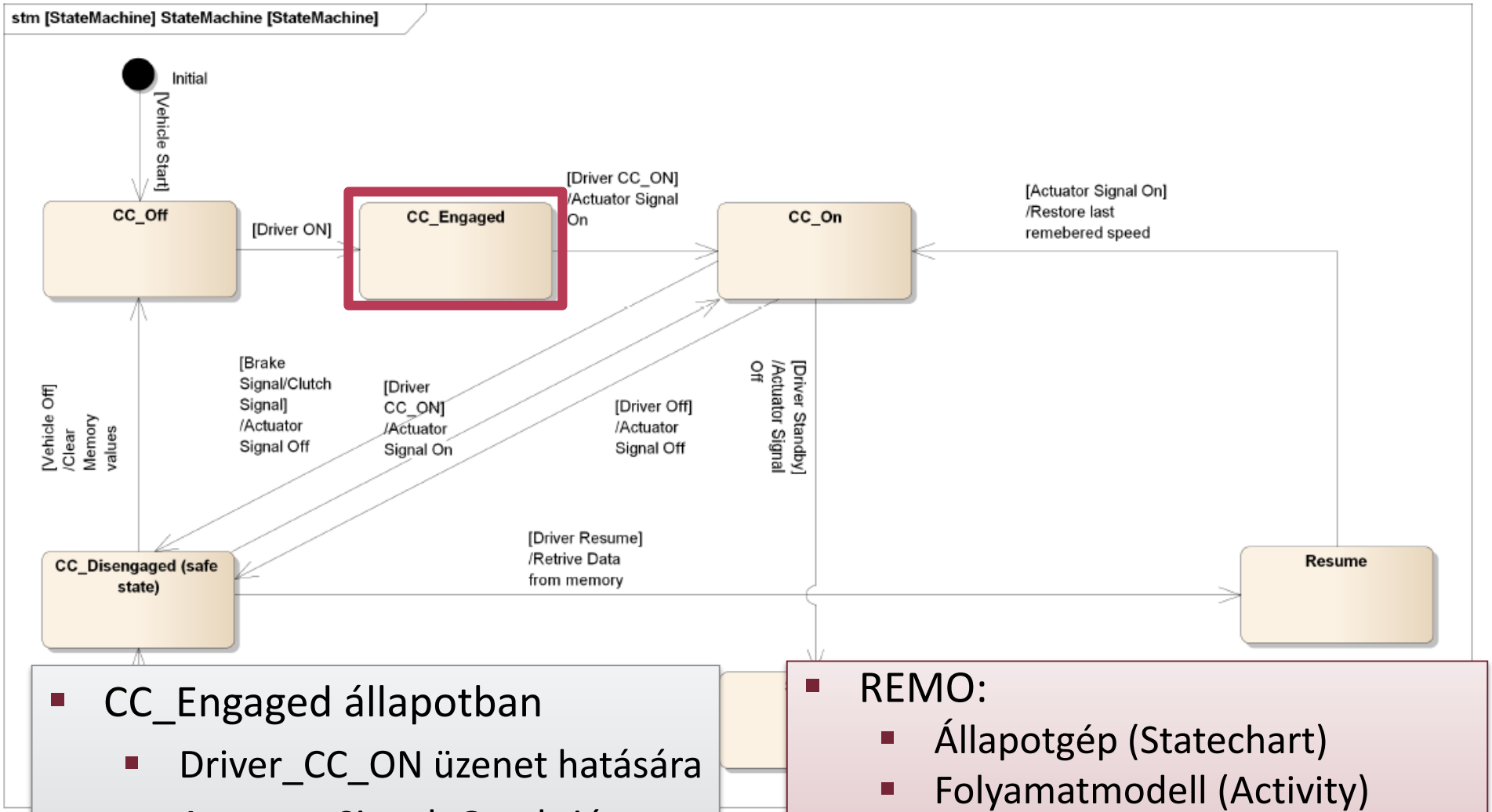
1 Adaptive Cruise Control
2 Electronic Brake System MK60E
3 Sensor Cluster
4 Gateway Data Transmitter
5 Force Feedback Accelerator Pedal
6 Door Control Unit
7 Sunroof Control Unit

Kérdések:
- Komponens belső viselkedése?
- Időzítések? Üzenetküldés



8 Reversible Seatbelt Pretensioner
9 Seat Control Unit
10 Brakes
11 Closing Velocity Sensor
12 Side Satellites
13 Upfront Sensor
14 Airbag Control Unit

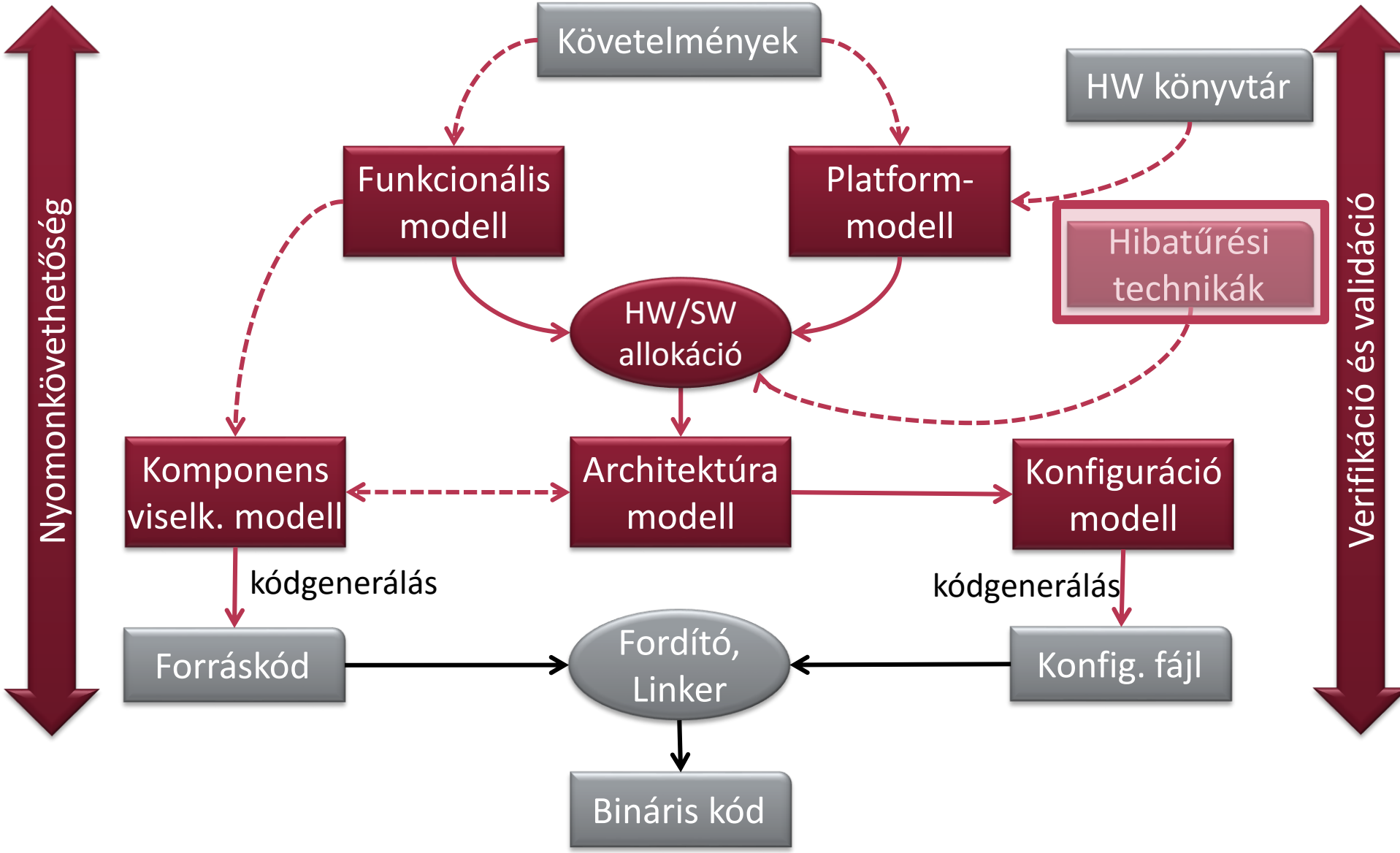
Példa: Komponens belső viselkedés



- CC_Engaged állapotban
  - Driver_CC_ON üzenet hatására
  - Actuator Signal_On akció
  - CC_On állapotba lépés

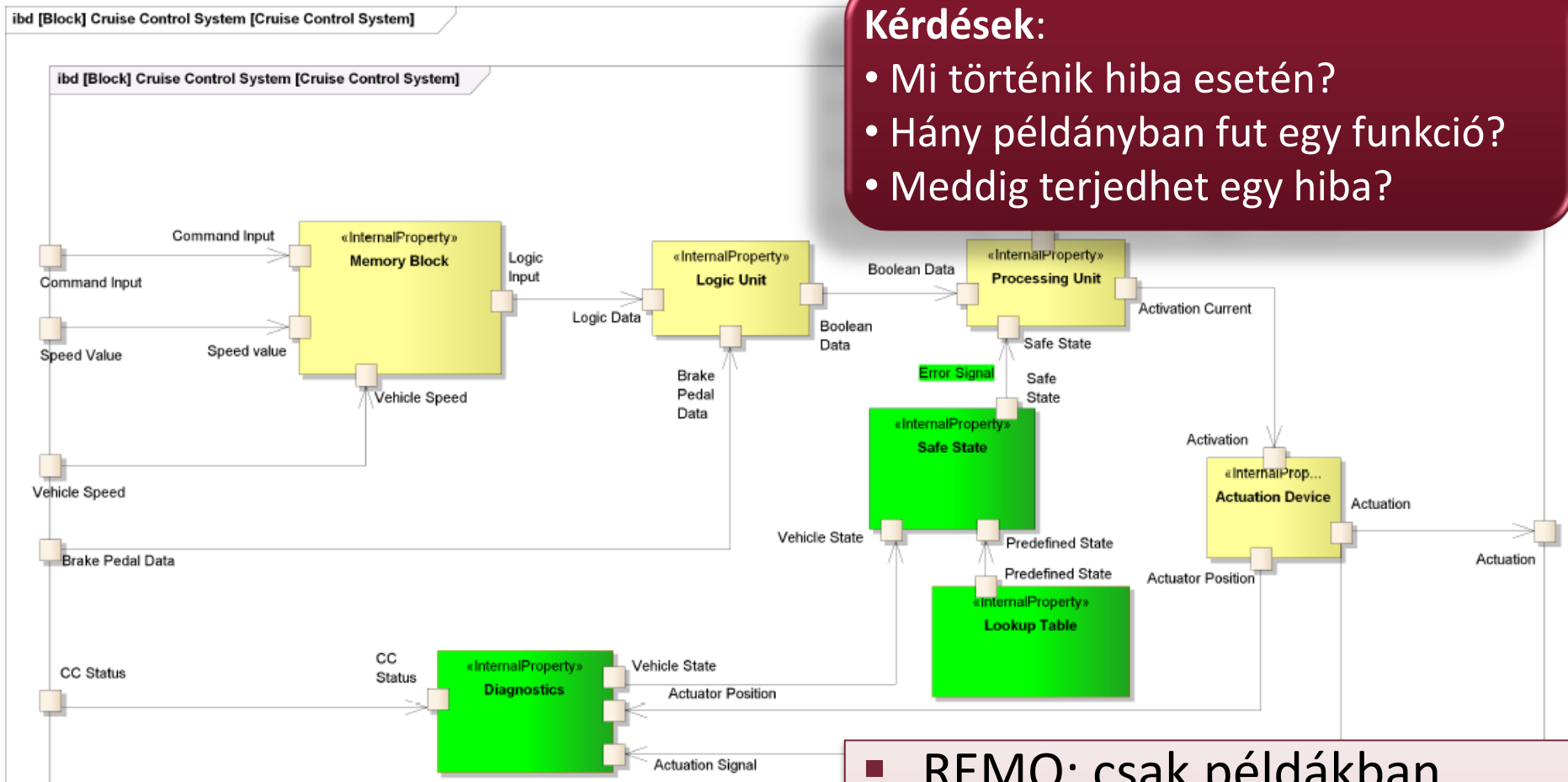
- REMO:
  - Állapotgép (Statechart)
  - Folyamatmodell (Activity)
- RETE (UML/SysML)
  - Statemachine, Activity and Sequence diagrams

Platform-alapú rendszertervezés



Biztonságra tervezés / Hibatűrés

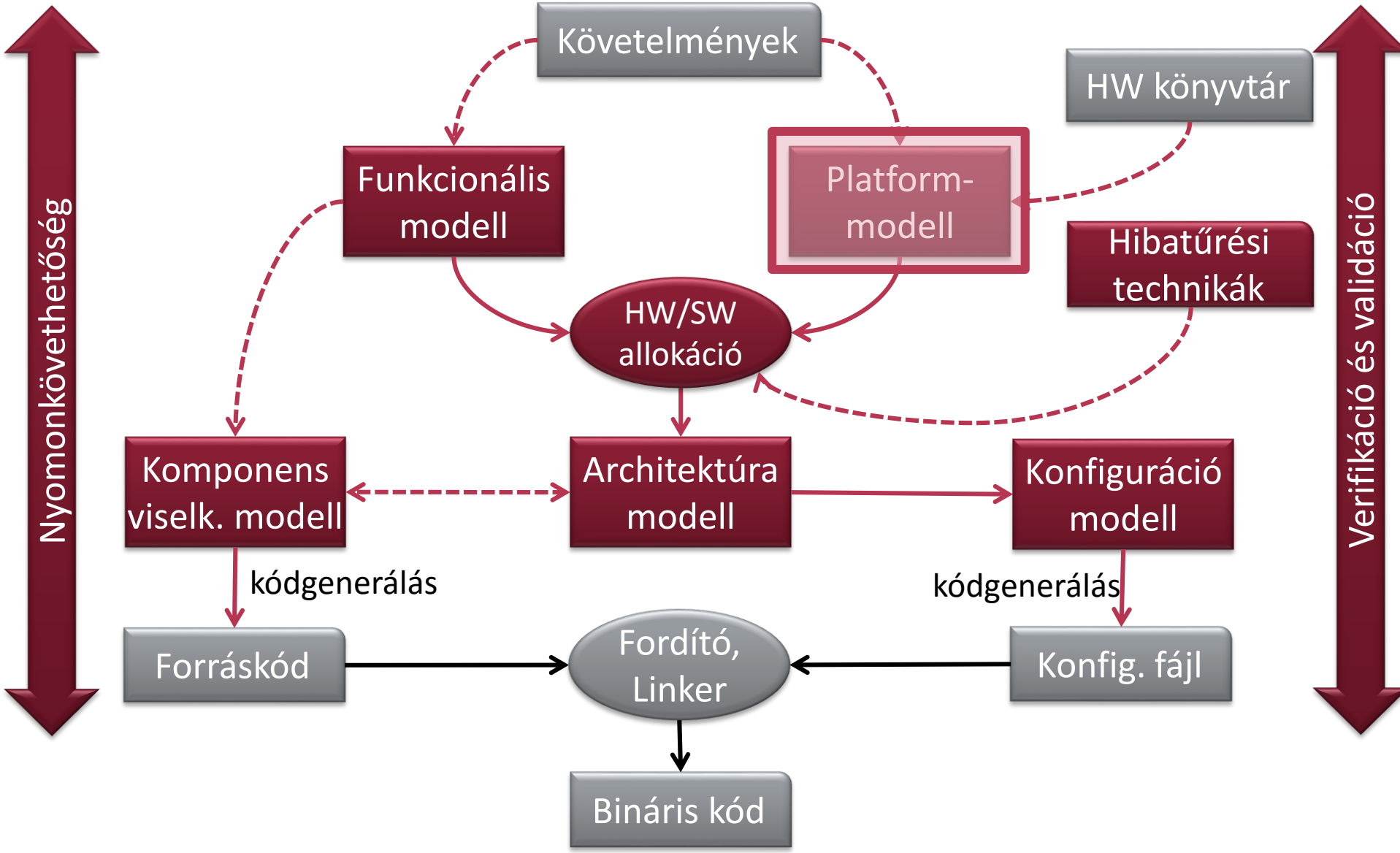
Kérdések:
- Mi történik hiba esetén?
- Hány példányban fut egy funkció?
- Meddig terjedhet egy hiba?



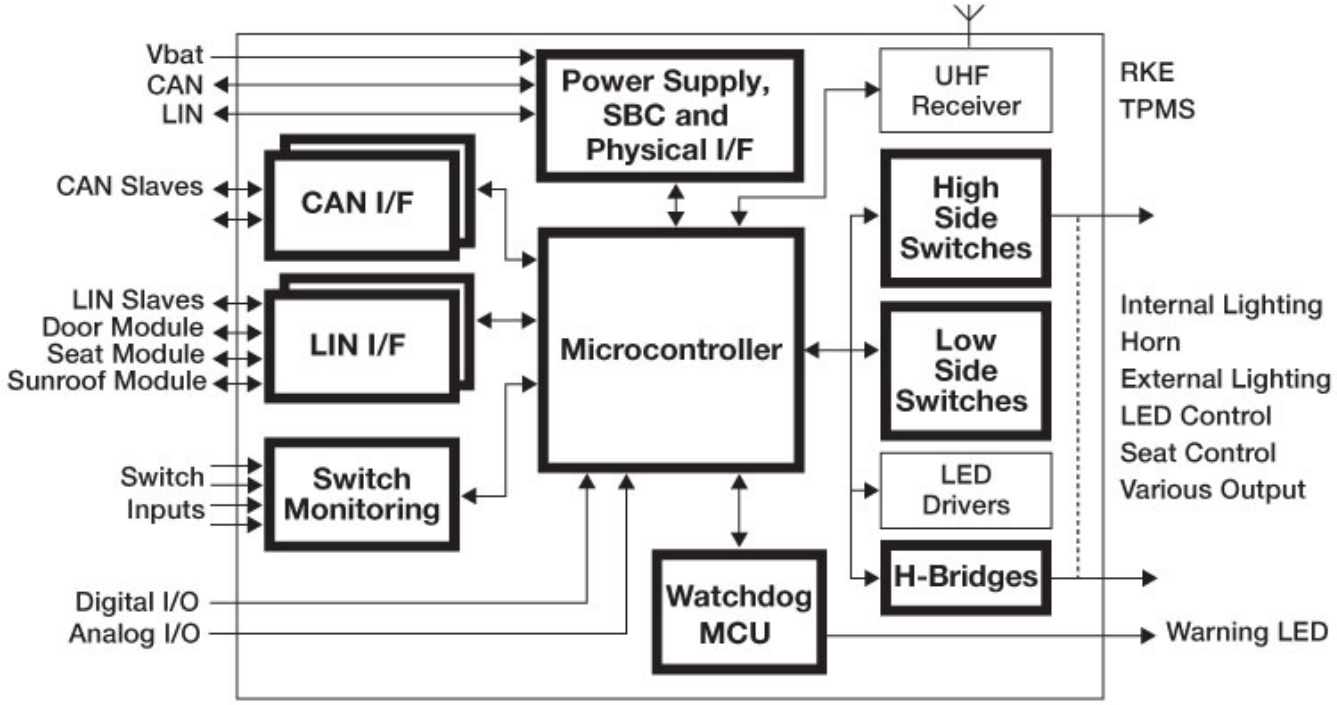
- Tempomat-kimenet monitorozása
- Összehasonlítás tárolt adatokkal
- Jelentős eltérés esetén hibajelzés
- Hibajelzés esetén deaktiválás

- REMO: csak példákban
- RETE:
  - Biztonság alapfogalmai
  - Hibatűrési technikák
  - Kockázatanalízis

Platform-alapú rendszertervezés



Platform modellezés

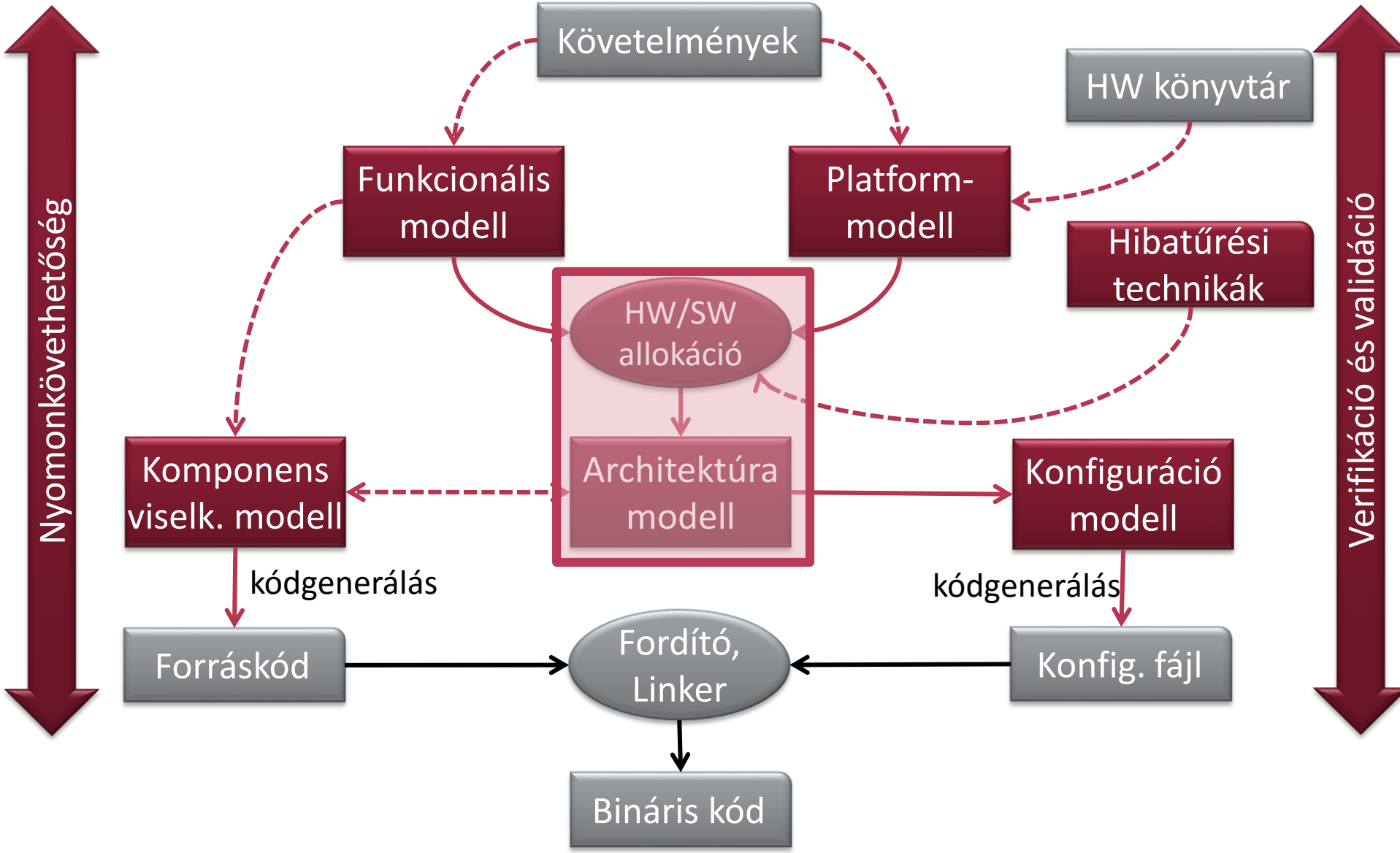


Példa

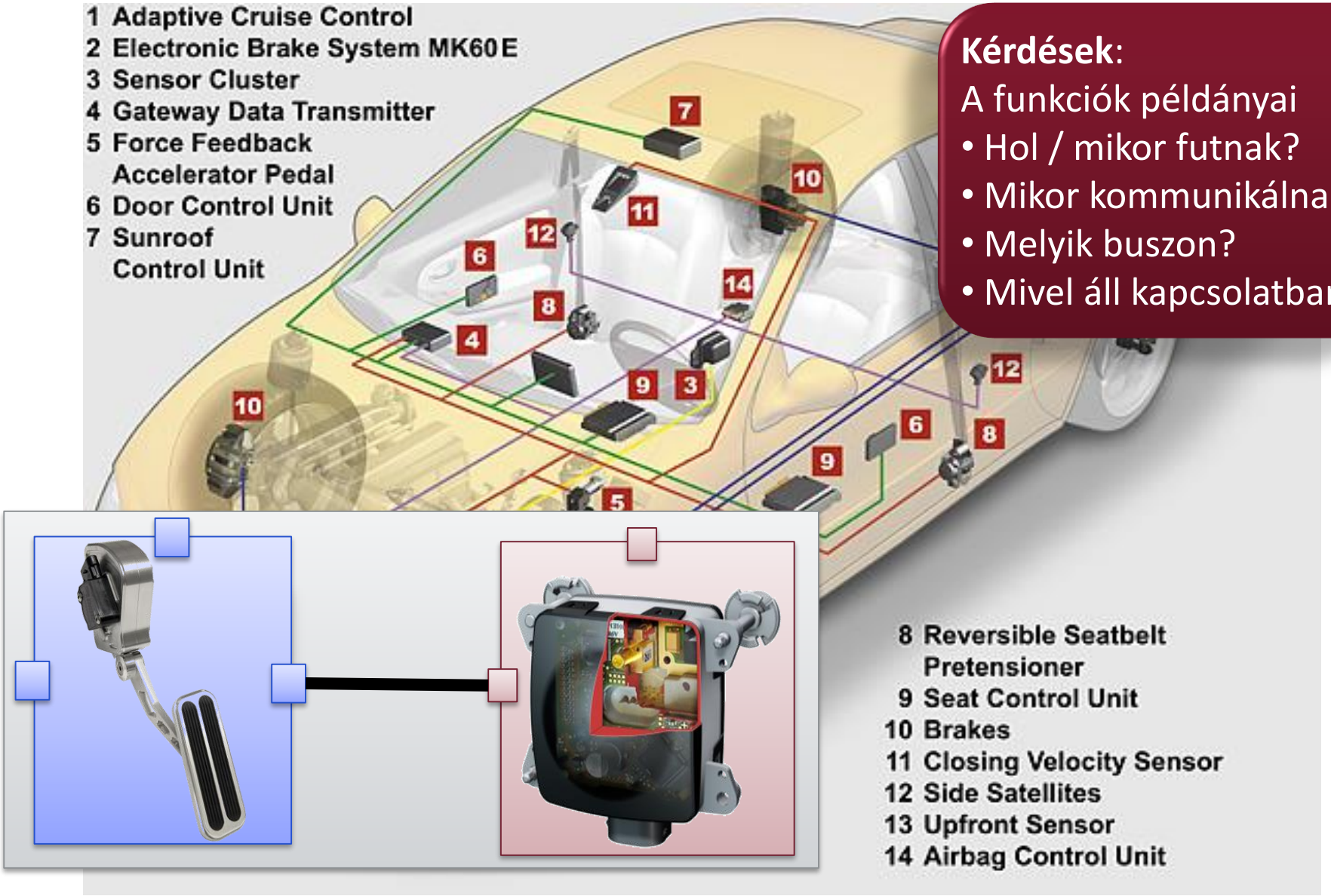
- Mikrovezérlő
- Kapcsolat szabványos interfészekkel (CAN, LIN)
- Watchdog processzor folyamatos ellenőrzésre

- DIGIT
- (REMO: Néhány példa)
- RETE:
  - Internal block diagram
  - Hibatűrési technikák

Platform-alapú rendszertervezés



Architektúra terv (aka. Rendszermodell)



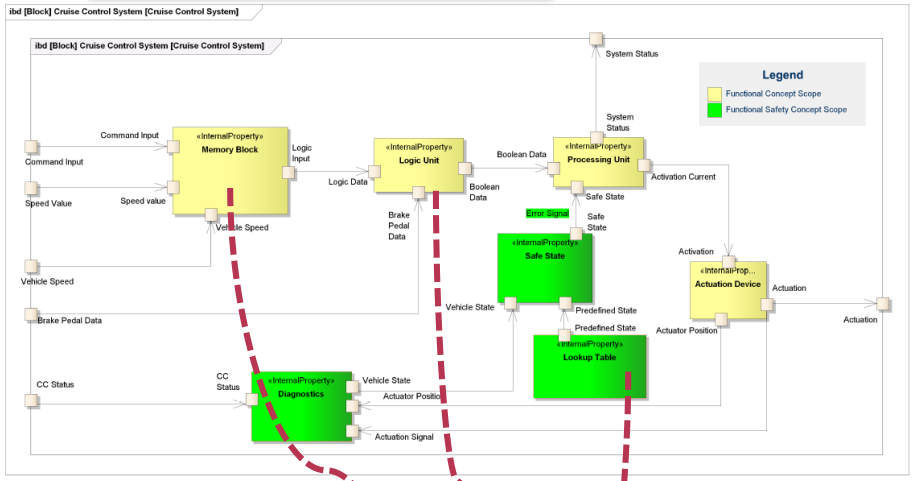
Kérdések:

A funkciók példányai

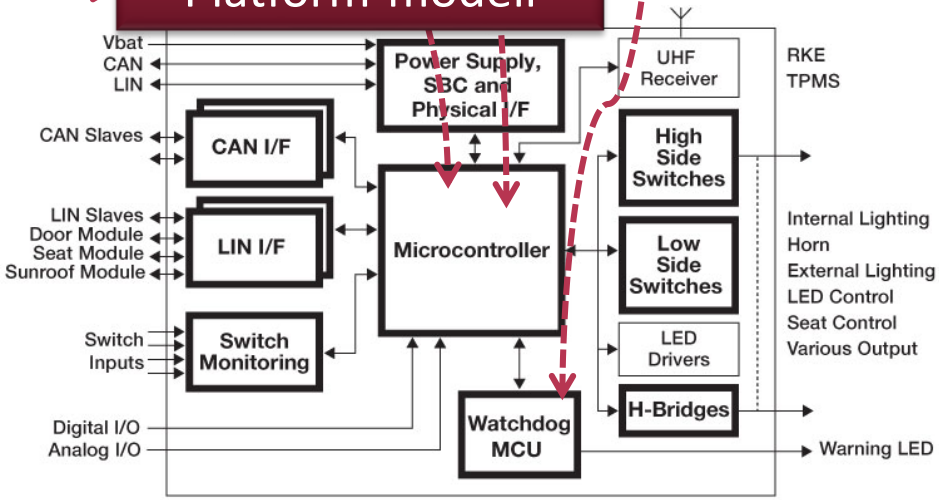
- Hol / mikor futnak?
- Mikor kommunikálnak?
- Melyik buszon?
- Mivel áll kapcsolatban?

Példa: Architektúra terv (Rendszermodell)

Funkcionális modell



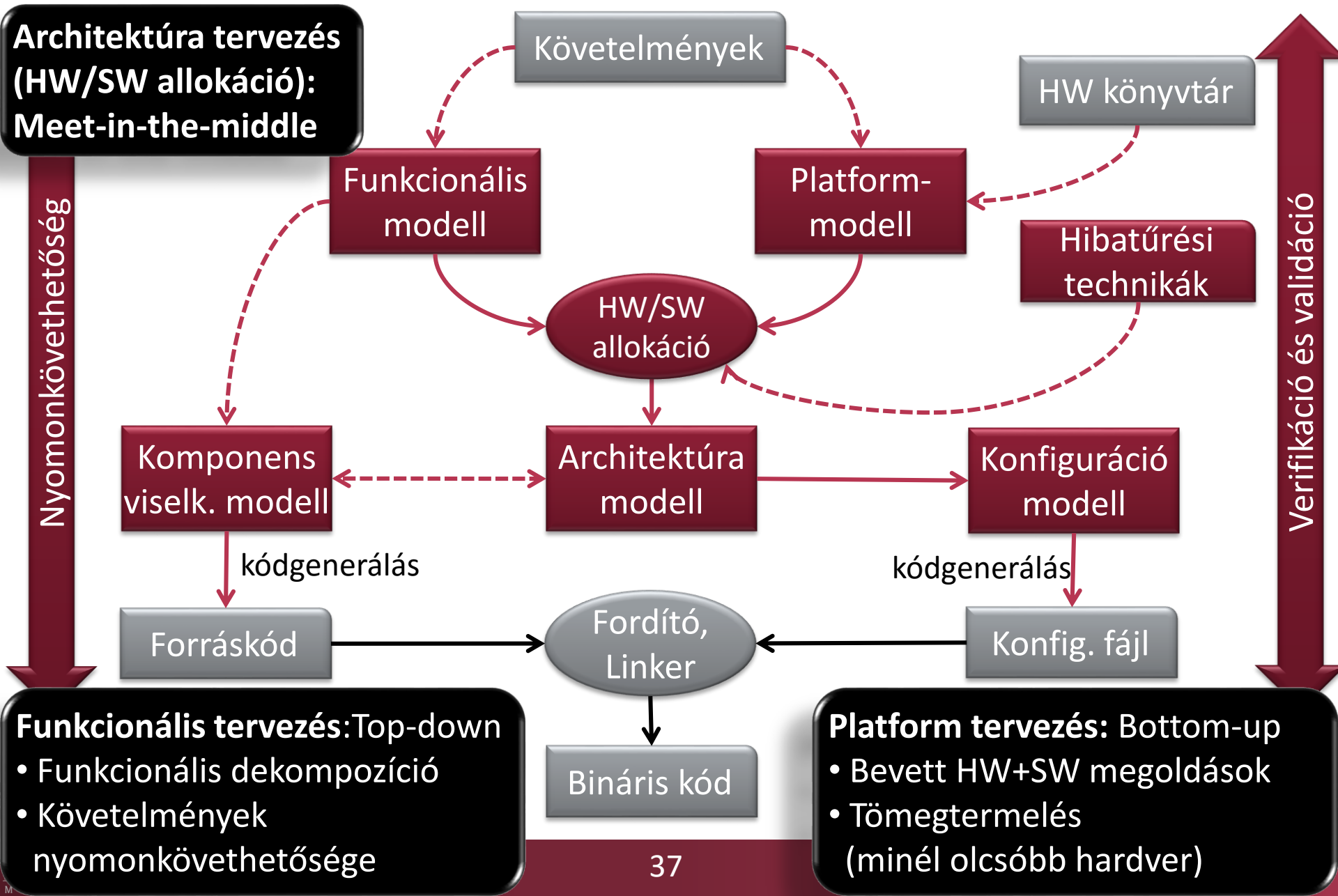
Platform-modell



HW/SW allokáció

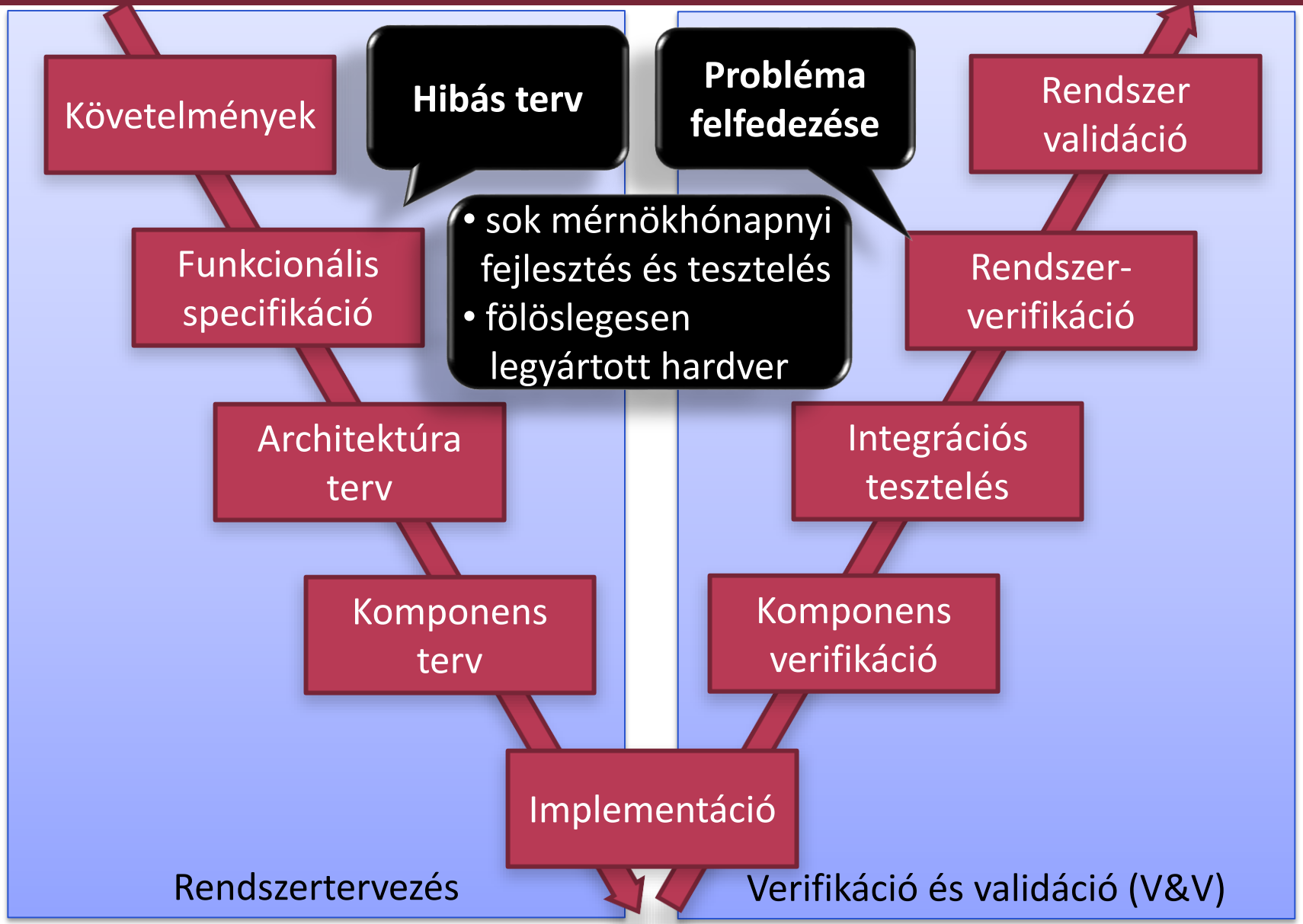
- REMO
  - Nemfunkcionális követelmények
  - Teljesítménymodellezés
- RETE
  - Nemfunkcionális követelmények analízise
    - Ütemezés
    - Rendelkezésre állás
  - Allokáció és telepítés

Platform-alapú rendszertervezés



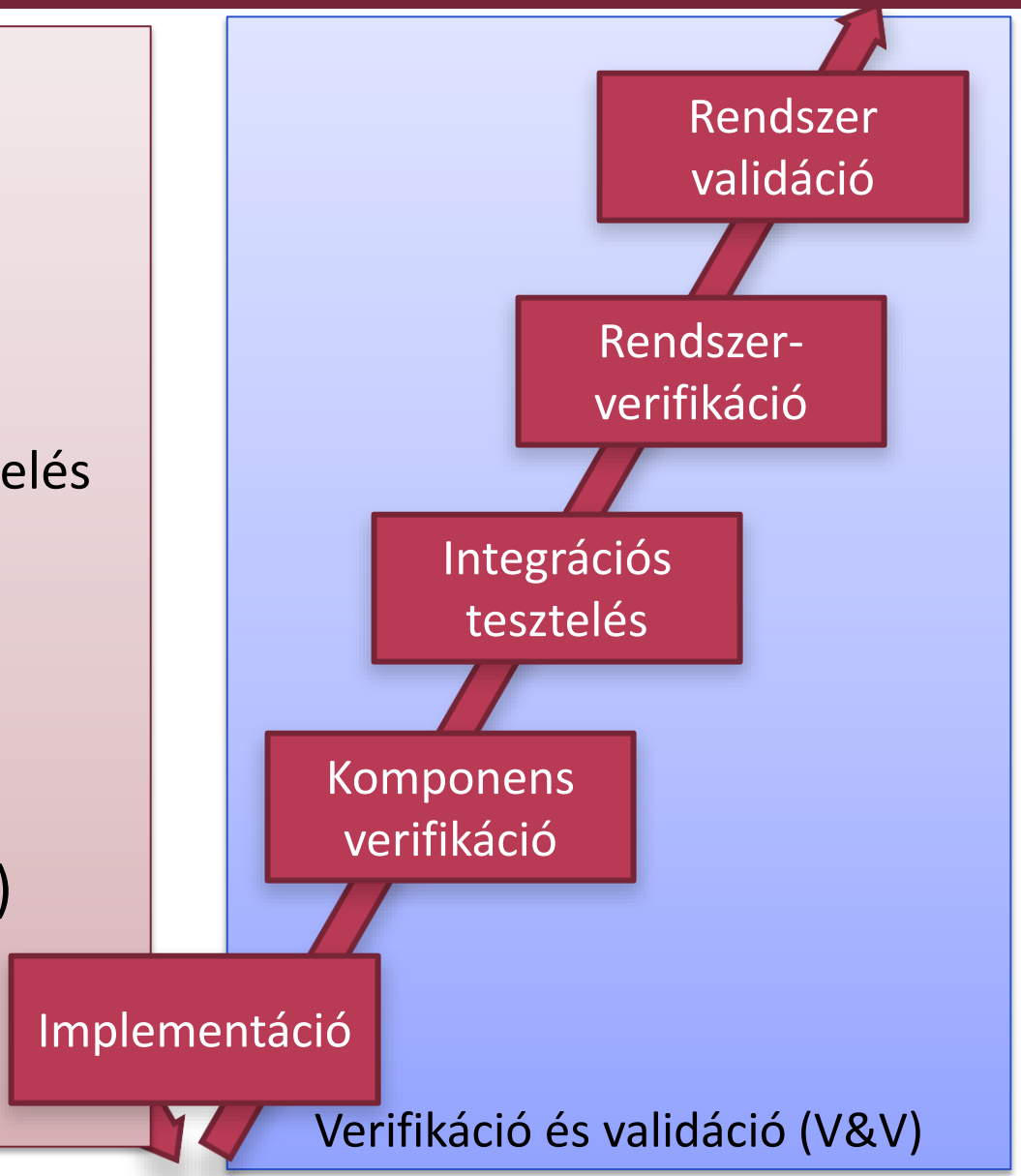
VERIFIKÁCIÓ ÉS VALIDÁCIÓ A RENDSZERTERVEZÉSBEN

Motiváció

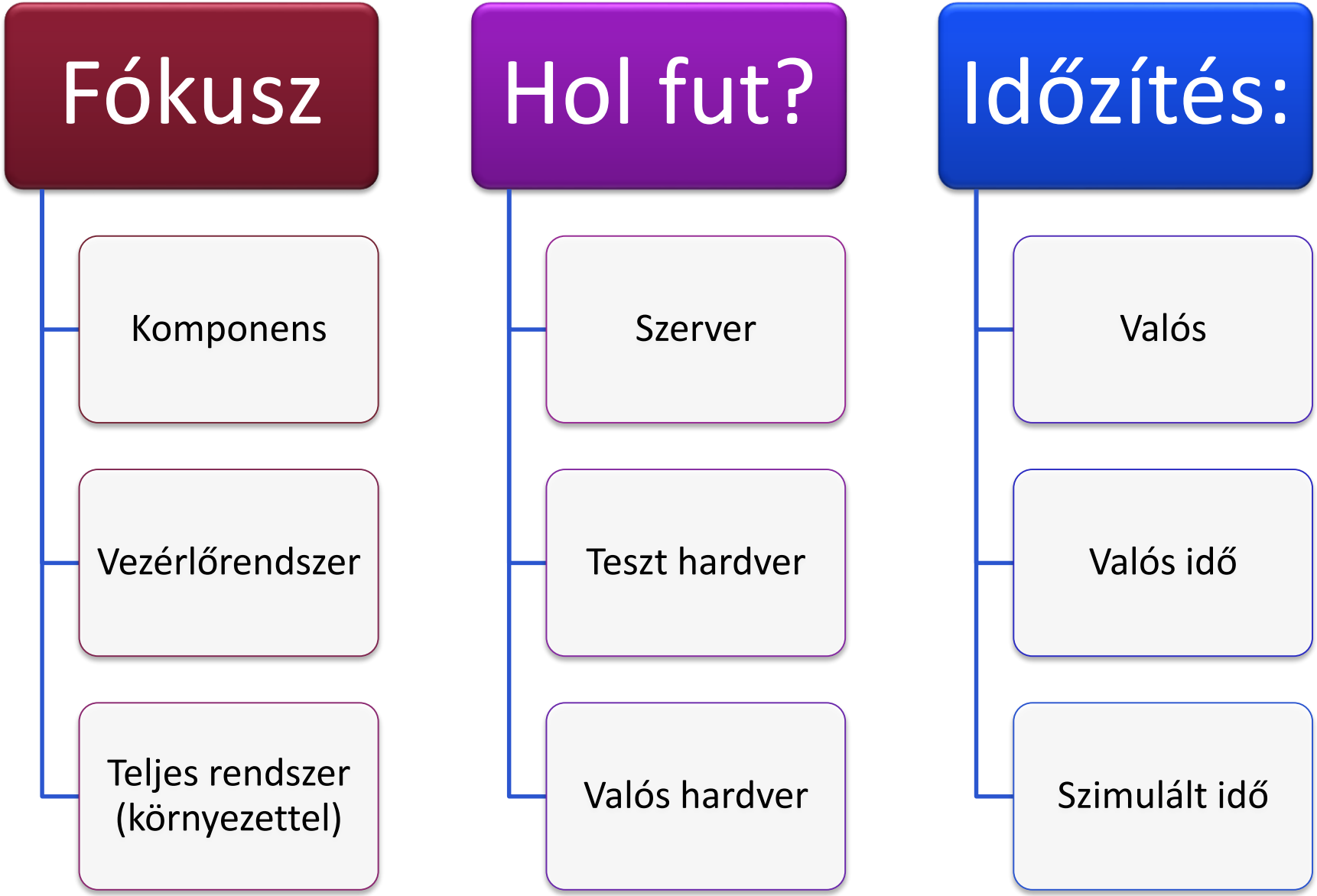

Követelmények
Hibás terv
Probléma felfedezése
Rendszer validáció
Funkcionális specifikáció
• sok mérnökhónapnyi fejlesztés és tesztelés
• fölöslegesen legyártott hardver
Rendszer-verifikáció
Architektúra terv
Integrációs tesztelés
Komponens terv
Komponens verifikáció
Implementáció
Rendszertervezés
Verifikáció és validáció (V&V)

V&V technikák a képzésben

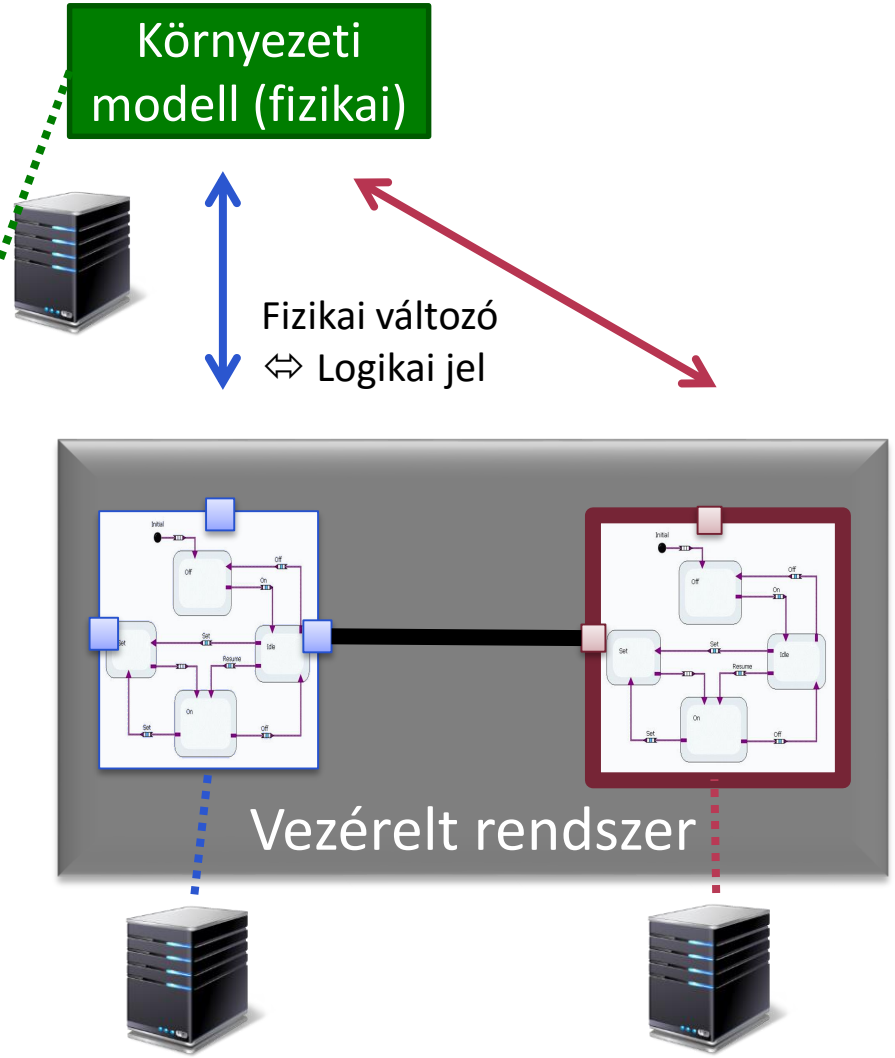
- REMO
  - Szimuláció (folyamat)
  - Tesztelés (orákulum / fedettség / öntesztelés)
  - Modellellenőrzés alapok
- RETE
  - Követelmény alapú tesztelés
  - Modell alapú tesztelés
- Ipari Informatika
  - HIL / SIL
  - Szimuláció
- Szoftver- és rendszerellenőrzés (MSc)
  - Számos további módszer



Szimuláció/tesztelés alapú verifikáció és validáció



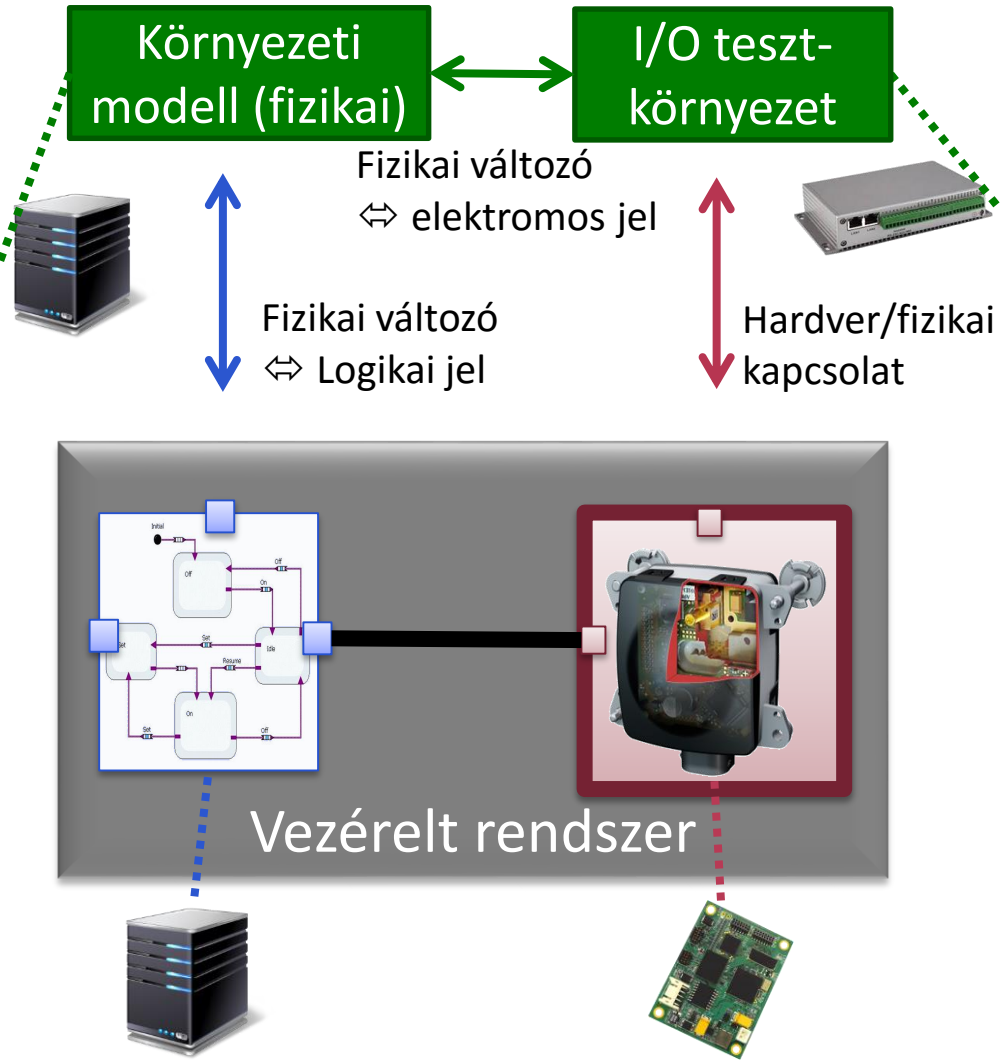
Komponens verifikáció



Software-in-the-loop

- Rendszer
  - Szimulált (nem valósidejű)
  - Integrálandó komponens
    - Modell / Lefordított kód
  - Más komponens szimulált
    - Modell / Telepített szoftver
- Fizikai környezet
  - Szimulált (nem valósidejű)
- Ellenőrzés:
  - Jellegzetes futási utak (szcenáriók) vizsgálata
  - Modell alapú tesztelés

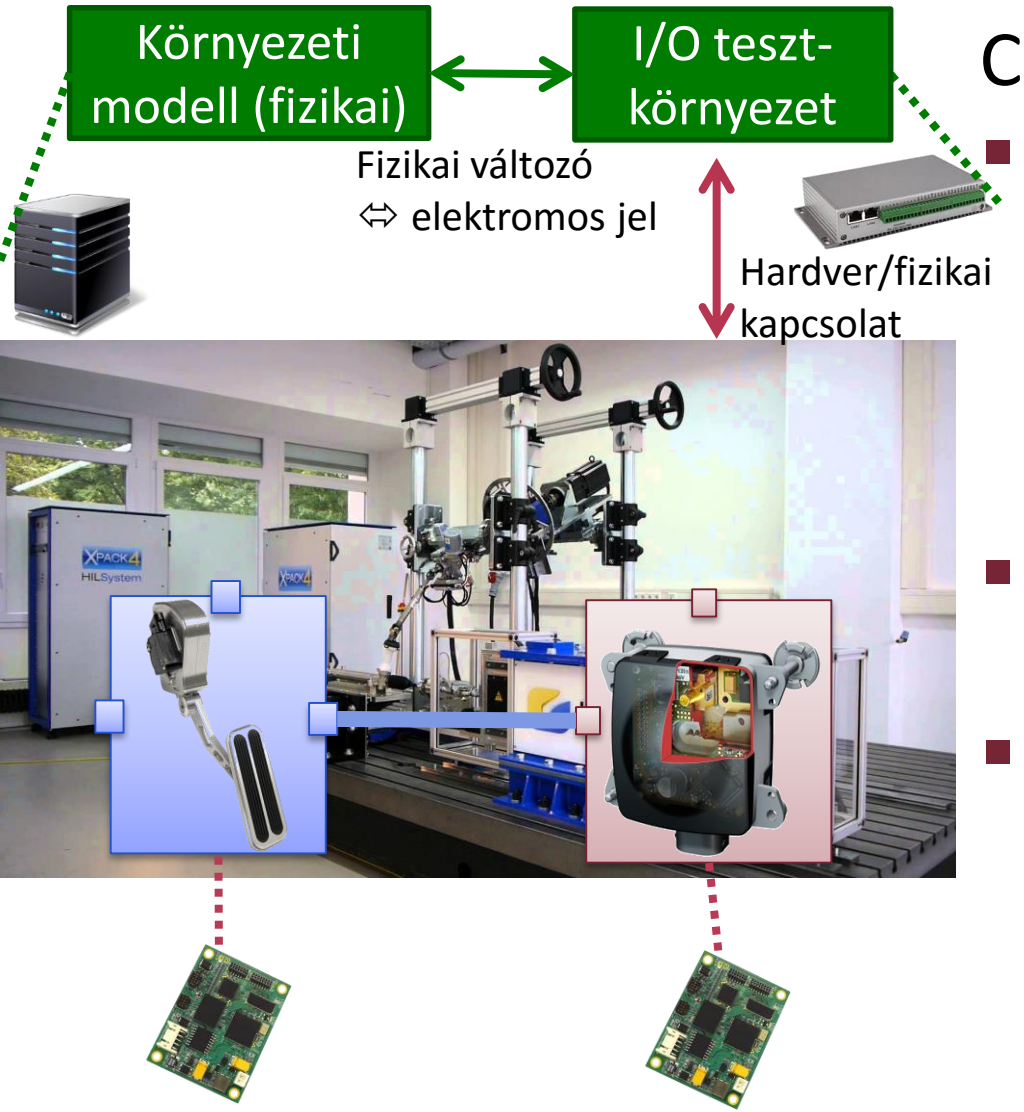
Integrációs tesztelés



Hardware-in-the-loop

- Rendszer:
  - Valós idejű szimuláció
  - Integrálandó komponens: valós hardverre telepített
  - Egyéb komponens: szimulált
    - (modell) / fordított szoftver
- Fizikai környezet: Valós idejű, szimulált
  - Környezeti modellből számított
  - Korábbi mérési adatok (benchmark)
- Ellenőrzés:
  - Hardveres integráció helyessége

Rendszerverifikáció



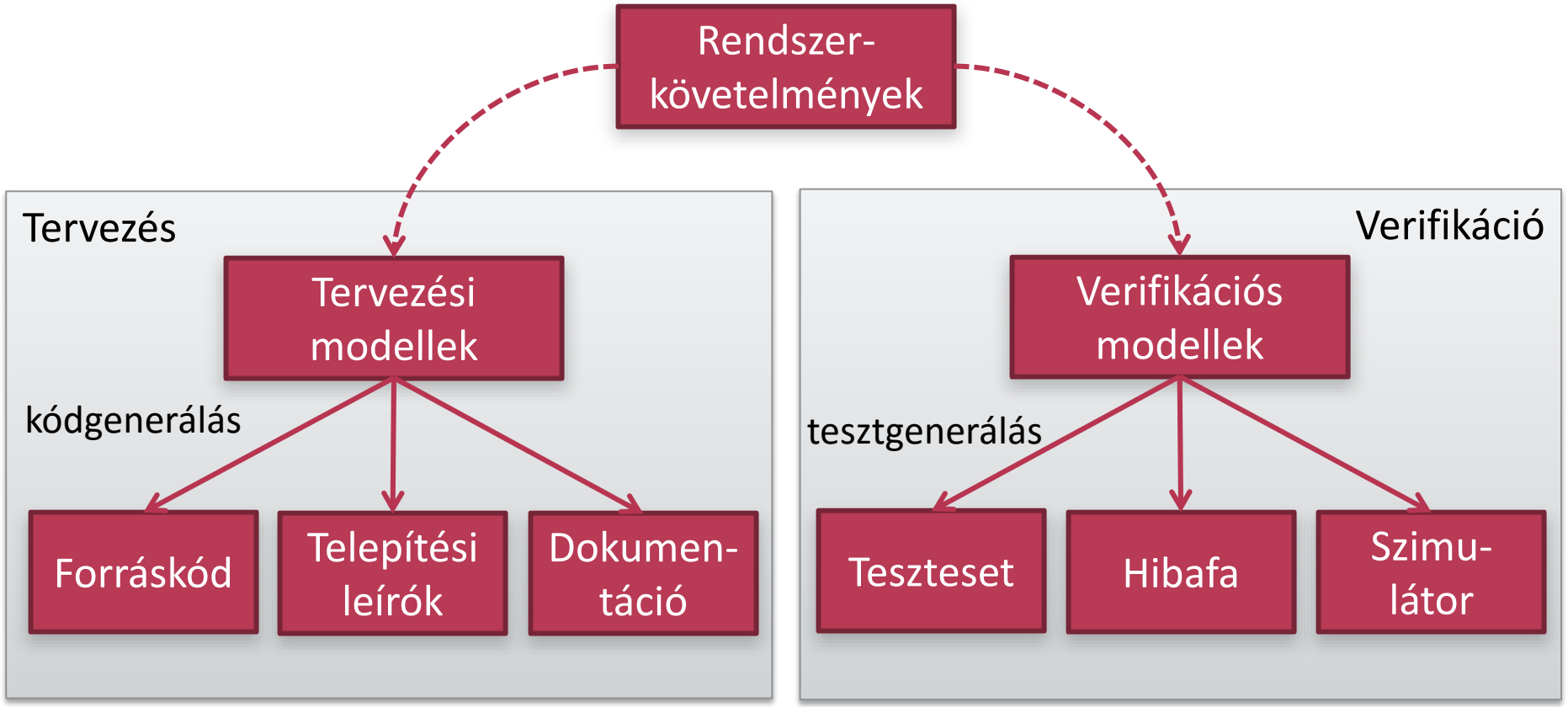
Component-in-the-loop

- Rendszer: Integrált
  - Valós hardverre telepített komponensek
  - Elektromos integráció (vezérlőjelek, tápellátás)
  - Valós működés
- Fizikai környezet:
  - Valós idejű, szimulált
- Ellenőrzés:
  - Korábbi mérési adatok (benchmark)
  - Virtuális töréstesztek, stb.

Rendszervalidáció

- Rendszer:
  - Valós hardverre telepített komponensek
  - Teljeskörű integráció (mechanika, stb.)
- Fizikai környezet: valós
  - Közút
  - Tesztpálya
- Ellenőrzés:
  - Tesztvezetés:
    Pl. hirtelen fékező autó
  - Törésteszt
  - Valós mérési adatok

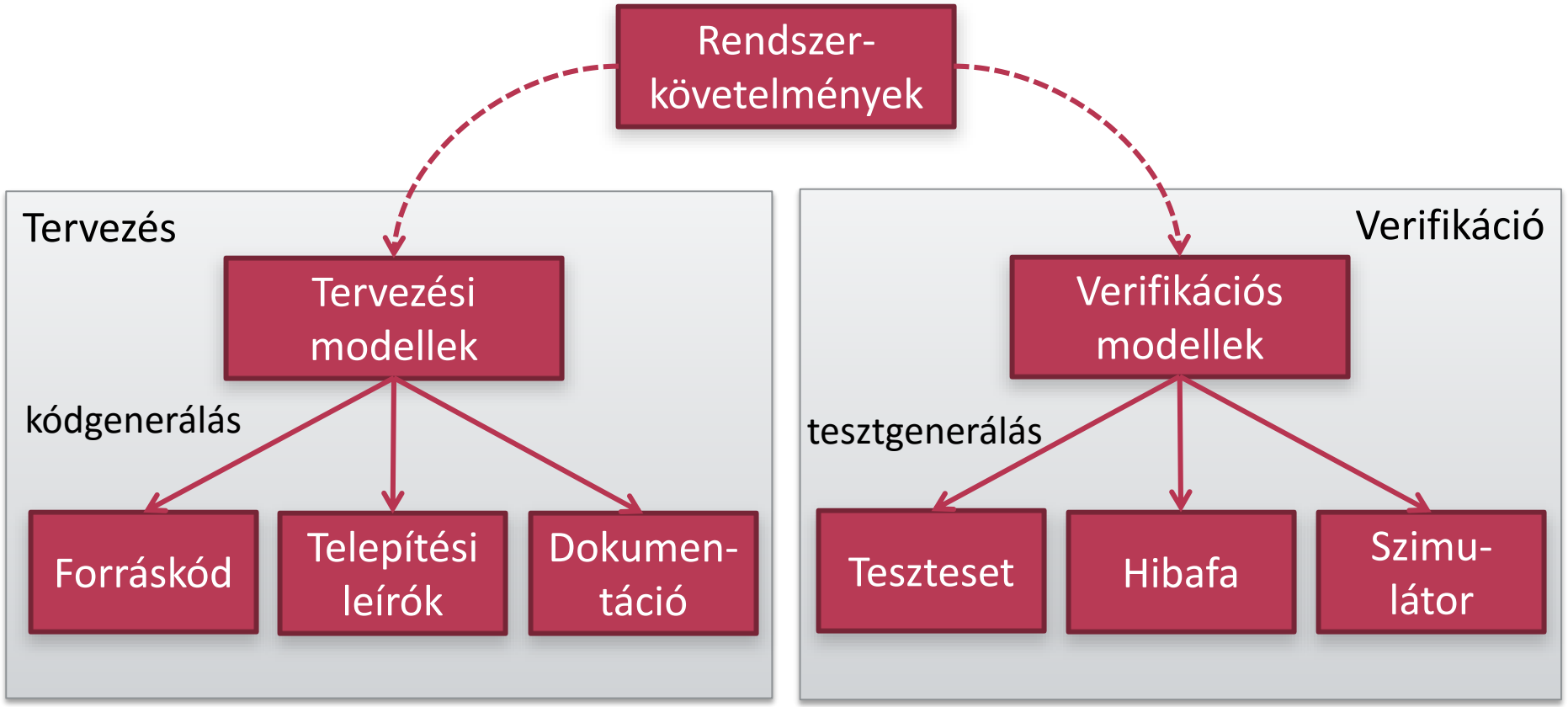
Modellek felhasználási célja



Miért nem közös modellből generálunk?

Biztosítani kell a tervezés és ellenőrzés függetlenségét!

Modellek felhasználási célja



Példák tervezési modellekre

- Állapotgépek (hierarchikus)
- Aktivitás diagramok
- Osztály diagram, Komponens diagram
- Telepítési modellek

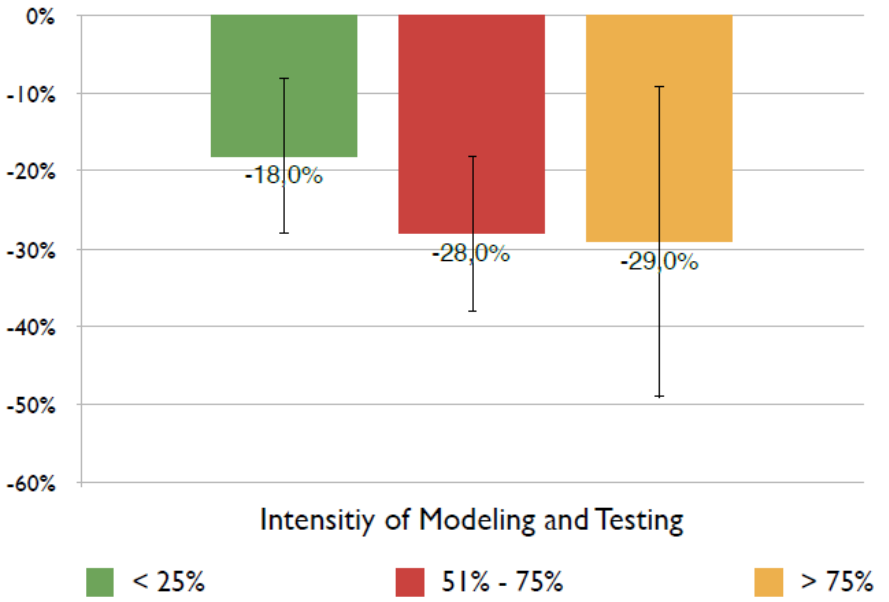
Példák verifikációs modellekre

- Állapotgépek (gyakran lapos)
- Szekvencia diagramok
- Petri hálók, Adatfolyam hálók
- Sorbanállási + ütemezési modellek

KITEKINTÉS

A modell alapú tervezés előnyei

- Jellegzetességek:
  - Tervezés:
    - 30-40%-kal több idő/költség
  - Ellenőrzés:
    - Átlagosan 40%-kal kevesebb
  - Kódgenerálás:
    - >90% a részvevők 40%-nál!
    - 40-50%-os megtakarítás
  - 3 éves megtérülés
- Miért?
  - Tervezési hibák 60%-a korai fázisban felderíthető
  - Virtuális prototípusok



Felmérés:
- autóipari szereplők
- 180 ember (14 országból)
- menedzserek, fejlesztők, R&D

M. Broy et. al: What is the benefit of a model-based design of embedded software systems in the car industry? In: Emerging Technologies for the Evolution and Maintenance of Software Models. IGI Global, 2010.

Informatikai rendszertervezés (áttekintés)

- Követelmények rögzítése
- Használati esetek

Követelmény analízis

- Funkcionális dekompozíció
- Komponens + Interfészek

Komponens tervezés

- Állapotgépek
- Adatfolyam
- Jellegzetes futási utak (szekvencia)

Viselkedés modellezés

- Biztonság (safety) alapok
- Hibatűrő rendszer-architektúrák

Biztonságra tervezés

- Platform modellezés
- Nemfunkcionális analízis
- Allokáció

Architektúra tervezés

- Specifikáció alapú tesztelés
- Modell alapú tesztelés
- Tesztfedettség

Verifikáció és validáció

- Modell-transzformáció
- Kódgenerálás

Automatizálási módszerek

Összegzés: Informatikai rendszertervezés