Informatikai rendszertervezés

Dr. Molnár Vince

(Dr. Varró Dániel fóliái alapján)

Budapesti Műszaki és Gazdaságtudományi Egyetem
Hibatűrő Rendszerek Kutatócsoport

A tárgy kontextusa

Előzmények	• Rendszermodellezés
Rendszertervezés BSc specializáció	• Informatikai rendszertervezés • Ipari informatika
MSc szakirány Kritikus rendszerek	• Modellalapú rendszertervezés • Szoftver- és rendszerellenőrzés • Kiberfizikai rendszerek

A tárgy oktatói

- Előadók
  - Dr. Molnár Vince
  - Dr. Micskei Zoltán

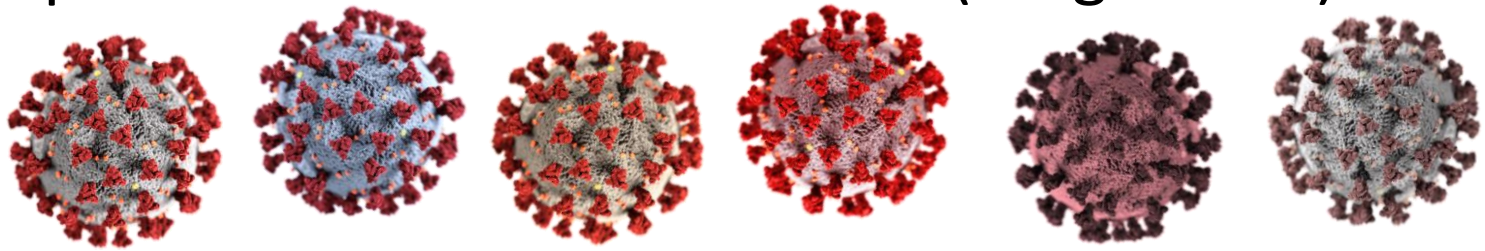

- Gyakorlat / házi feladat:
  - Demonstrátorok
    - Bajczi Levente
    - Csuvarszki Csanád
    - Dobos-Kovács Mihály
    - Szekeres Dániel
    - Szkupien Péter





Tárgykövetelmények (kivonat)

- **Házi feladat**
  - Rendszertervezési feladat 3 fős csapatoknak
  - Végső jegy 50%-a (!)
  - Formátum
    - 6 részfeladat (10 pont feladatonként)
    - Legjobb 4 teljesített (min. 4 pont) részfeladat pontja számít
    - Maradék kettőből extra pont szerezhető (max. 6-6 pont)
  - Nincs pótlás és javítás!
  - Vezető ipari tervezőeszköz használata (MagicDraw)
- **Vizsga**
  - …?



Újdonság: Megajánlott jegy

- **Megvédett házi feladat alapján**
- Feltételek:
  - Mind a **6** házi elfogadva (≥4 pont)
  - Szóbeli védés, bármelyik részletbe belekérdezhetünk
  - Minden csapattagnak külön, jelentkezés alapján

  - **Megajánlott ötös:**
    - Legalább **5** feladat ≥8 pont
  - **Megajánlott négyes:**
    - Legalább **4** feladat ≥8 pont

IMSc pontok

- Legfeljebb **20 pont** szerezhető

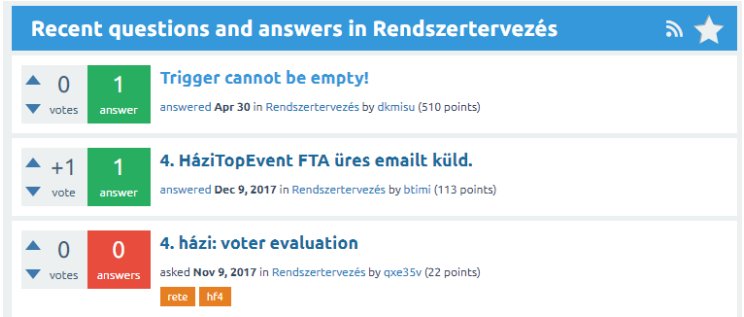
- IMSc pontok
  - IMSc rész a házi feladatokban: max. 12 pont
  - Extra házi feladat pont: max. 12 pont
  - Opcionális, egyedi feladat: max. 10 pont

- Nem csak IMSc hallgatóknak
- DE: csak jelest elért hallgatóknak
  - Megajánlott jegy esetén is

Weboldalak

- **Teams csoport**
- https://inf.mit.bme.hu/edu/courses/rete
  - Hírek, naptár
  - Segédanyagok
  - HF feladatok

- http://q2a.inf.mit.bme.hu/questions/rete
  - Technikai kérdések
  - HF segítség



- YouTube csatorna: HF eszköz használata

Teendő a héten

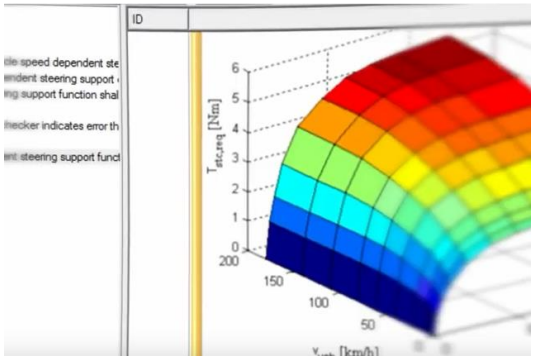
- **Csapatalakítás**
- Határidő: péntek 16:00
  - Nem jelentkező hallgatókat automatikusan beosztjuk
- Űrlap linkje: hírben publikáljuk

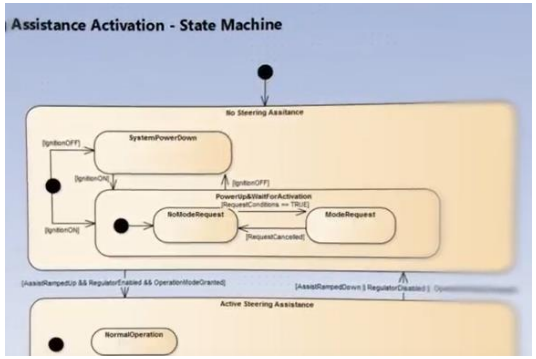
MOTIVÁCIÓ

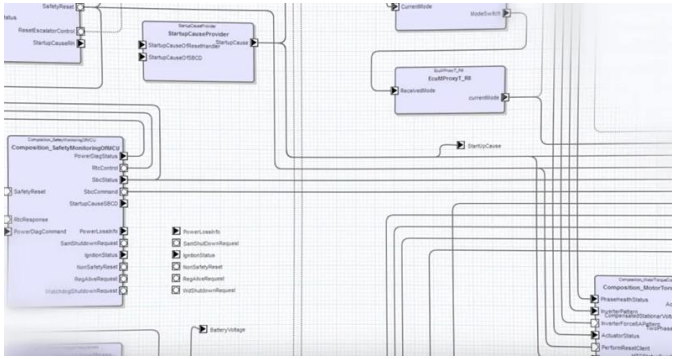
Miért van szükség rendszertervezésre?

Példa modellalapú rendszertervezésre

thyssenkrupp kormányszervó fejlesztése







https://www.youtube.com/watch?v=RND9PpbOcqc&amp=&feature=youtu.be

Hol fontos a rendszertervezés?








Járműipar, közlekedés, űripar, orvosi eszközök, robotika, nukleáris technológia, ipari rendszerek, gyártás…

Continental · Audi · PROLAN · evopro · National Instruments · ThyssenKrupp · BOSCH · GE Healthcare · SIEMENS · KNORR-BREMSE · KUKA

Egy kis motiváció

Applications of Model-Based Engineering at JPL

JPL is applying MBE practice in several projects

- Missions to Europa
  - Europa Clipper
  - Europa Lander
- Missions to Mars
  - Mars 2020
  - InSight
  - Mars Sample Return (MSR)
- Thirty Meter Telescope
- Ground Data Systems
- Psyche
- MAIA

Engineering Products

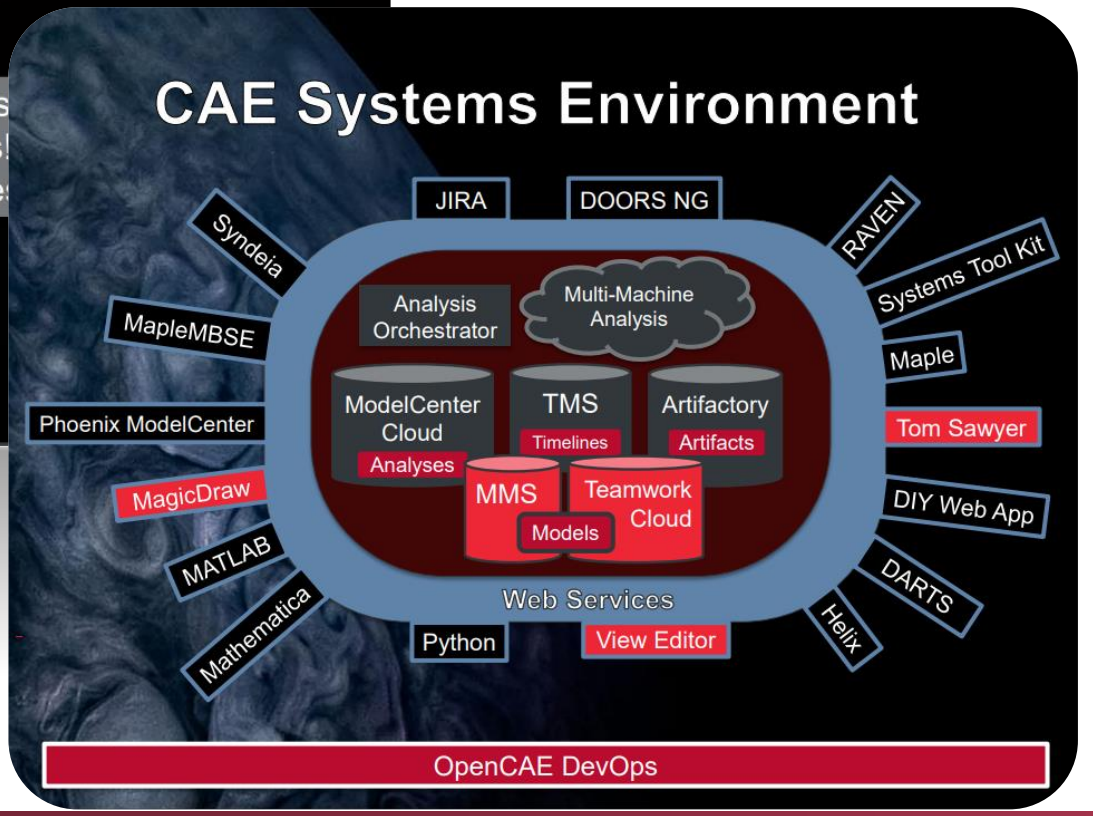
- MELs, PELs
- Resource allocation analysis
- System decomposition,
- Libraries / reusable models

Not jus
missions!
phase

12 April 2018

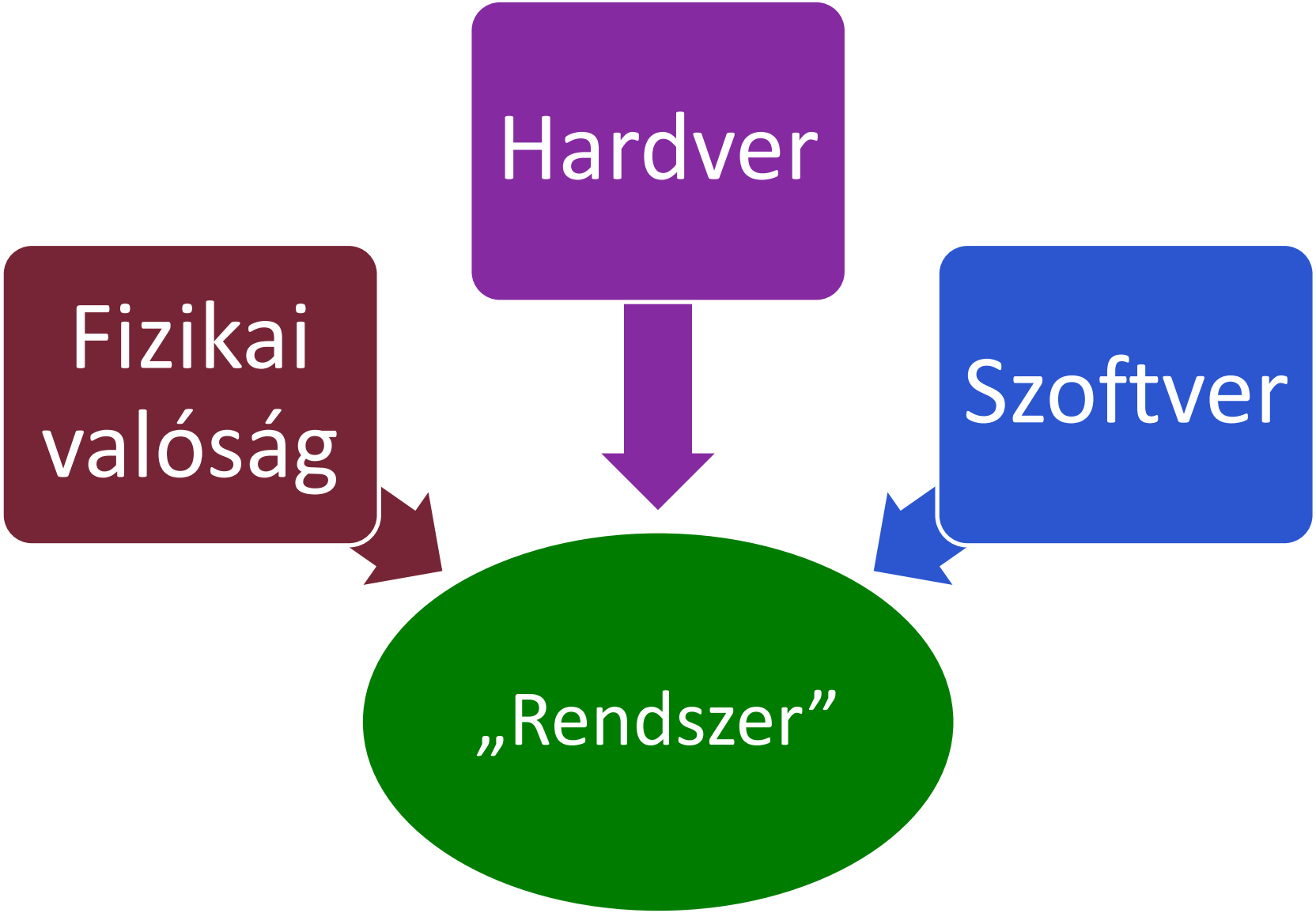
For Planning and Discussion Purposes Only

Jet Propulsion Laboratory
California Institute of Technology



Forrás: https://www.phoenix-int.com/wp-content/uploads/2018/05/Phx2018UC_MBSE_NASA-JPL_Brower-Delp.pdf

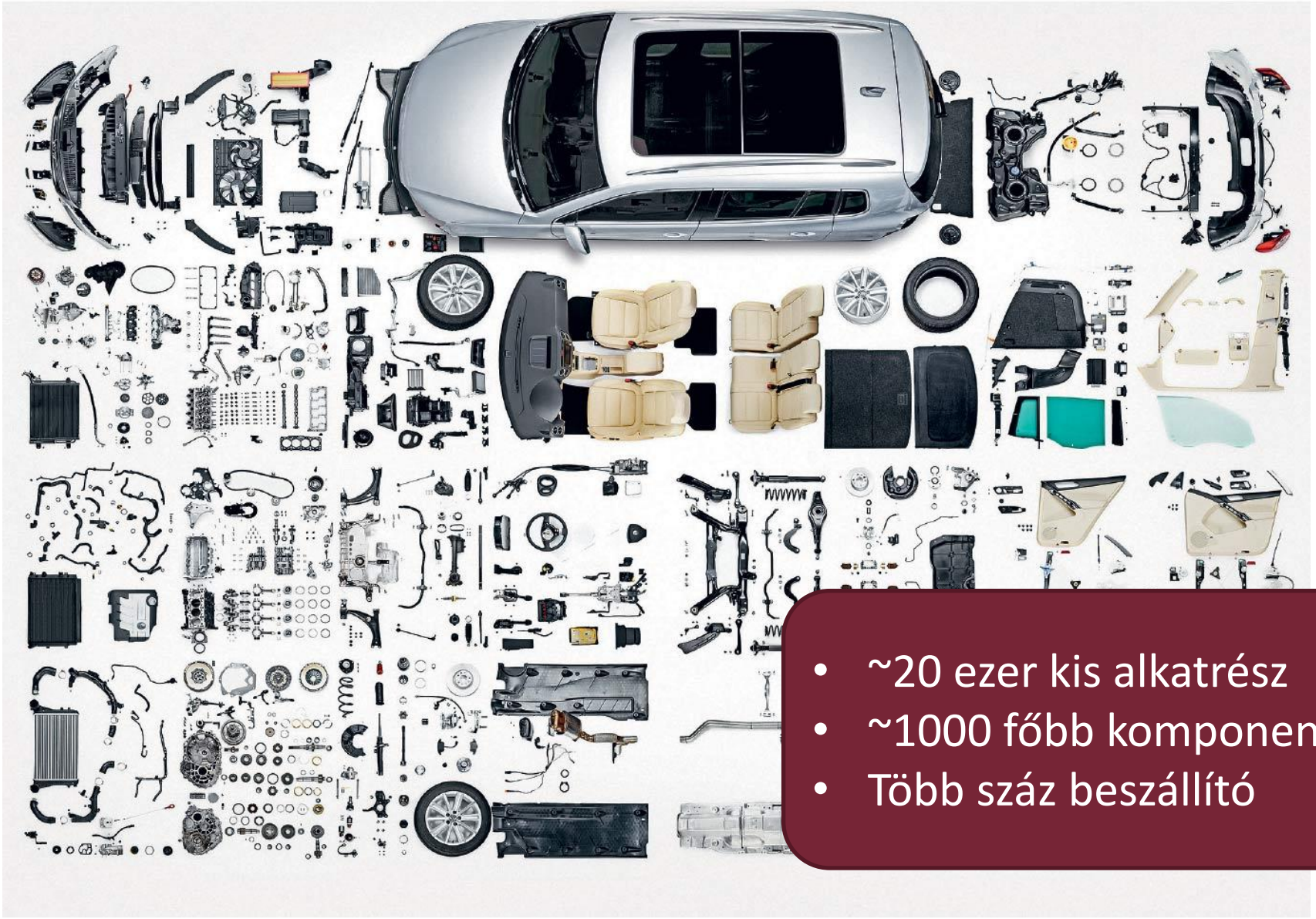
Alkalmazási területek jellegzetességei



Alkalmazási területek jellegzetességei

Valóság korlátai	• Beavatkozás behatárolt • Méret/súly/stb. kényszer
Együttműködés	• Más szakmákkal (pl. gépész) • Sok beszállító, partner
Gyártás	• Prototípus is drága • Euro cent is számít
Biztonság	• (Biztonság)kritikus rendszerek • Engedélyezés, tanúsítás

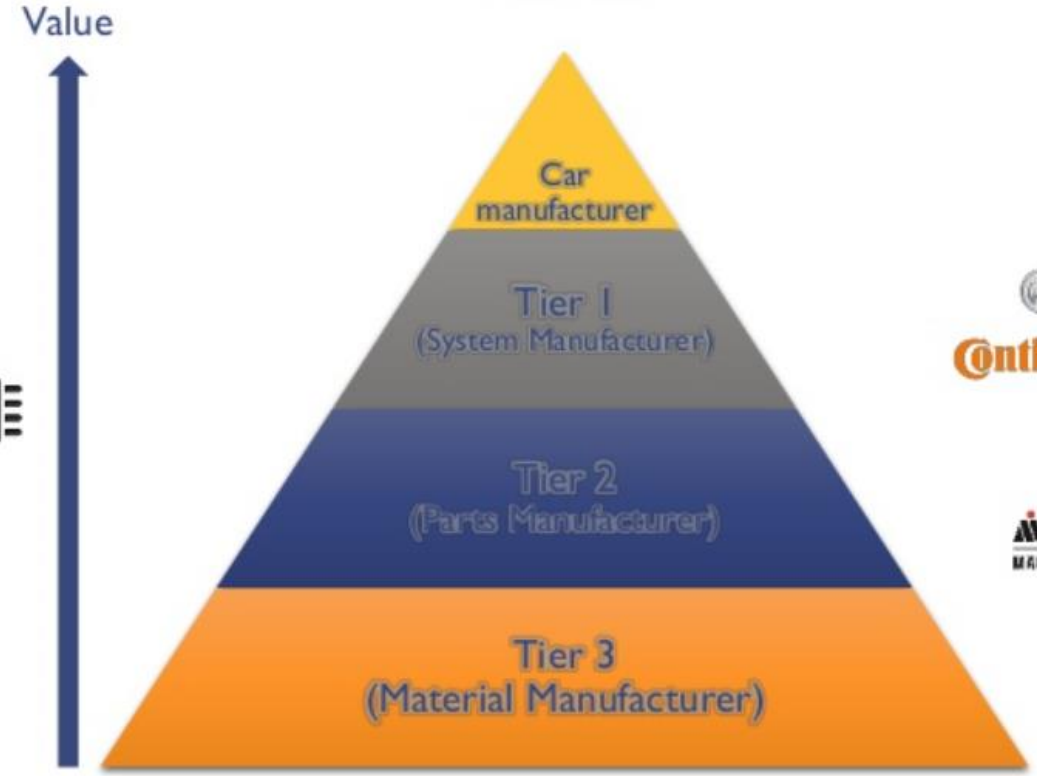
Példa: Egy mai modern autóban…



- ~20 ezer kis alkatrész
- ~1000 főbb komponens
- Több száz beszállító

Forrás: volkswagenag.com

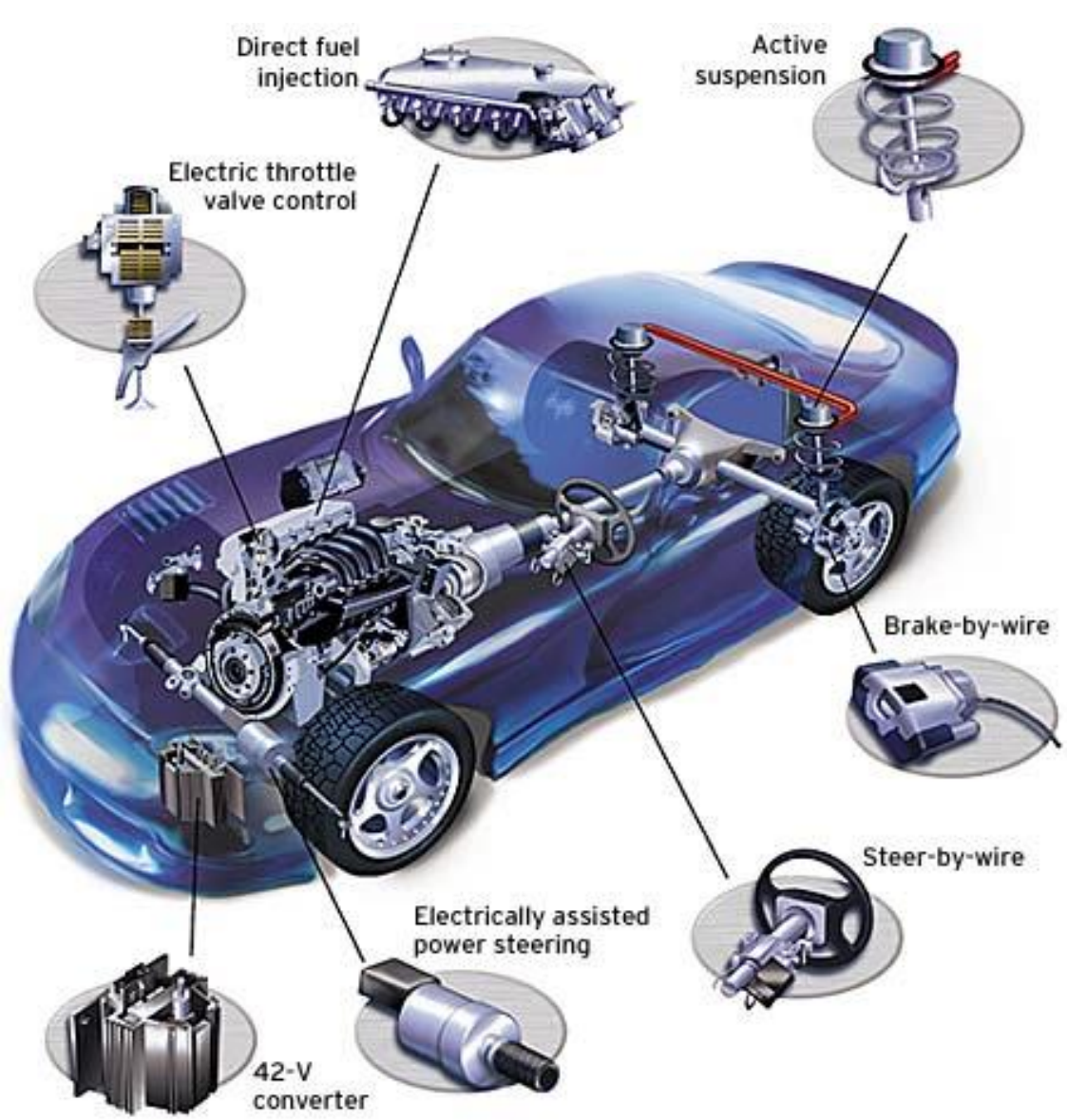
Példa: Egy mai modern autóban…



Autógyártó feladata

- Követelmények megadása
- Komponensek integrálása

Példa: Egy mai modern autóban…



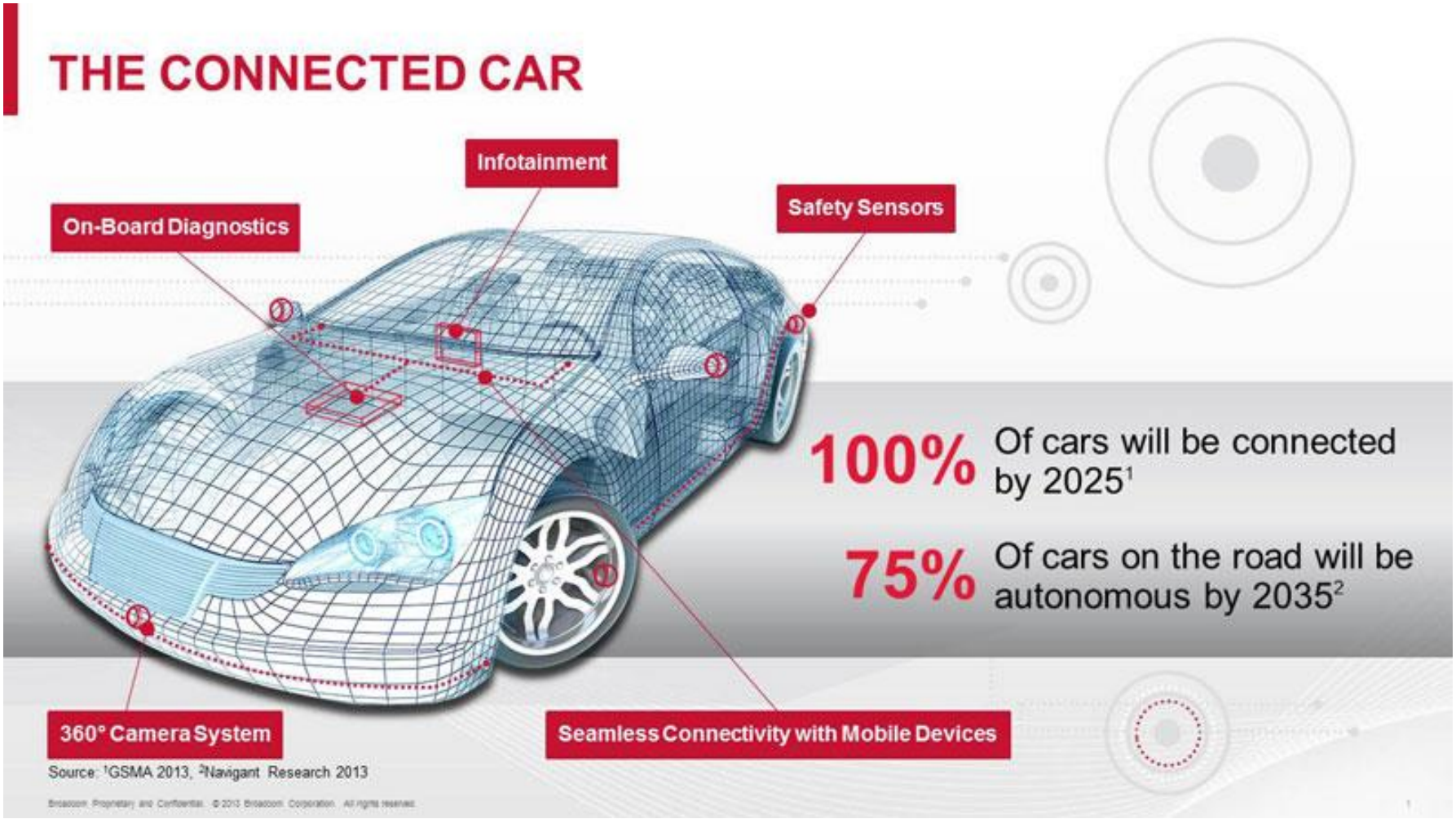
Drive-by-wire: Nincs mechanikus kapcsolat

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

Van viszont helyette

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

… és a jövő autójában



Kiber-fizikai rendszerek

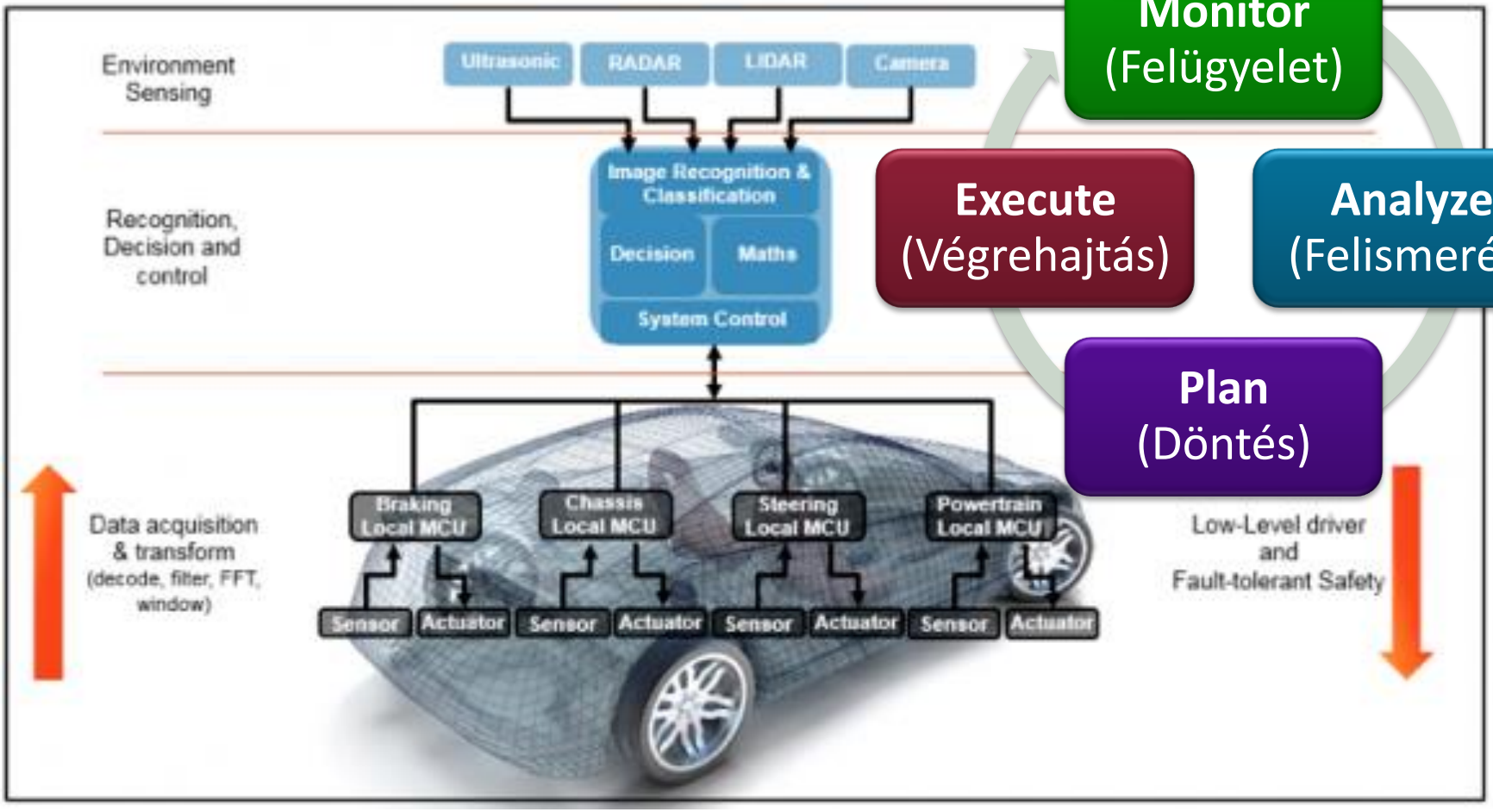
… és a jövő autójában

Változó fizikai környezet

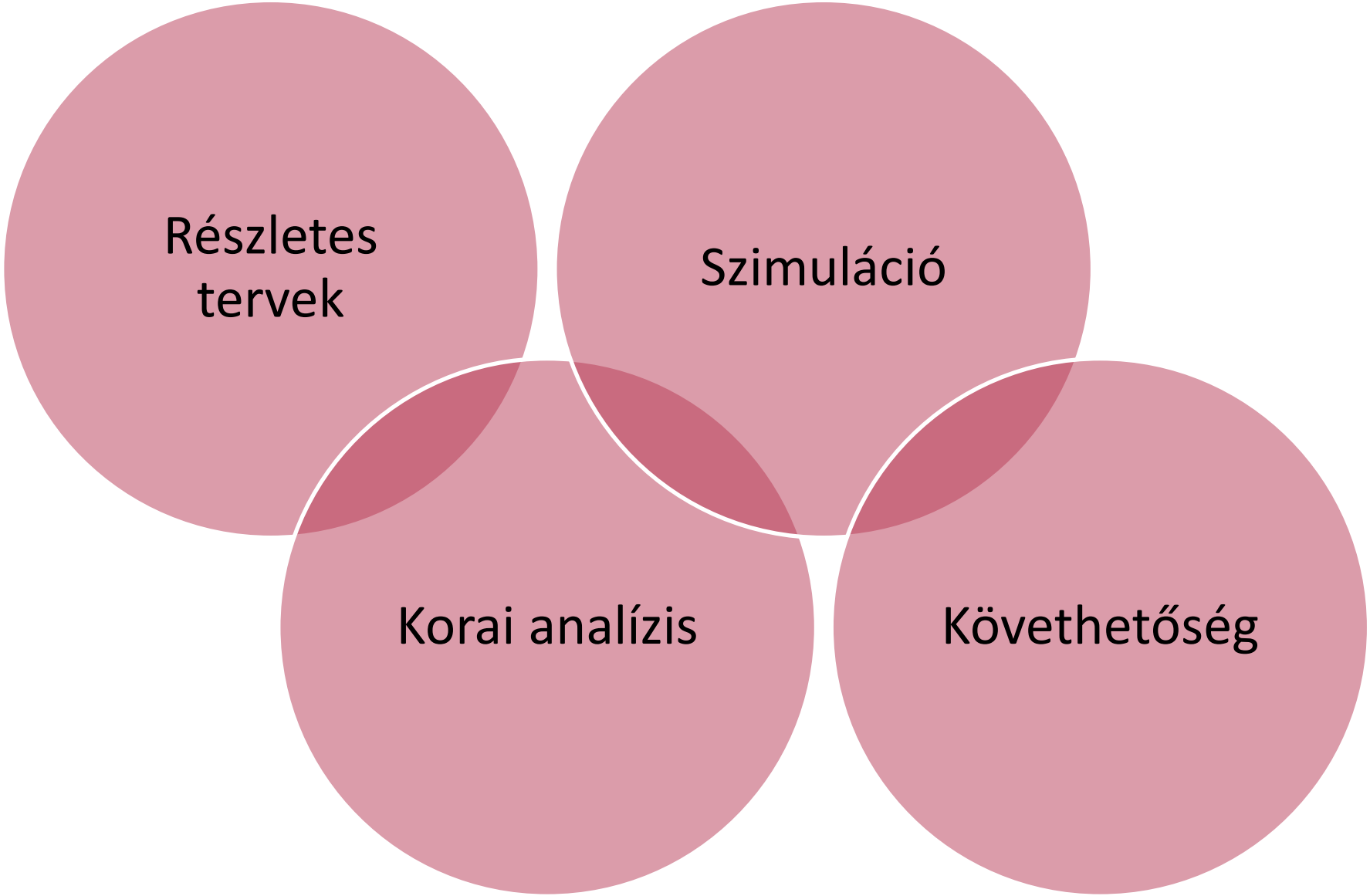
Hálózatba kapcsolt

Dinamikus nyílt rendszer

Biztonságos működés?



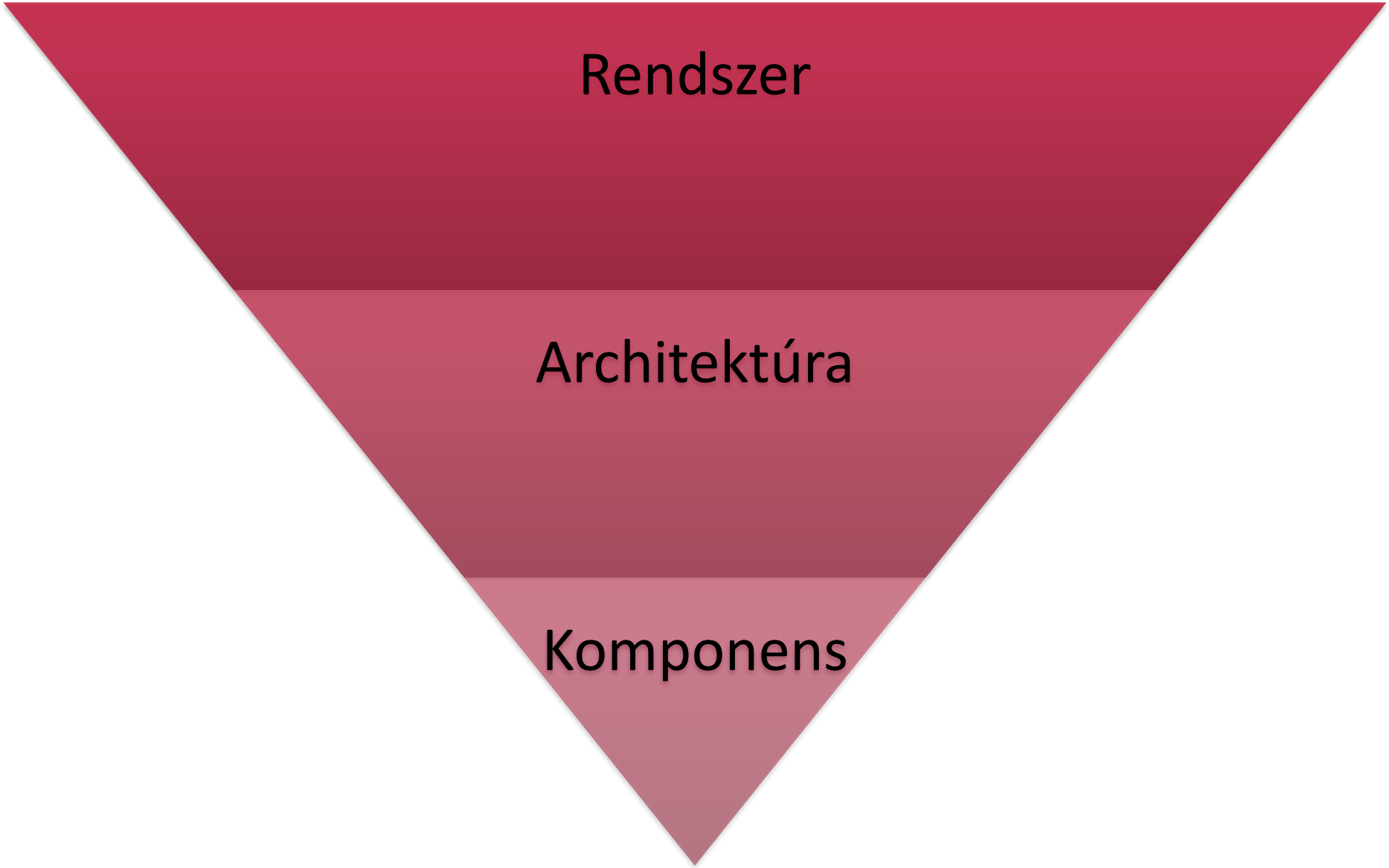
Következmény: rendszerTERVEZÉS



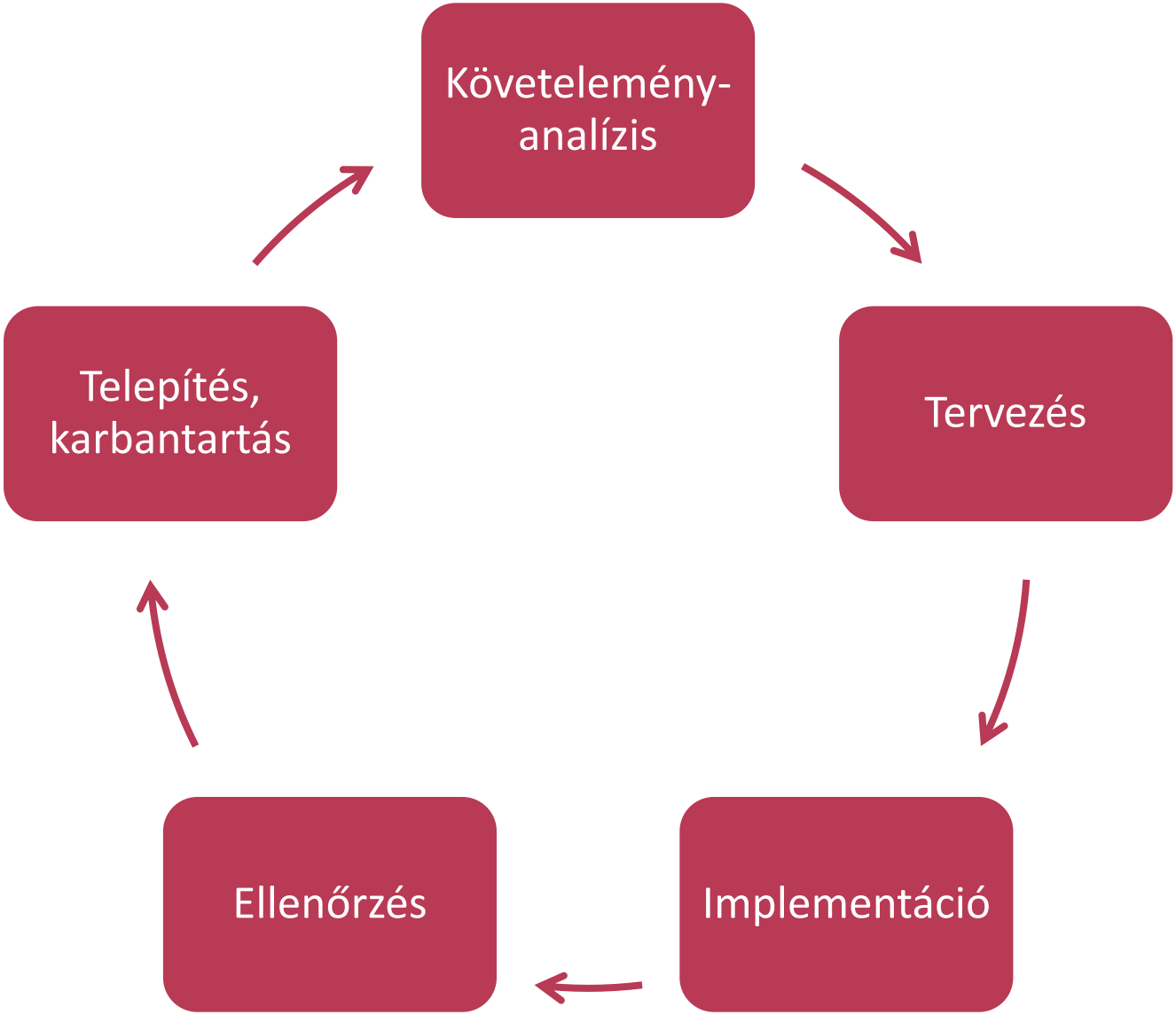
MODELLEK A RENDSZERTERVEZÉSBEN

Hol és miért használunk modelleket?

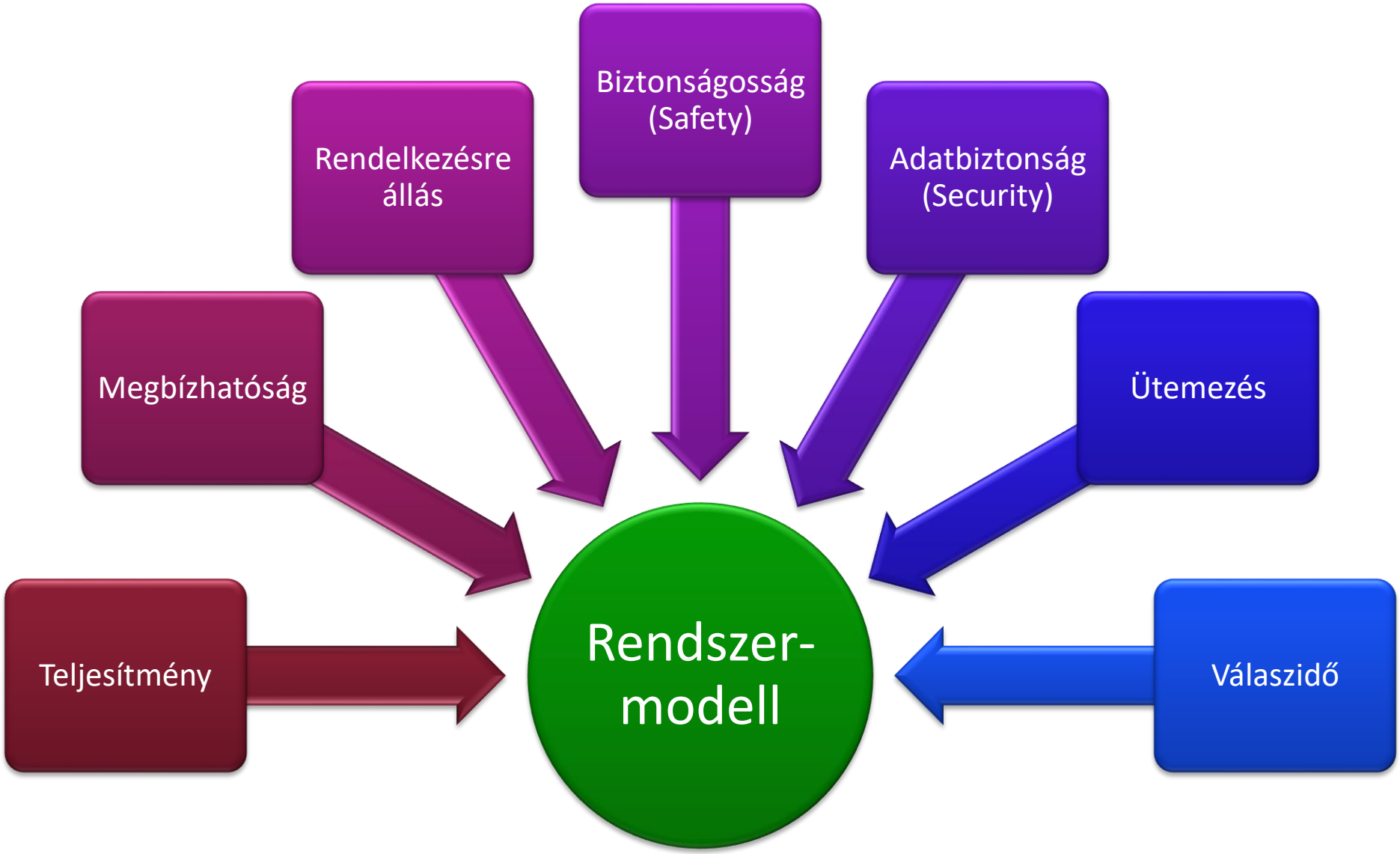
Különböző absztrakciós szinteken…



Különböző tervezési fázisokban…



Többféle nézőpontból…



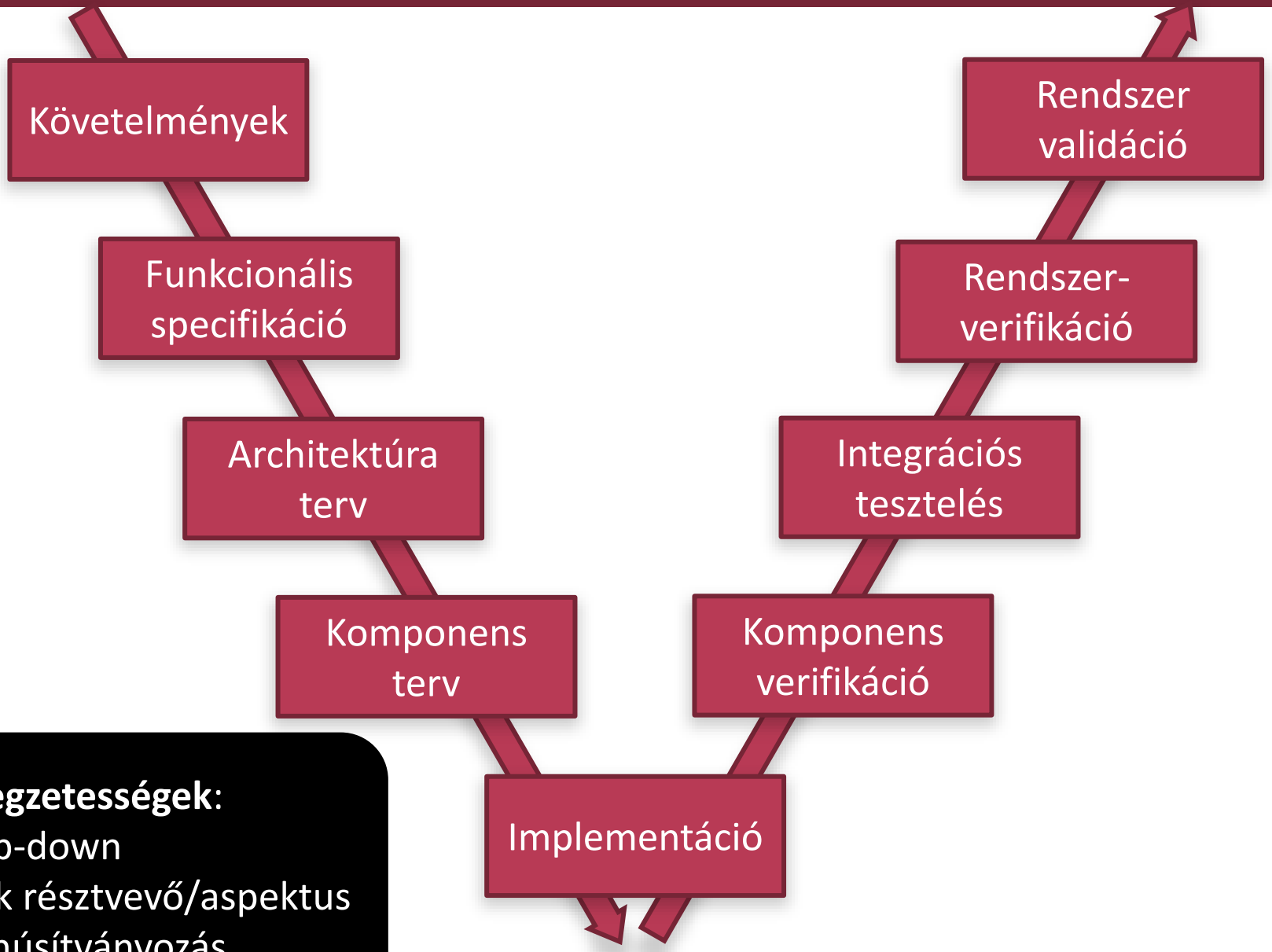
Többféle célból…

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 RENDSZERTERVEZÉS FOLYAMATA

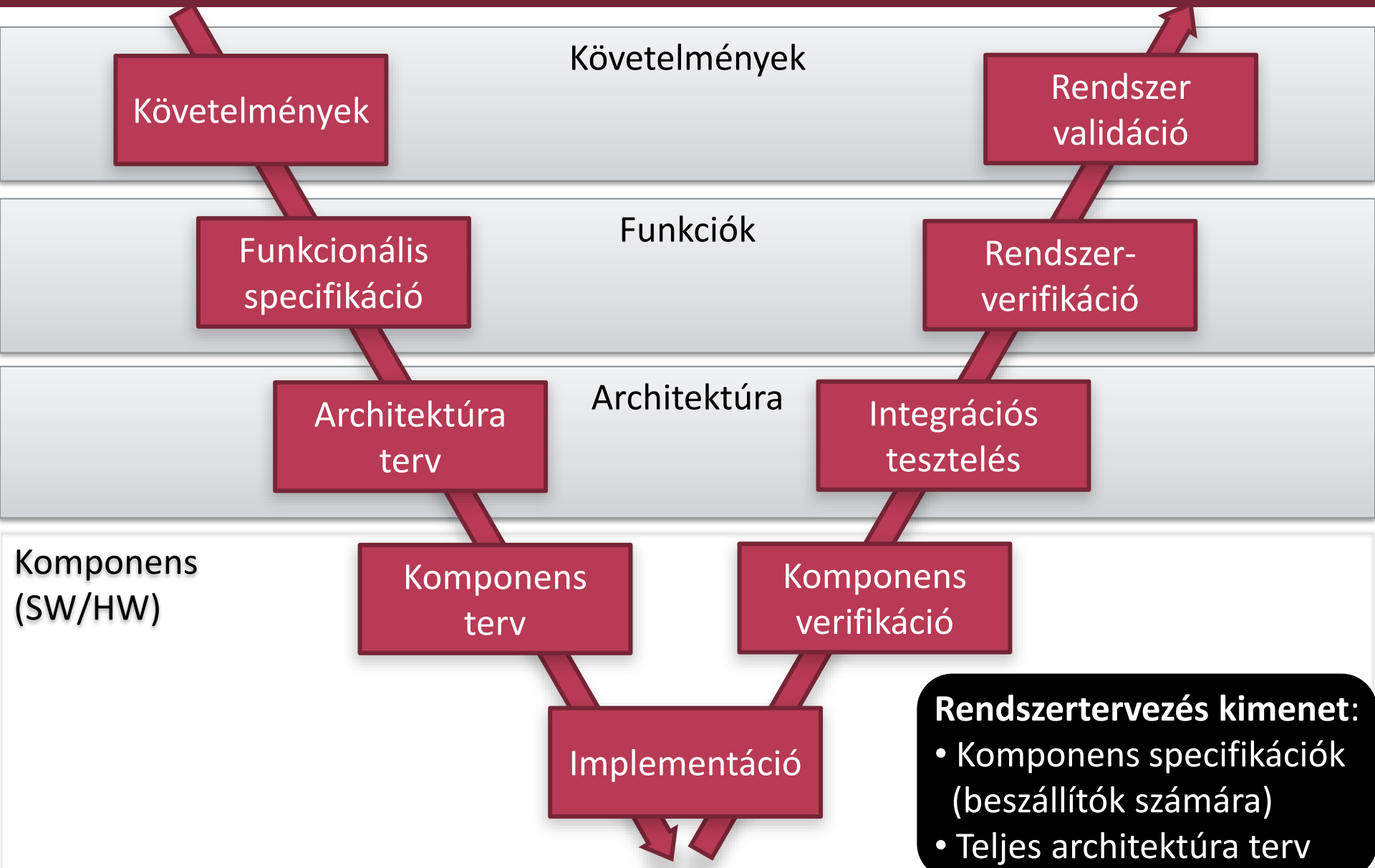
Milyen tipikus lépésekből áll a rendszertervezés?

V-modell: Kritikus rendszerek



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

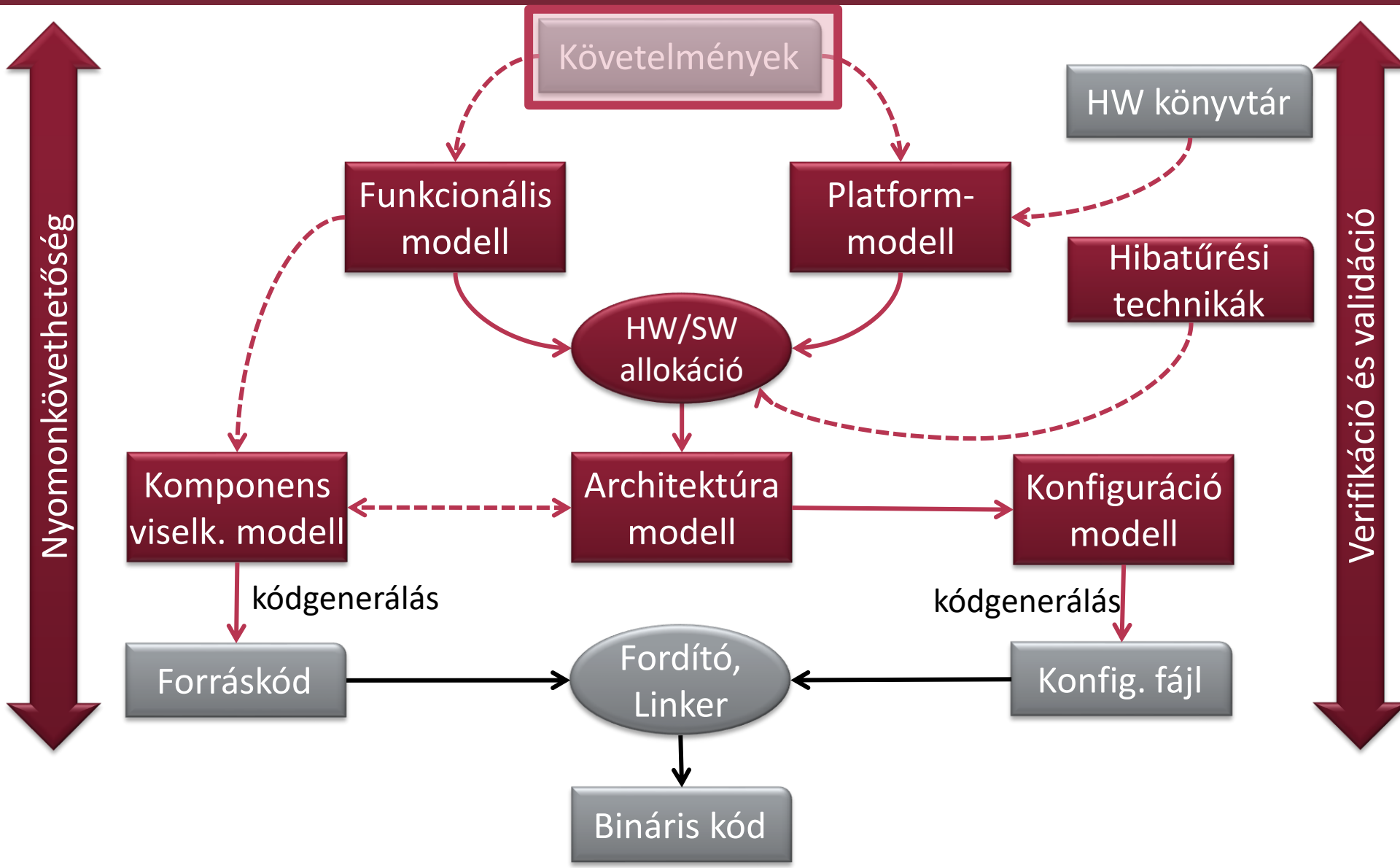
A rendszertervezés feladata



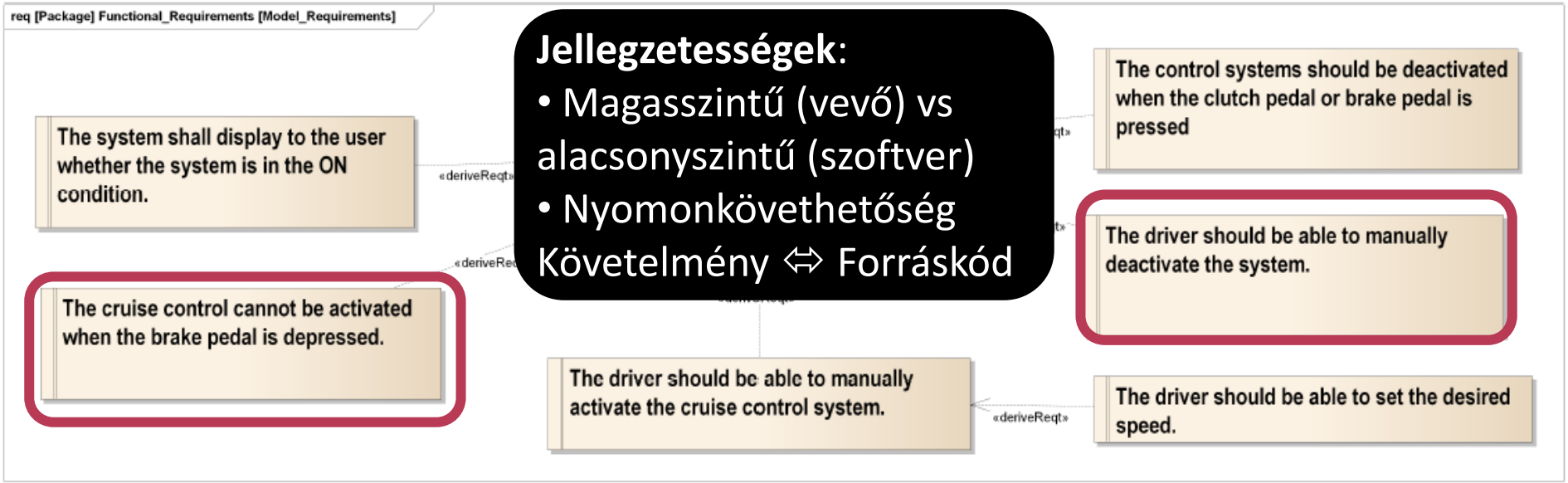
Rendszertervezés kimenet:

- Komponens specifikációk (beszállítók számára)
- Teljes architektúra terv

Platform-alapú rendszertervezés



Követelmények



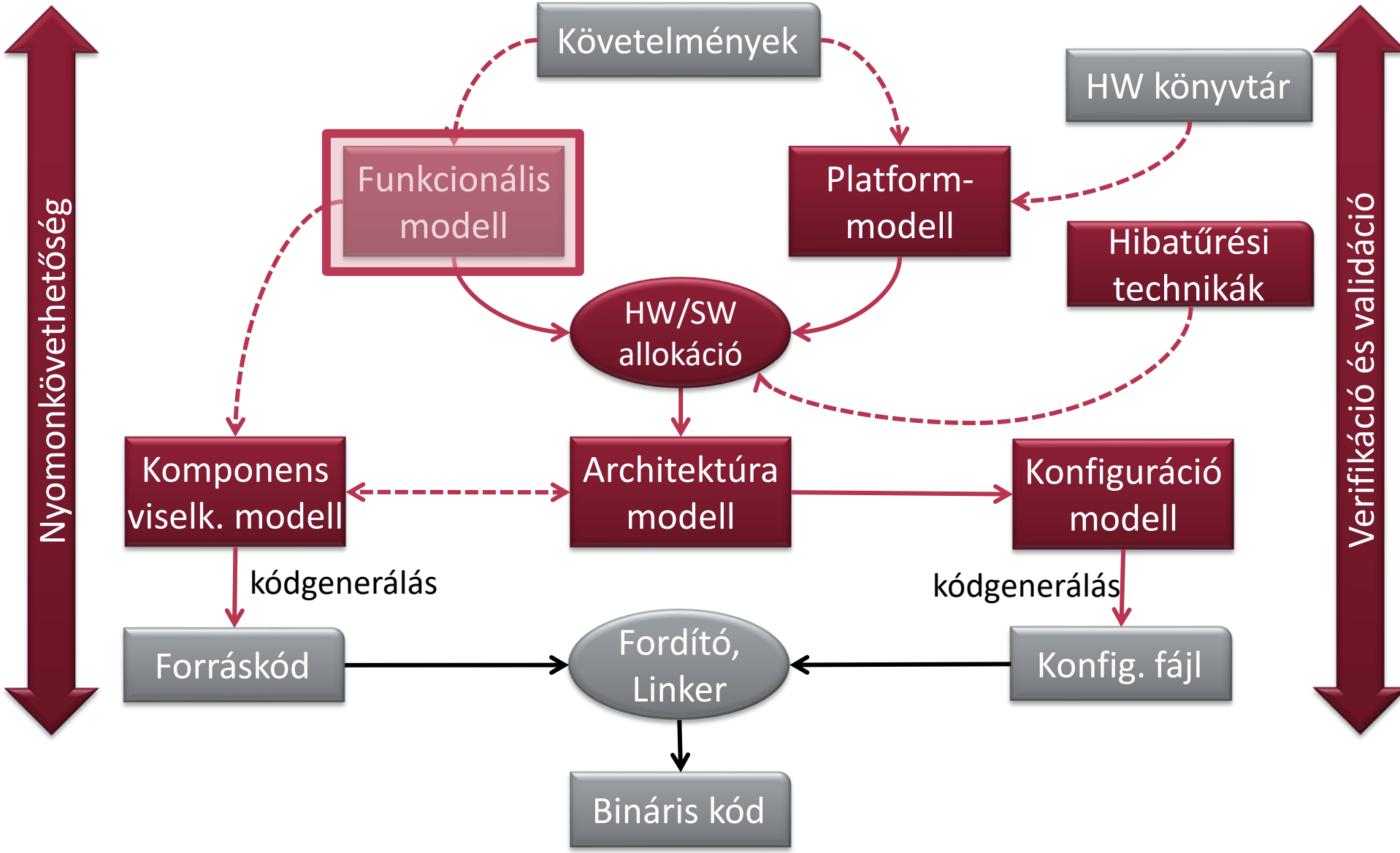
Példa

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

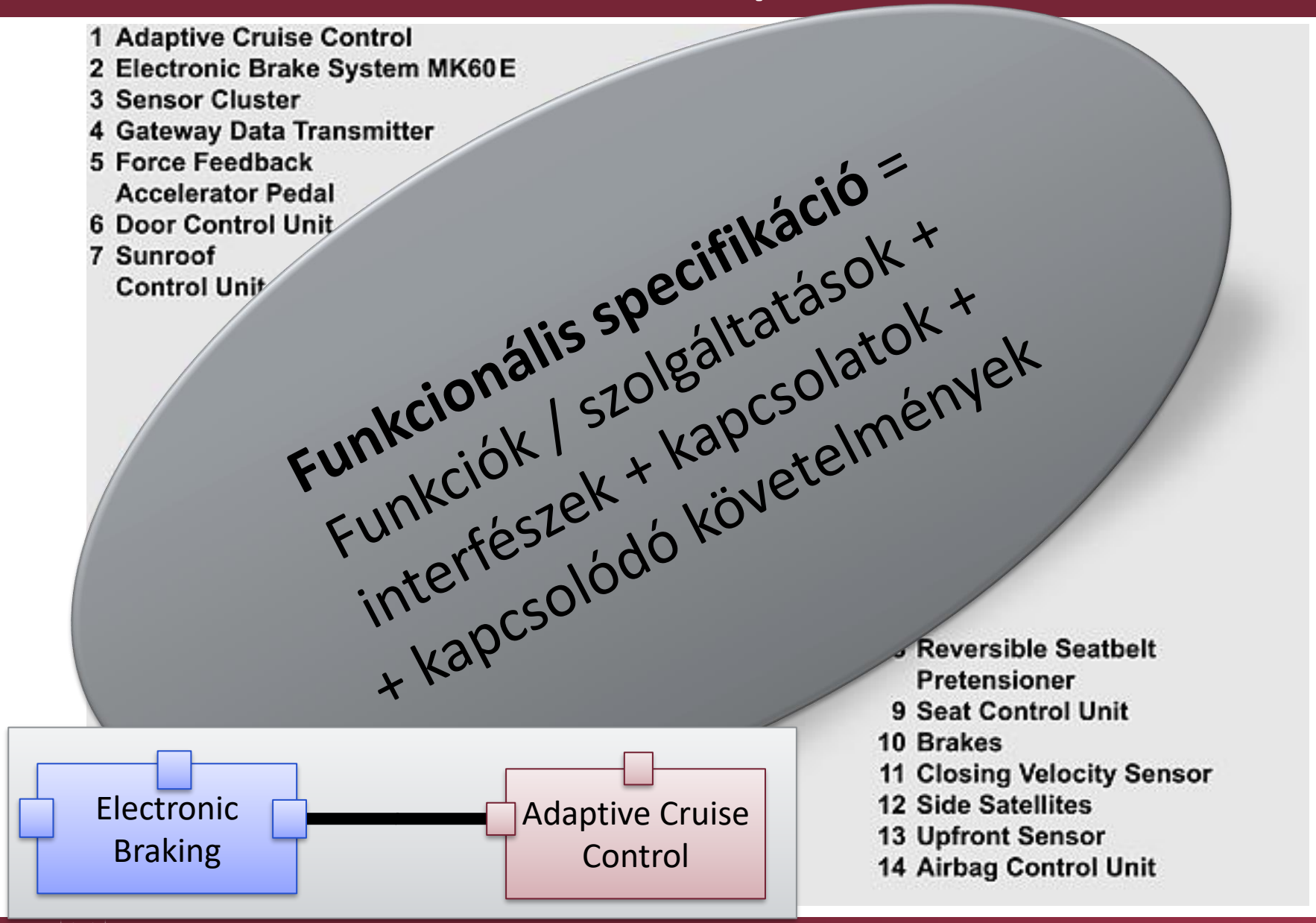
- REMO:
  - Követelmények modellezése
  - Funkcionális / nemfunkcionális
  - Finomítás / Konfliktus
- RETE (UML / SysML):
  - Requirements diagram
  - Use case diagram

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

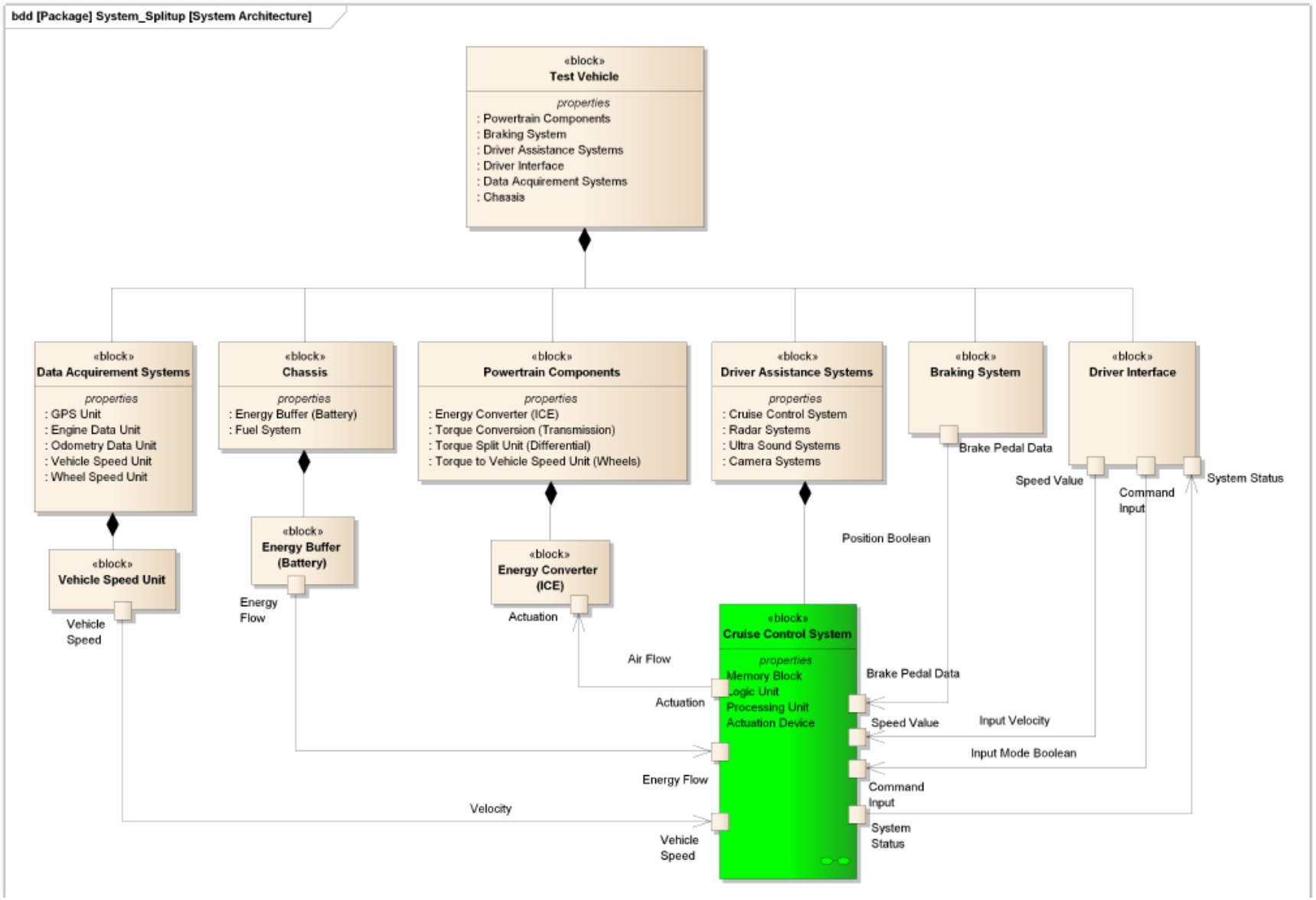
Platform-alapú rendszertervezés



Funkcionális specifikáció

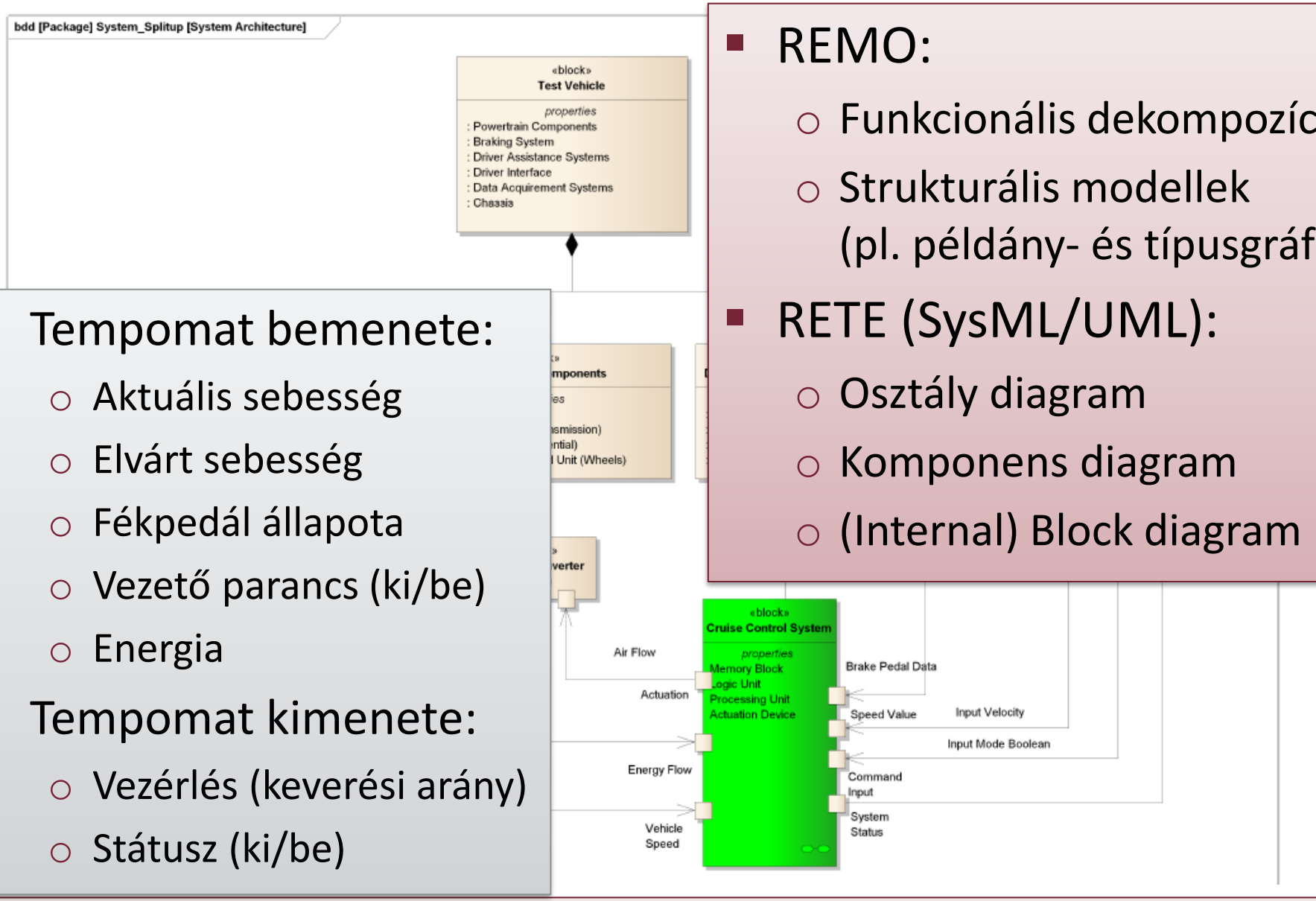


Példa: Funkcionális specifikáció



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

Példa: Funkcionális specifikáció

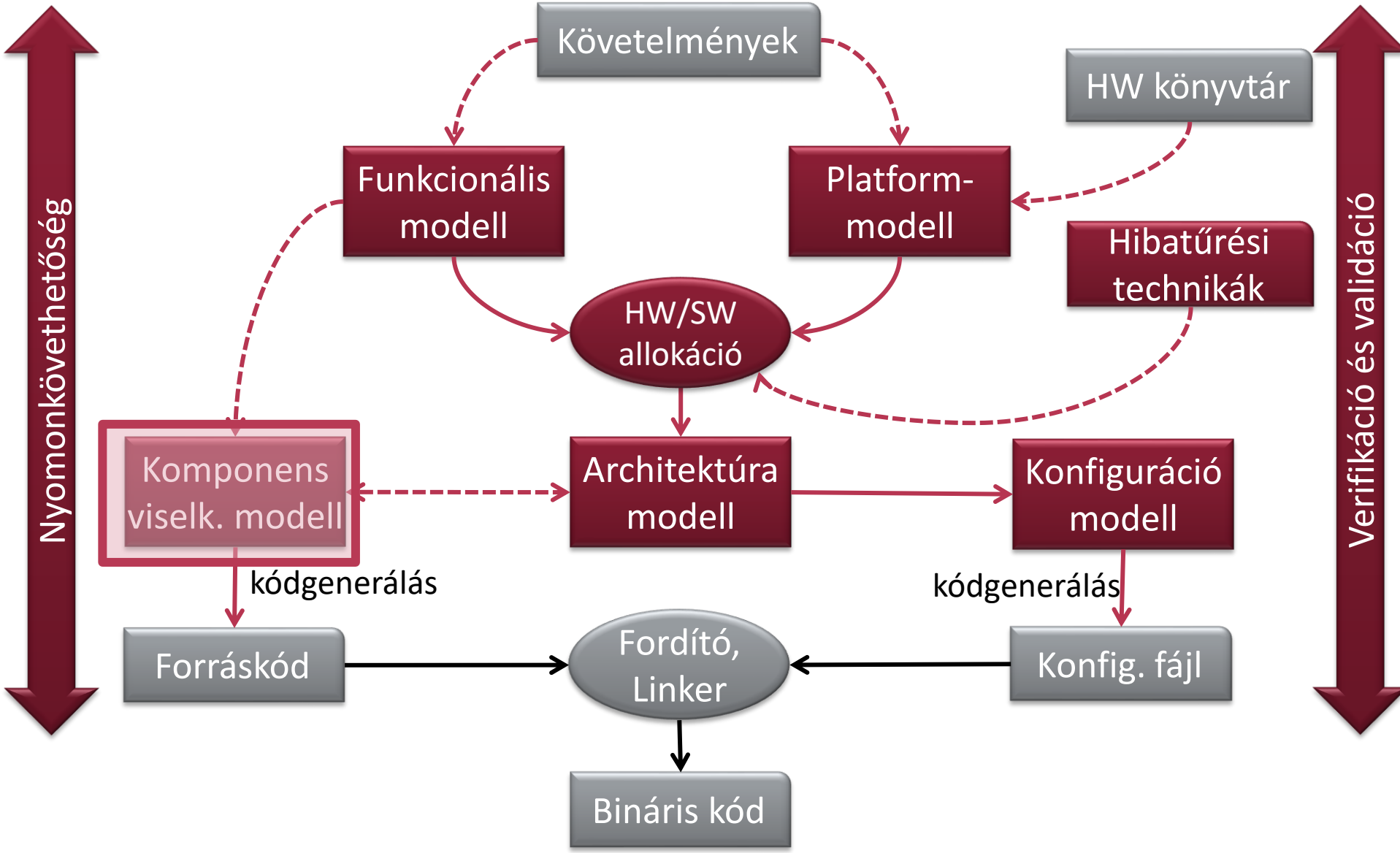


- Tempomat bemenete:
  - Aktuális sebesség
  - Elvárt sebesség
  - Fékpedál állapota
  - Vezető parancs (ki/be)
  - Energia
- Tempomat kimenete:
  - Vezérlés (keverési arány)
  - Státusz (ki/be)

- 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

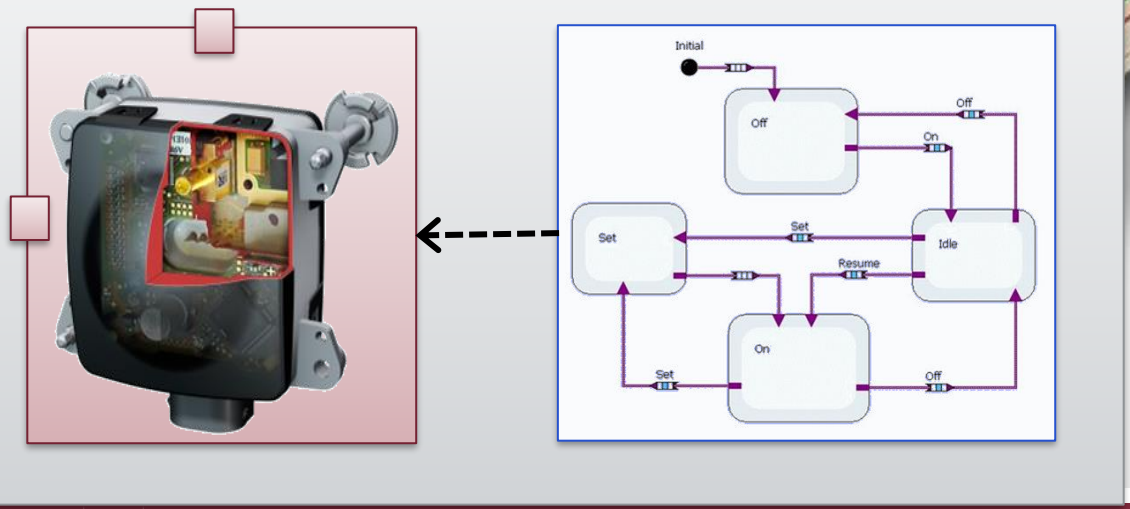
Platform-alapú rendszertervezés



Komponens terv

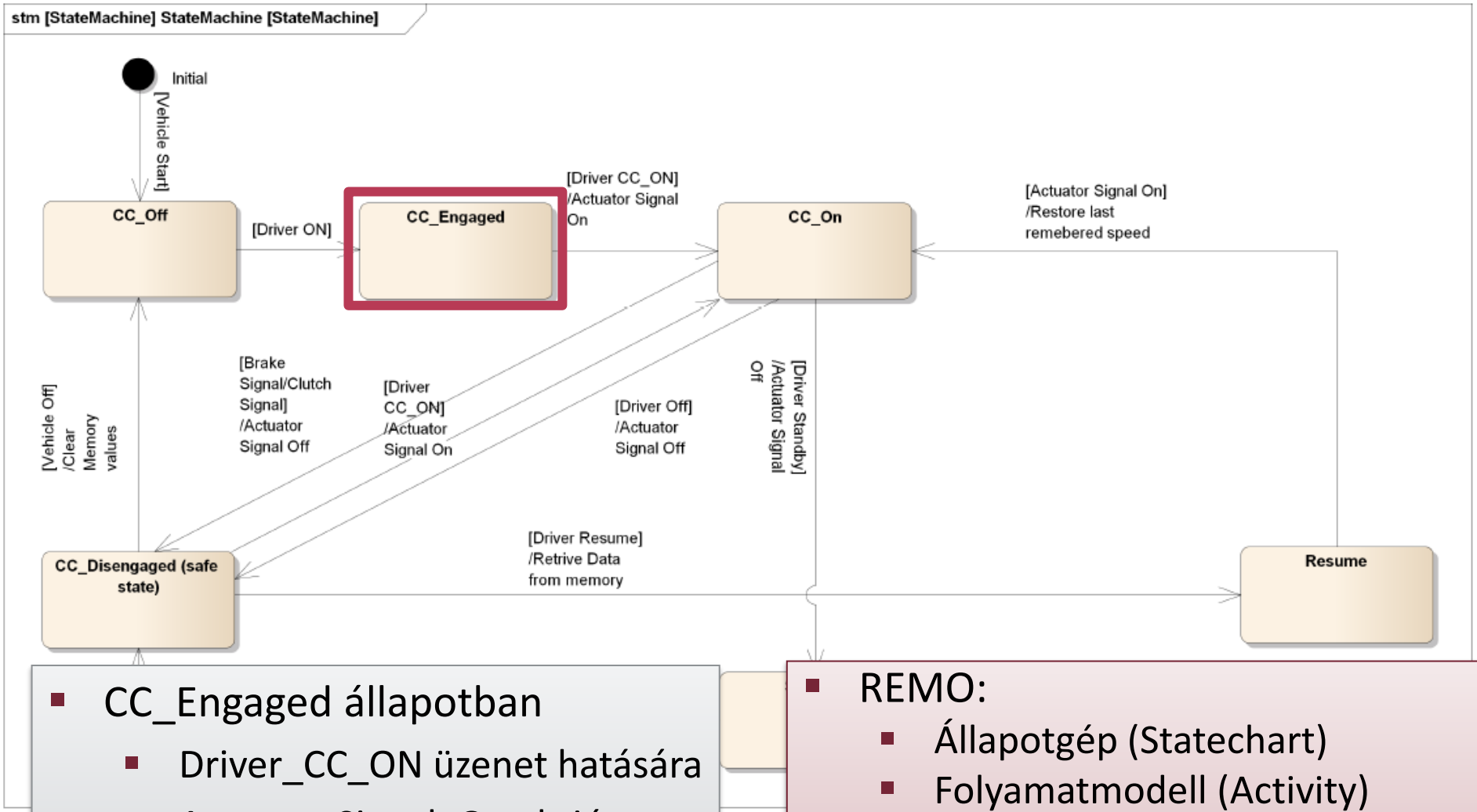
1 Adaptive Cruise Control
2 Electronic Brake System MK60E
3 Sensor Cluster
4 Gateway Data Transmitter
5 Force Feedback Accelerator Pedal
6 Door Control Unit
7 Sunroof Control Unit

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

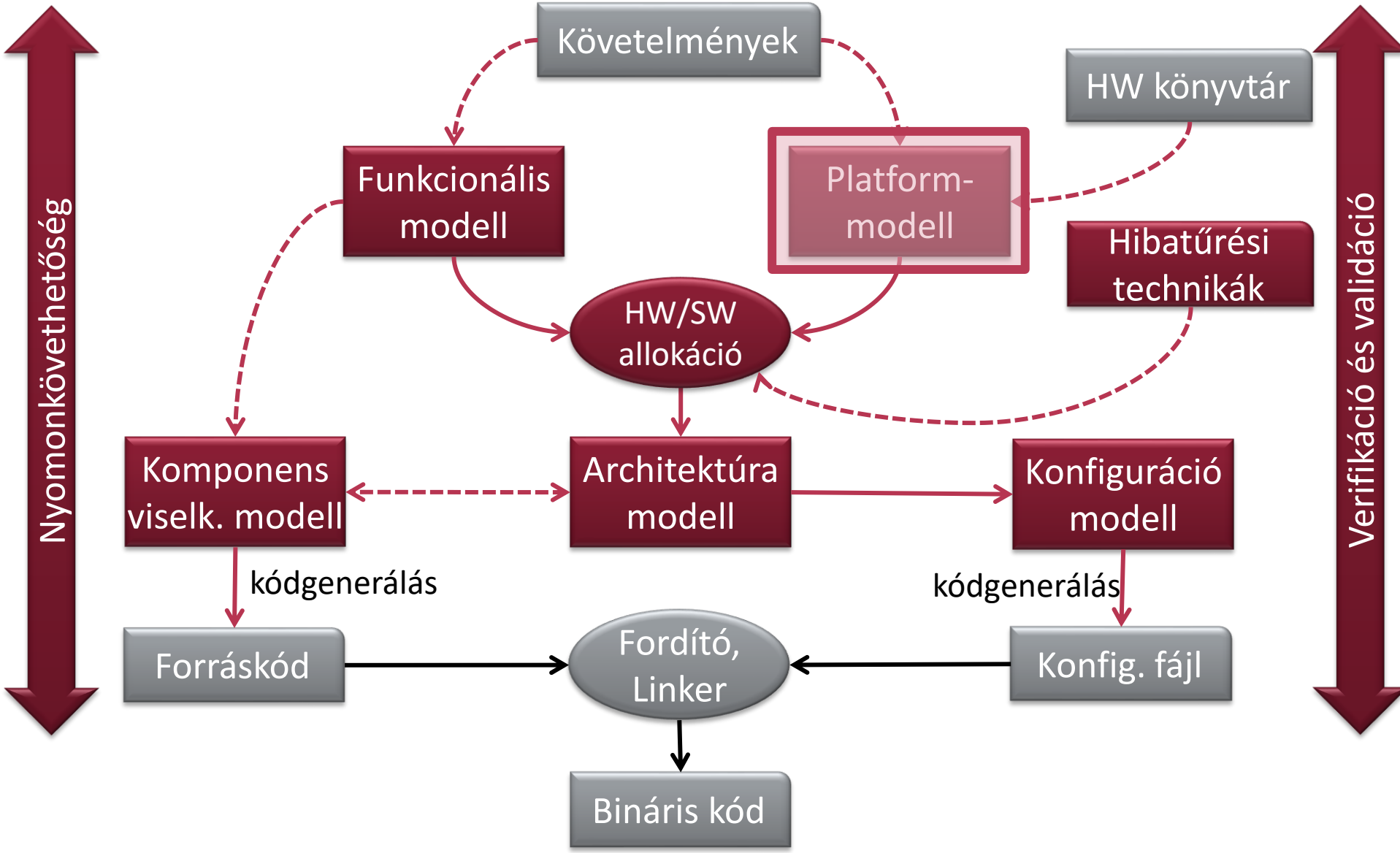
Példa: Komponens belső viselkedés



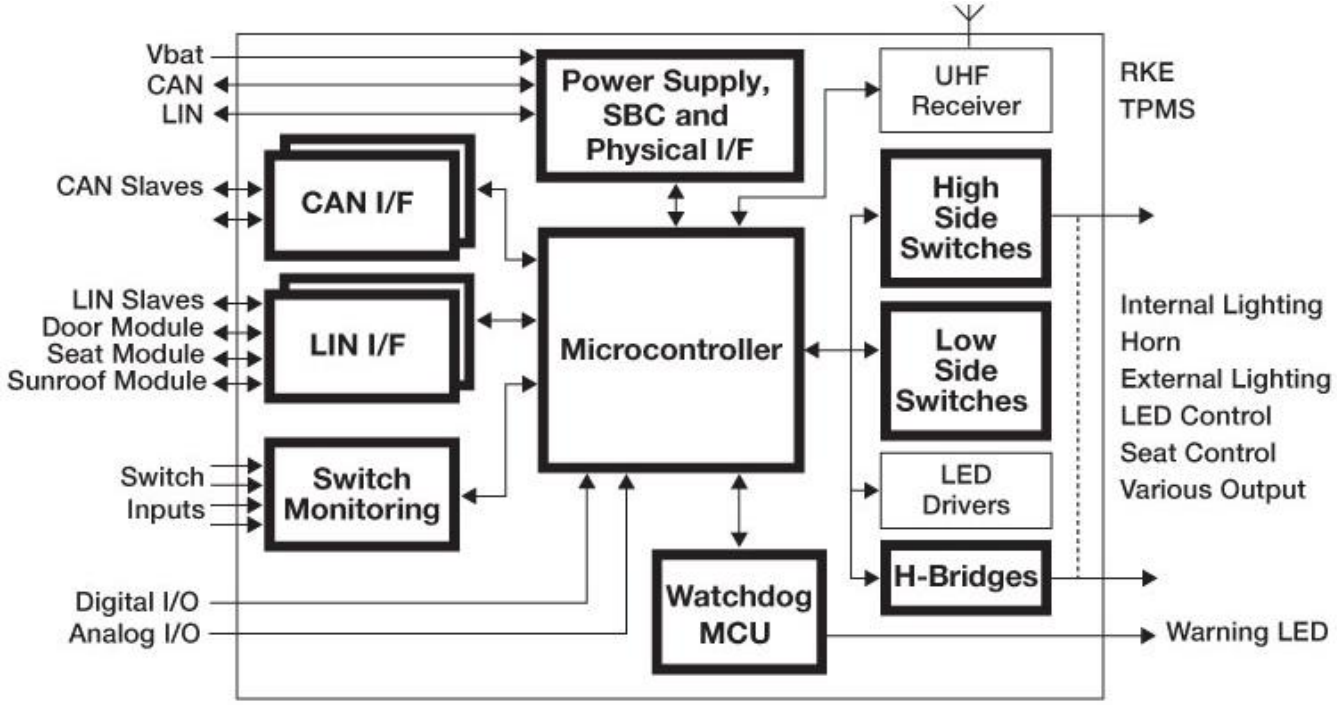
- CC_Engaged állapotban
  - Driver_CC_ON üzenet hatására
  - Actuator Signal_On akció
  - CC_On állapotba lépés

- REMO:
  - Állapotgép (Statechart)
  - Folyamatmodell (Activity)
- RETE (UML/SysML)
  - Statechart, Activity diagram
  - Sequence diagram

Platform-alapú rendszertervezés



Platform modellezés

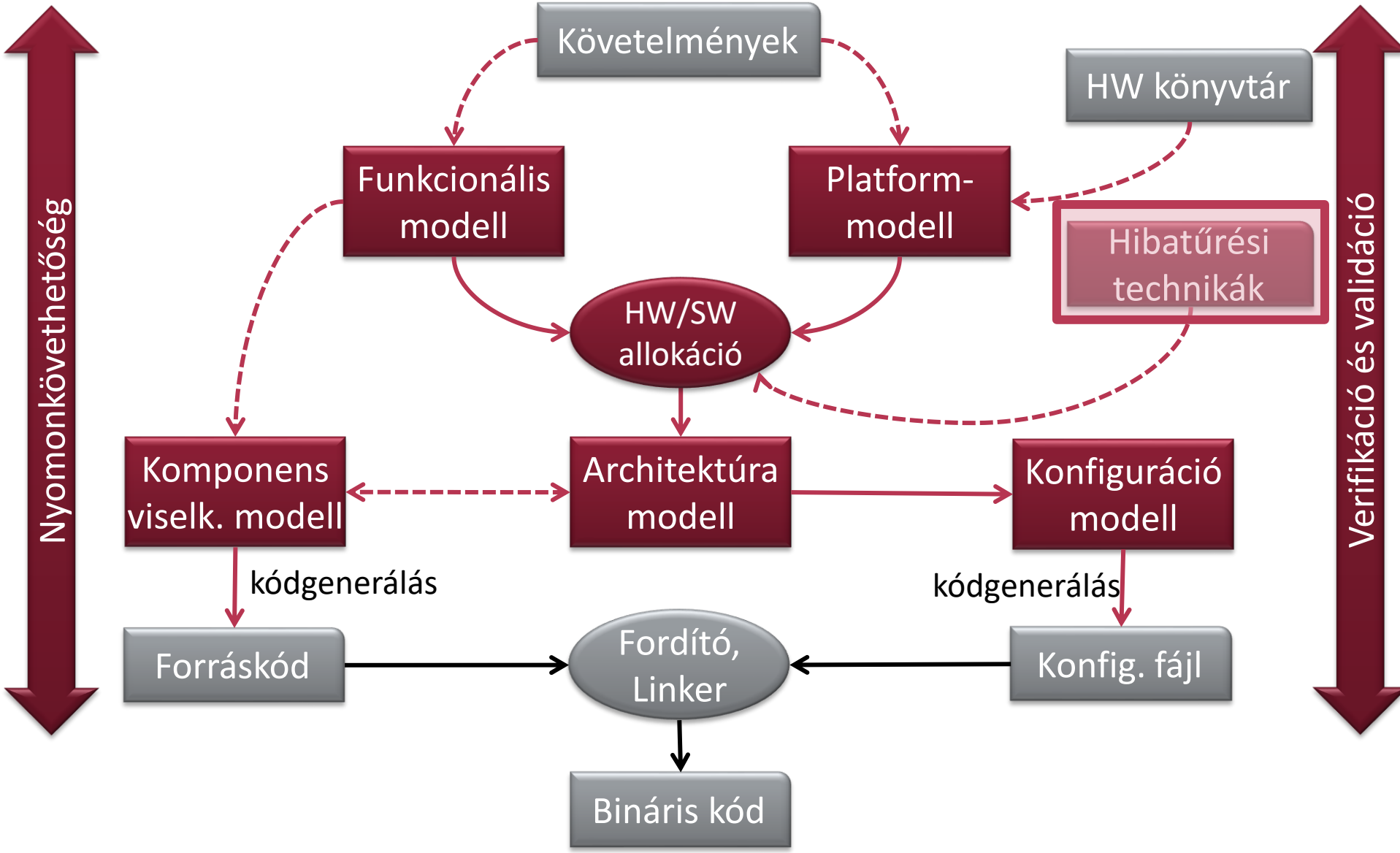


Példa

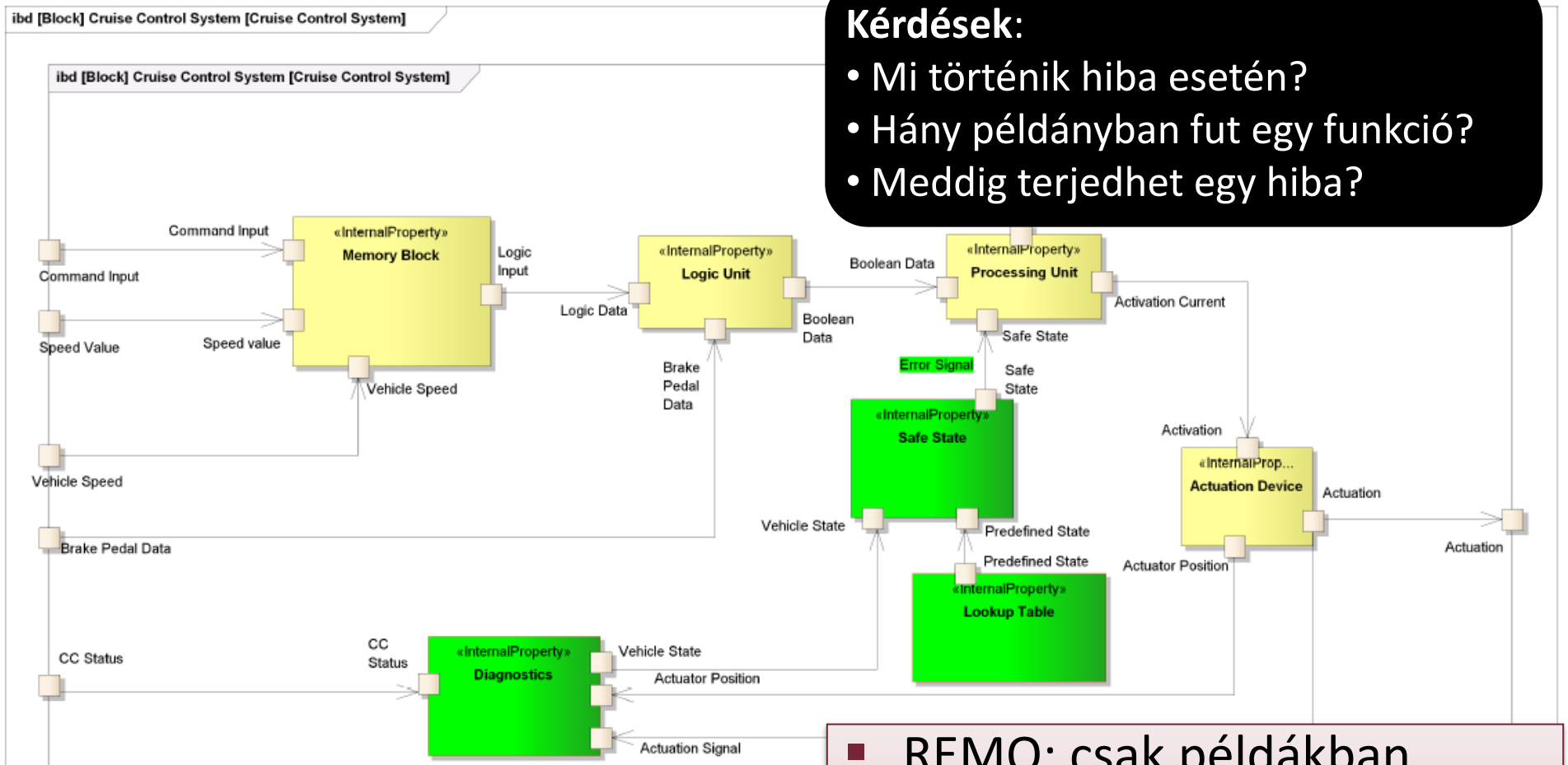
- Mikrovezérlő
- Kapcsolat szabványos interfészekkel (CAN, LIN)
- Watchdog processzor folyamatos ellenőrzésre

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

Platform-alapú rendszertervezés



Biztonságra tervezés / Hibatűrés



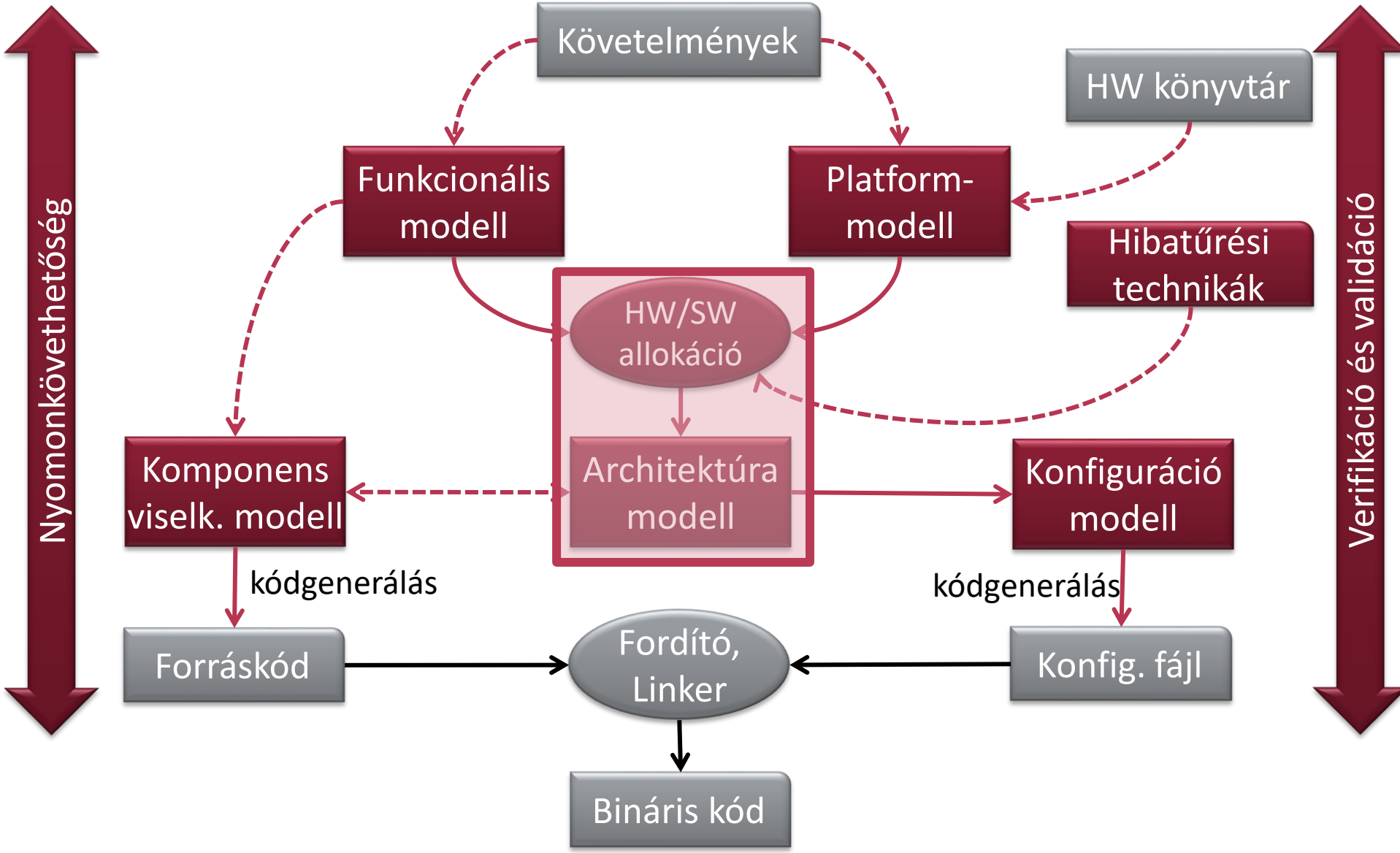
Kérdések:

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

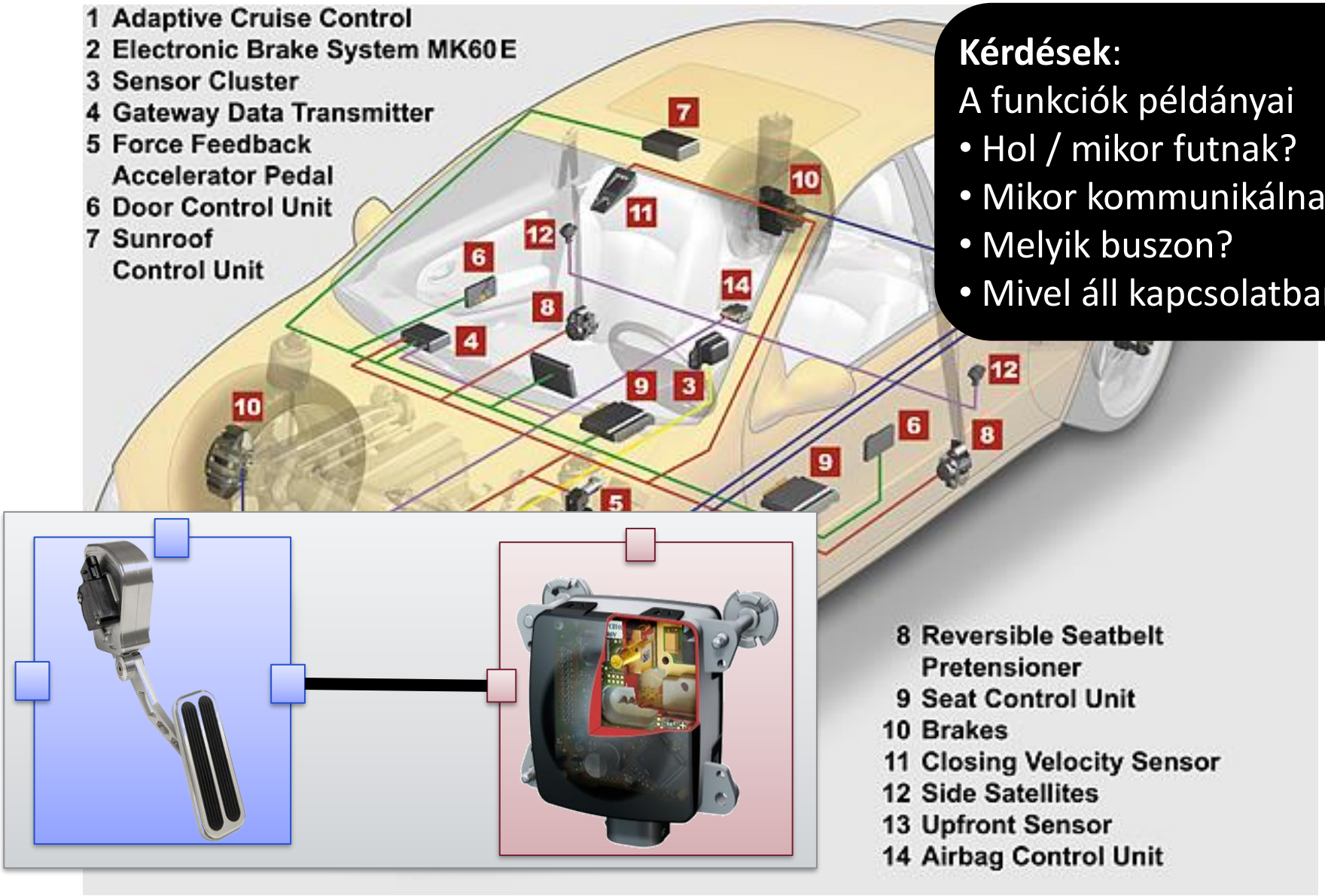
- Tempomat-kimenet monitorozása
- Összehasonlítás tárolt adatokkal
- Jelentős eltérés esetén hibajelzés
- Hibajelzés esetén deaktiválás

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

Platform-alapú rendszertervezés



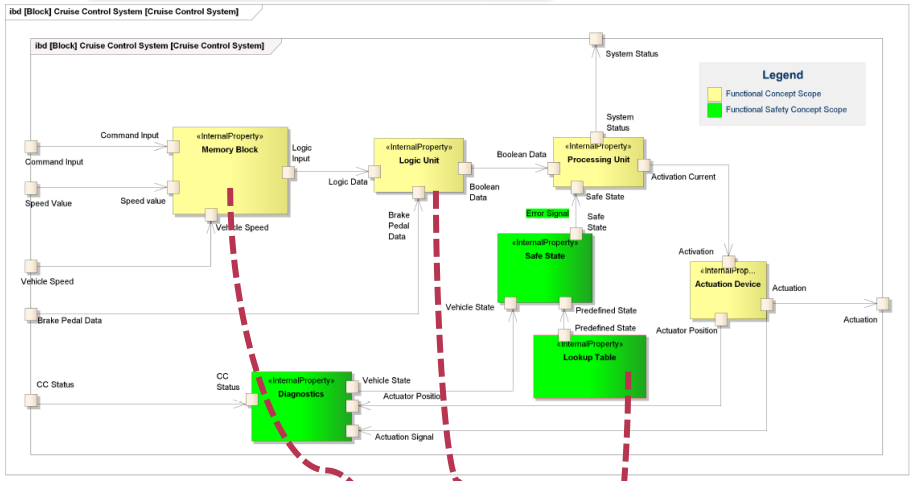
Architektúra terv (aka. Rendszermodell)



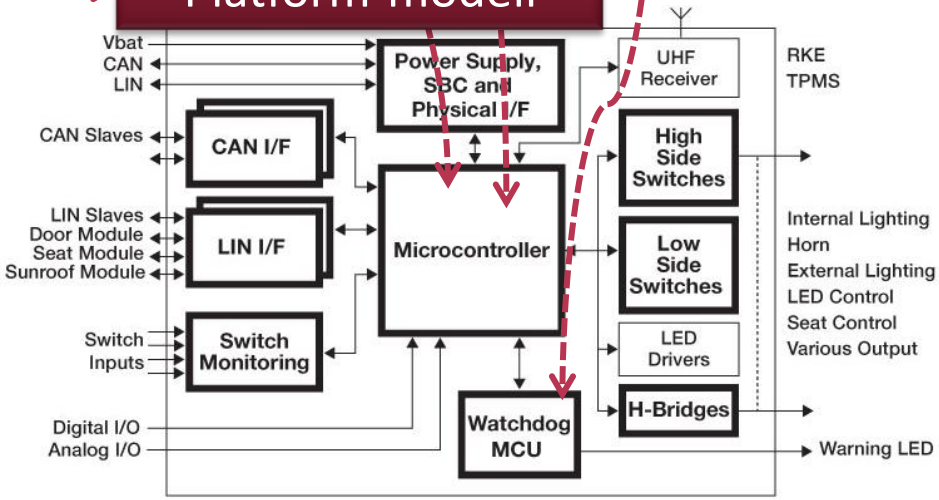
Kérdések:
A funkciók példányai
- Hol / mikor futnak?
- Mikor kommunikálnak?
- Melyik buszon?
- Mivel áll kapcsolatban?

Példa: Architektúra terv (Rendszermodell)

Funkcionális modell



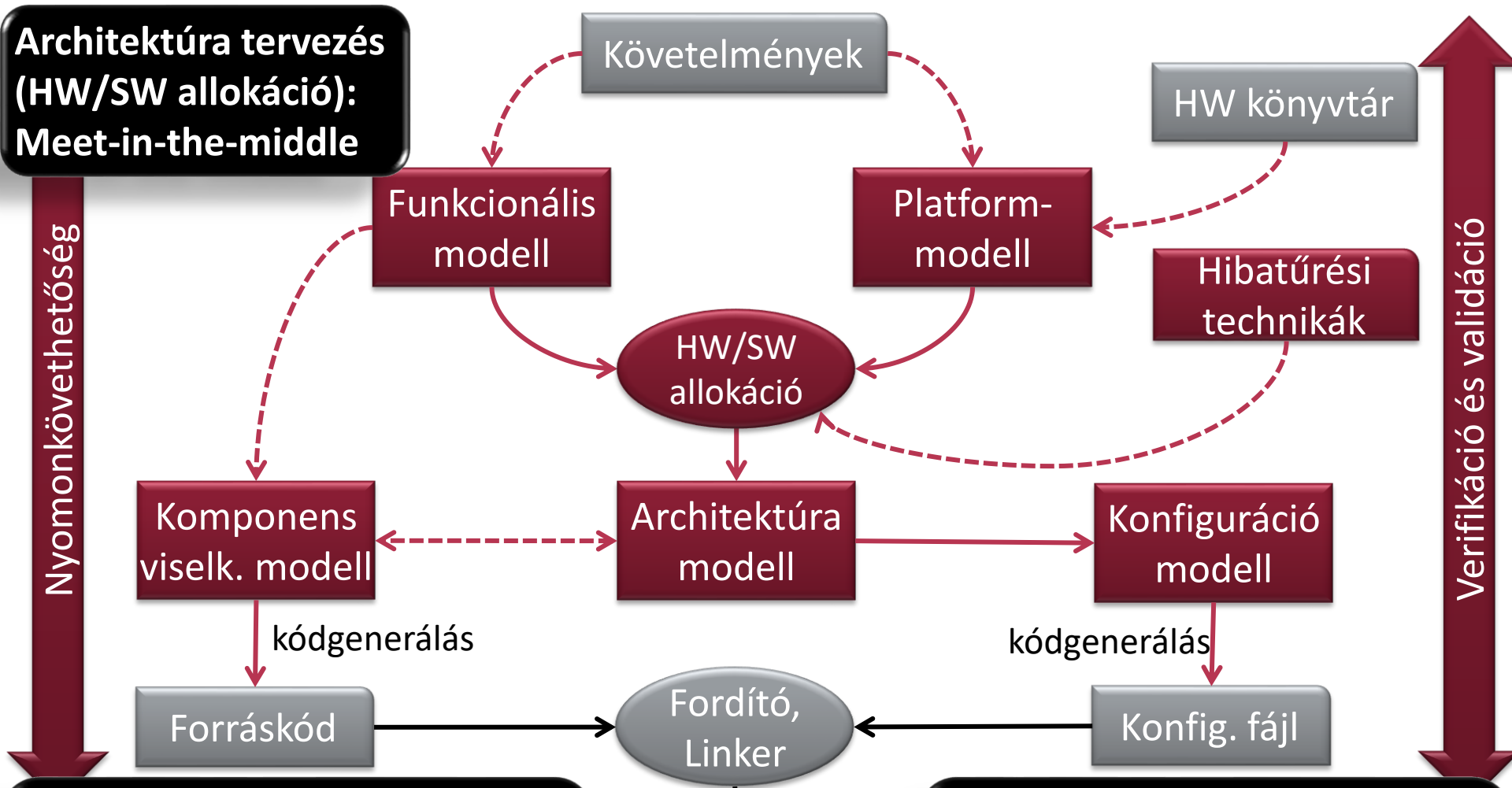
Platform-modell



HW/SW allokáció

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

Platform-alapú rendszertervezés



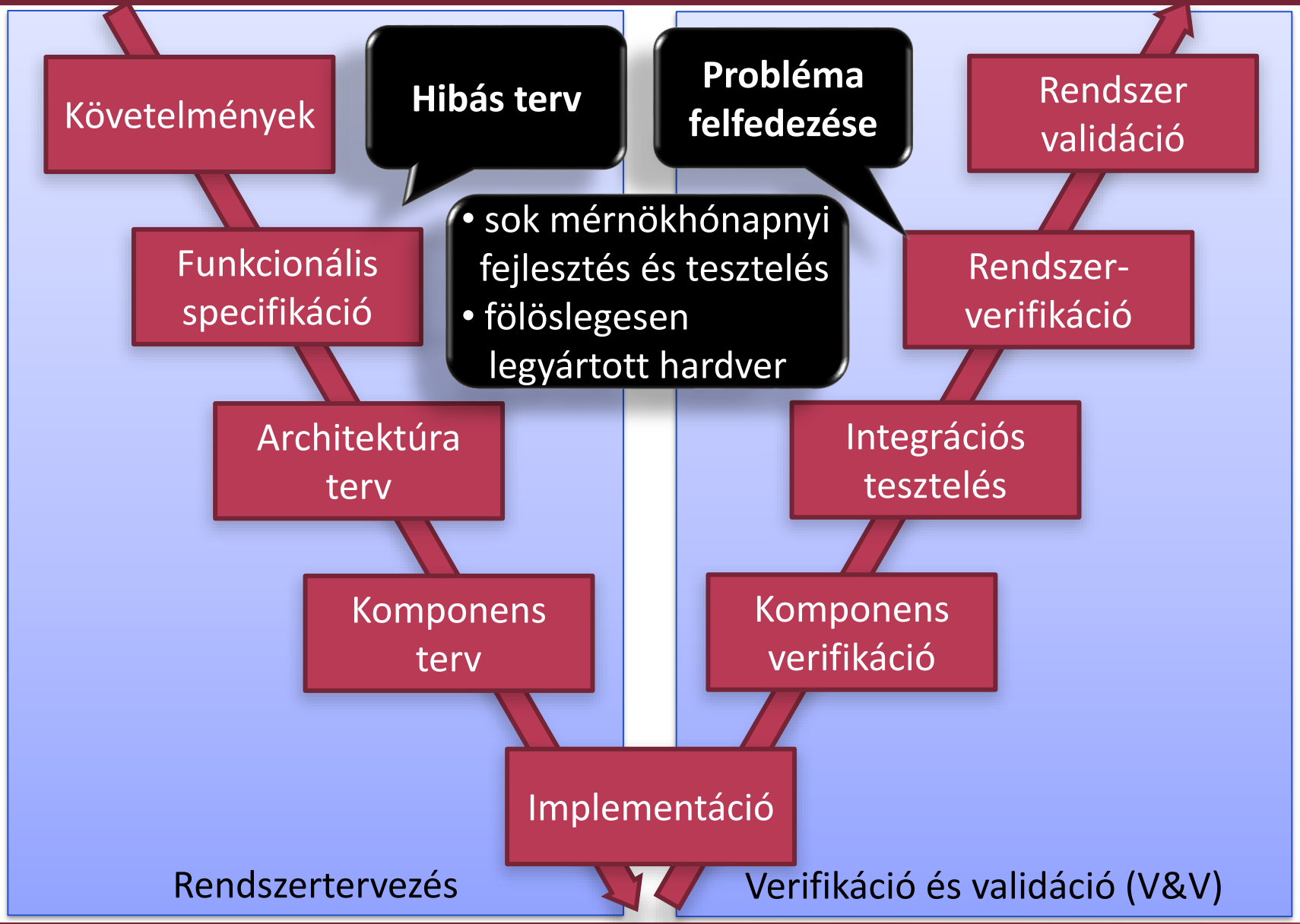
Funkcionális tervezés:Top-down
- Funkcionális dekompozíció
- Követelmények nyomonkövethetősége

Platform tervezés: Bottom-up
- Bevett HW+SW megoldások
- Tömegtermelés (minél olcsóbb hardver)

VERIFIKÁCIÓ ÉS VALIDÁCIÓ A RENDSZERTERVEZÉSBEN

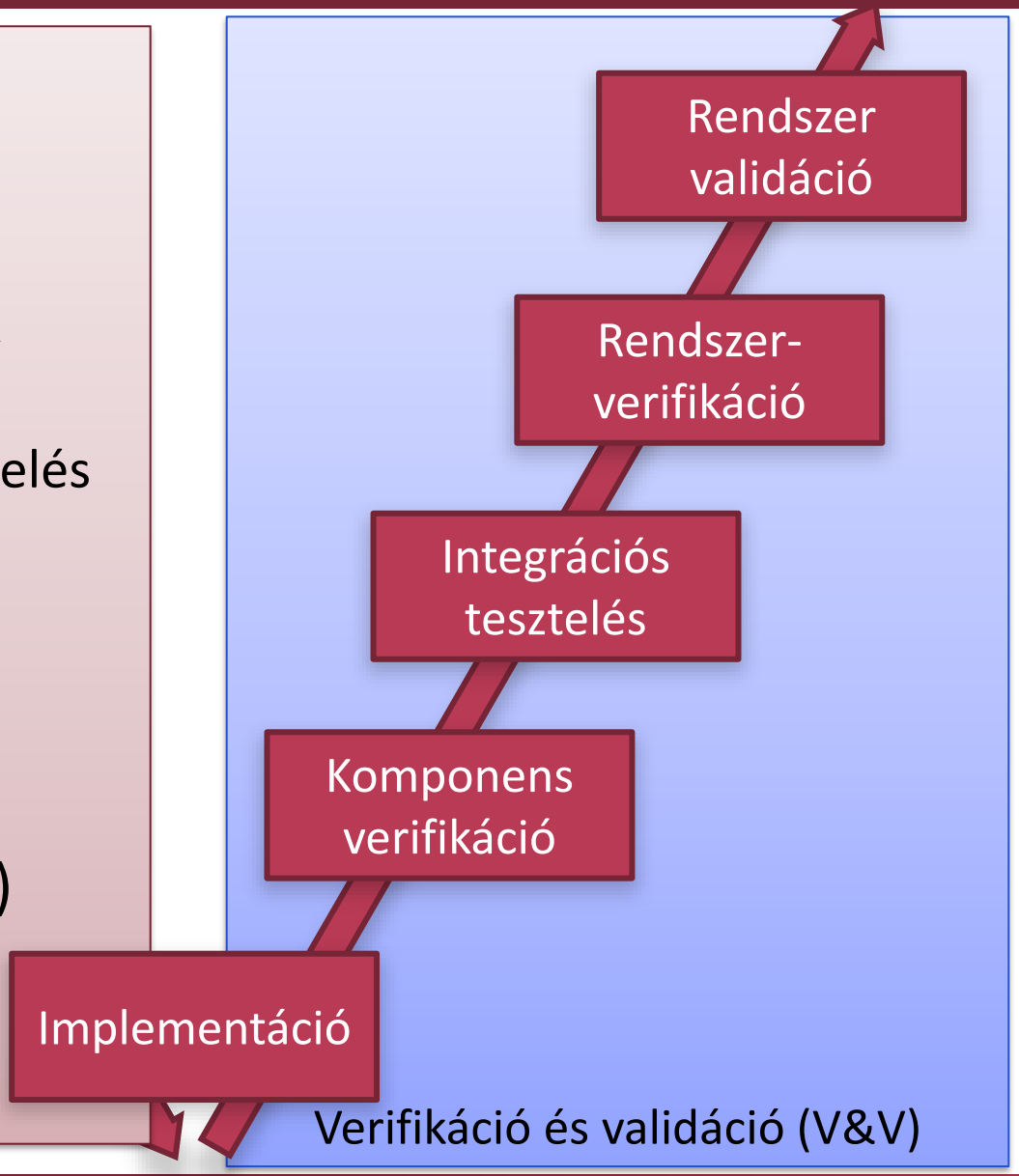
Miért működik mégis egy ennyire komplex rendszer?

Motiváció

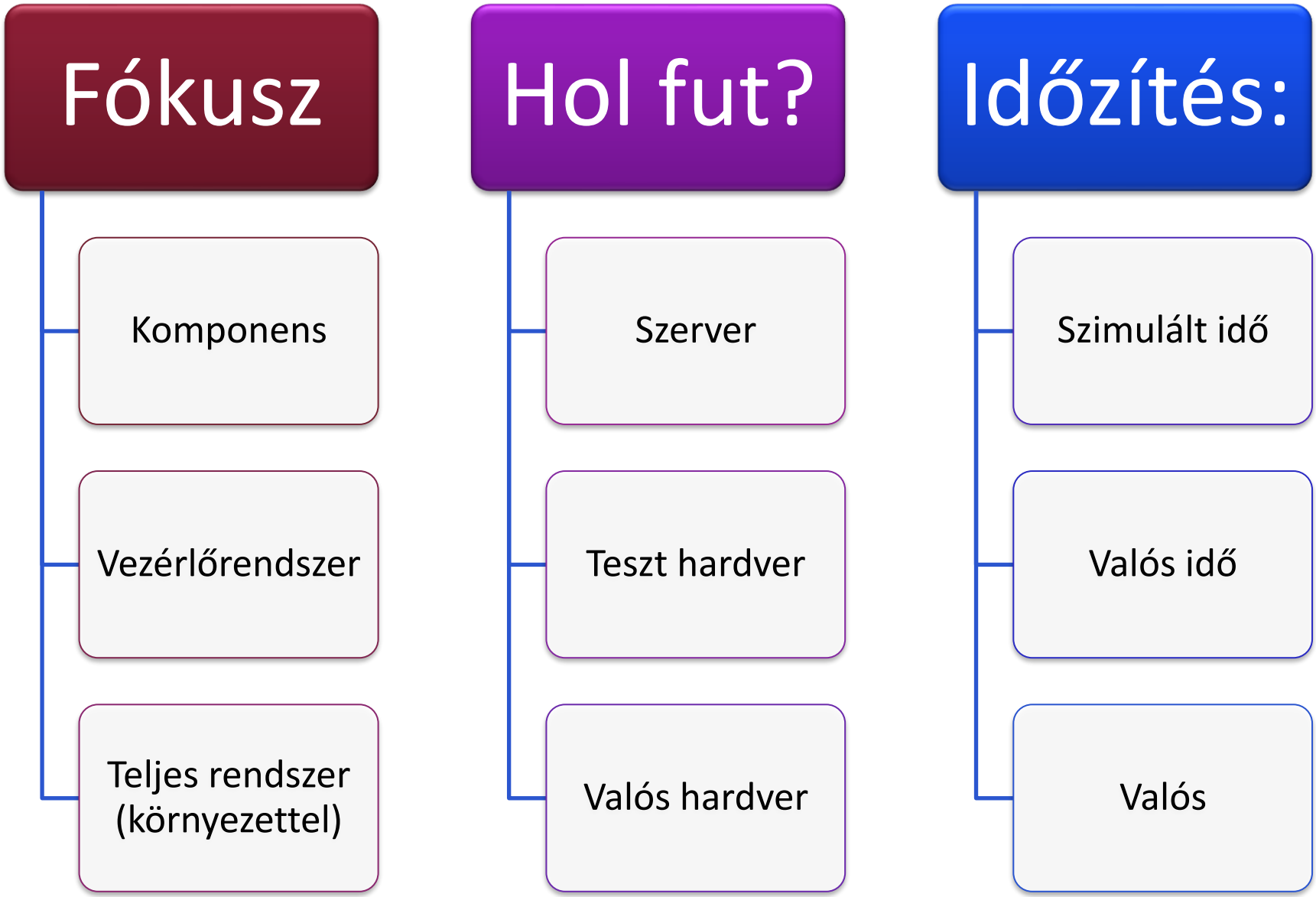

Követelmények
Hibás terv
Probléma felfedezése
Rendszer validáció
Funkcionális specifikáció
• sok mérnökhónapnyi fejlesztés és tesztelés
• fölöslegesen legyártott hardver
Rendszer-verifikáció
Architektúra terv
Integrációs tesztelés
Komponens terv
Komponens verifikáció
Implementáció
Rendszertervezés
Verifikáció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

V&V technikák a képzésben

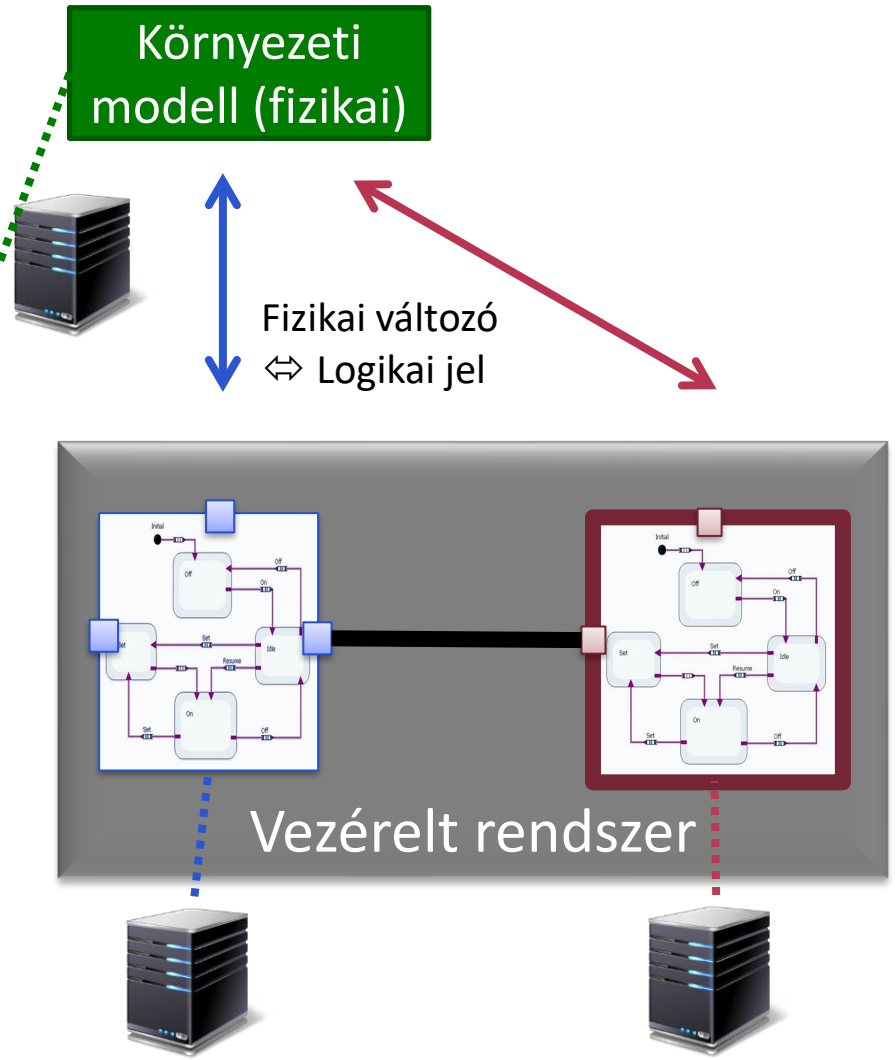
- REMO
  - Szimuláció (folyamat)
  - Tesztelés (orákulum / fedettség / öntesztelés)
  - Modellellenőrzés alapok
- RETE
  - Követelmény alapú tesztelés
  - Modellalapú tesztelés
- Ipari Informatika
  - HIL / SIL
  - Szimuláció
- Szoftver- és rendszerellenőrzés (MSc)
  - Számos további módszer



Szimuláció/tesztelés alapú verifikáció és validáció



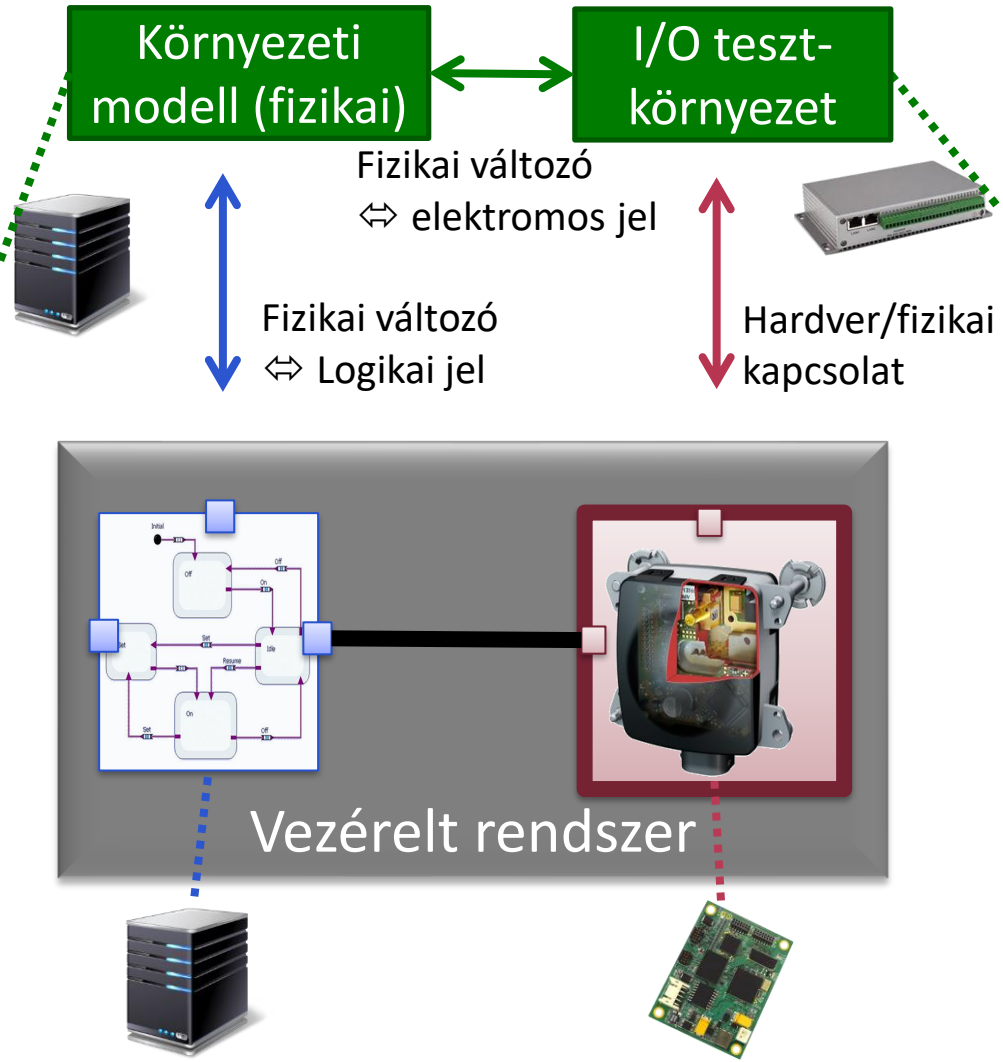
Komponens verifikáció



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
  - Modellalapú tesztelés

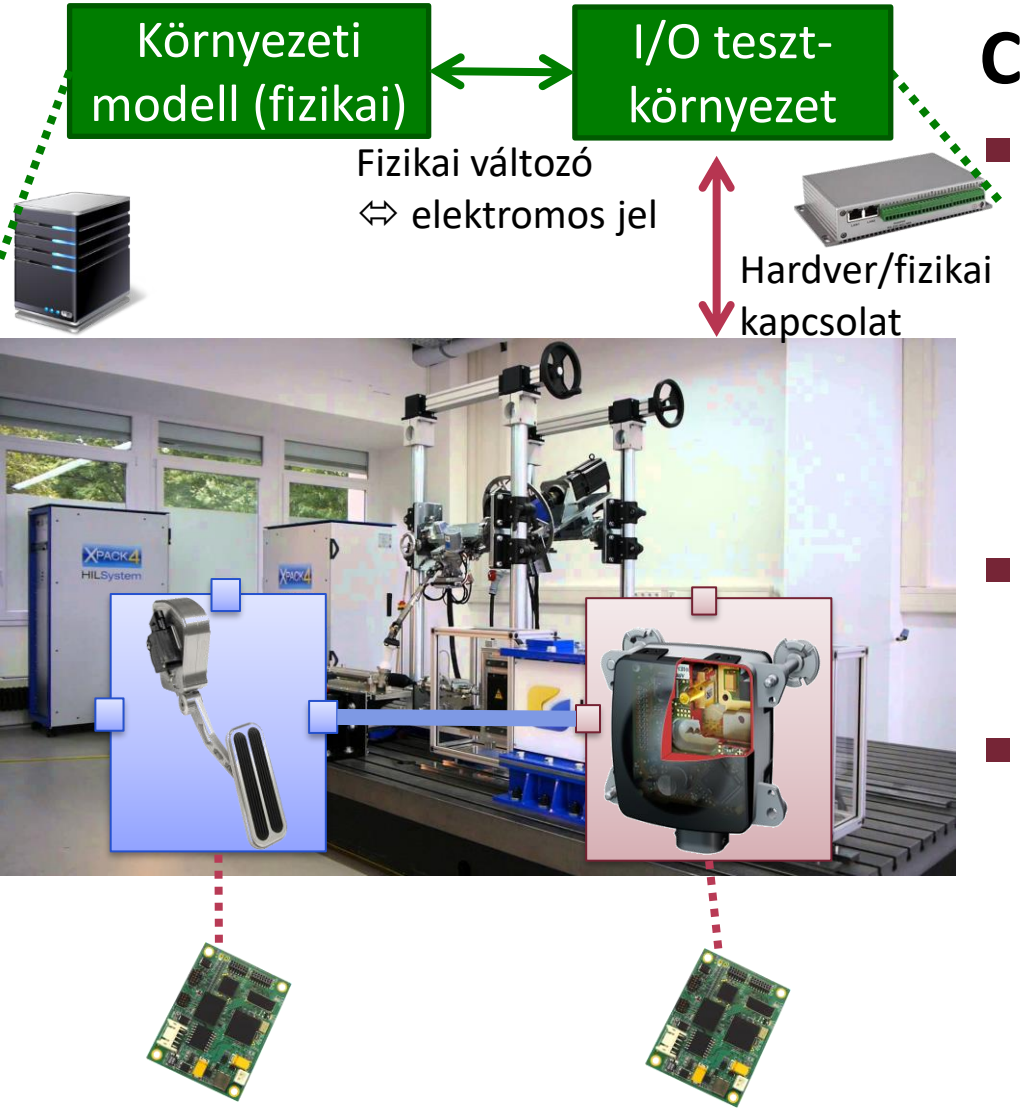
Integrációs tesztelés



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



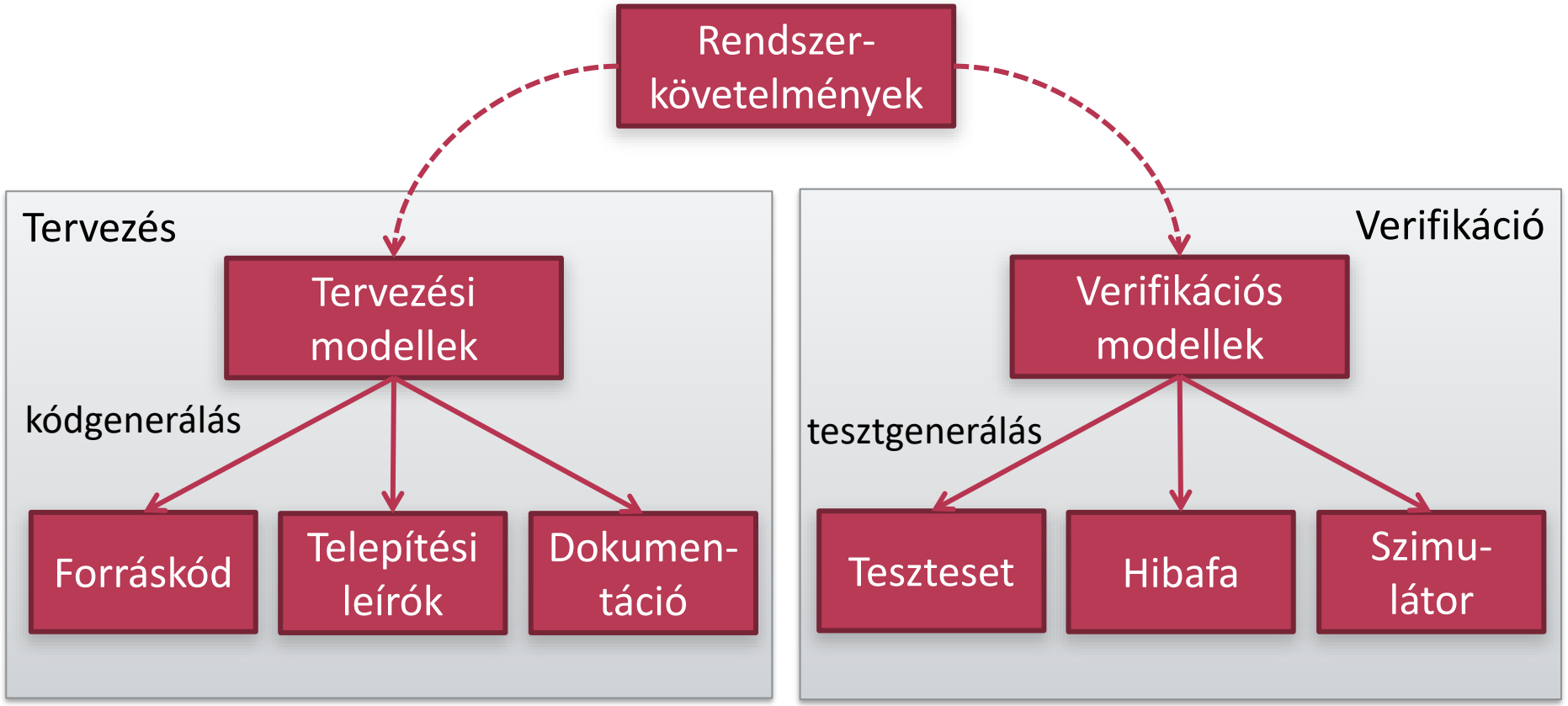
Component-in-the-loop

- 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

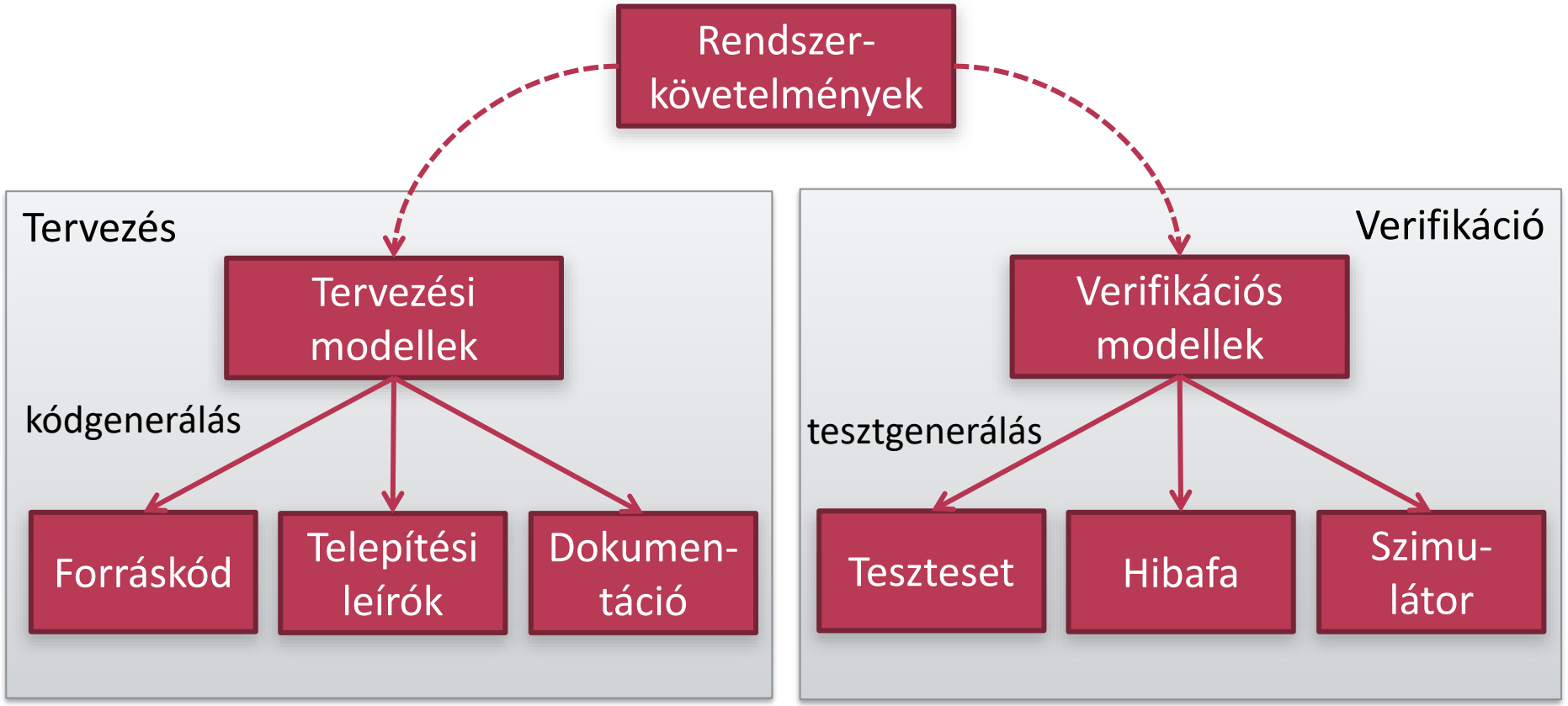
Modellek felhasználási célja



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

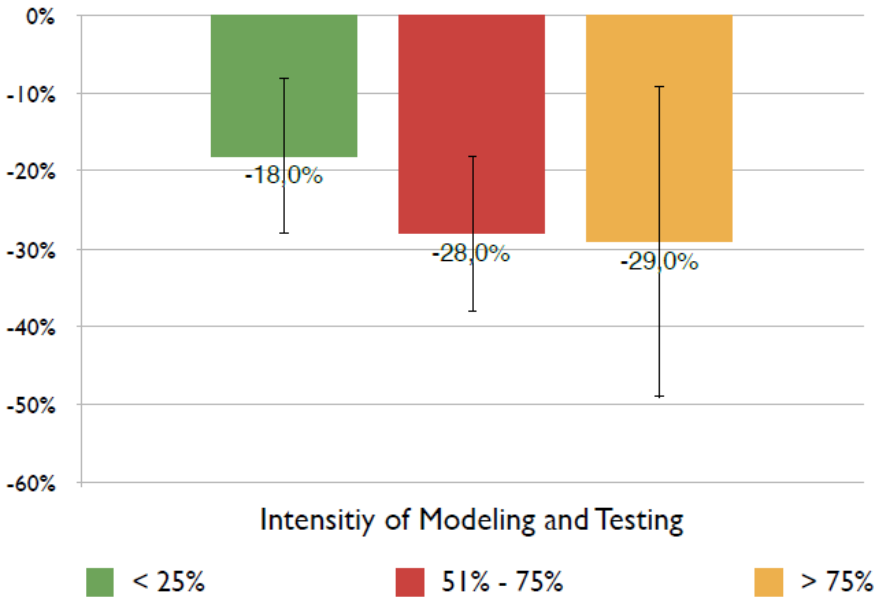
Példák verifikációs modellekre

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

ÖSSZEFOGLALÁS

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

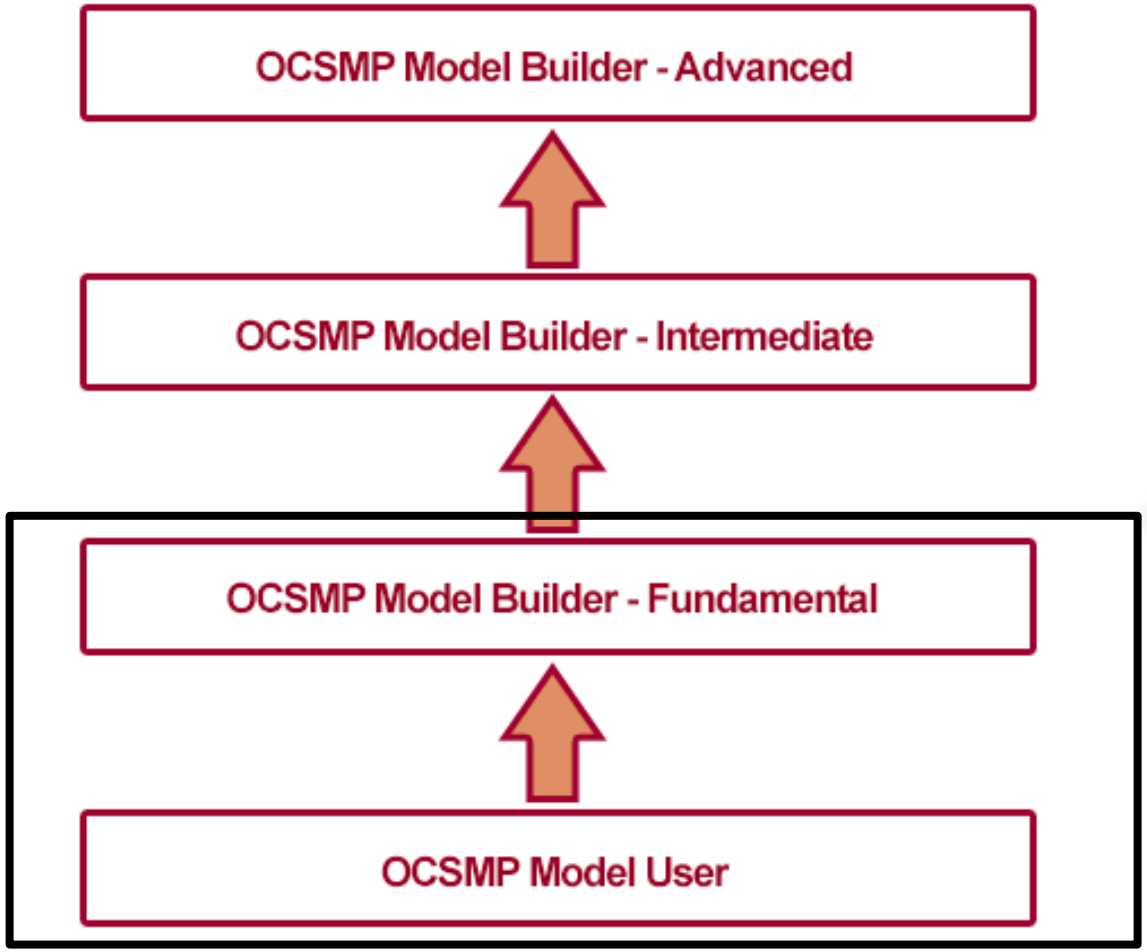


Felmérés:
- autóipari szereplők
- 180 ember (14 országból)
- menedzserek, fejlesztők, R&D

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.

Mit tanulhatok itt?

OMG-Certified Systems Modeling Professional

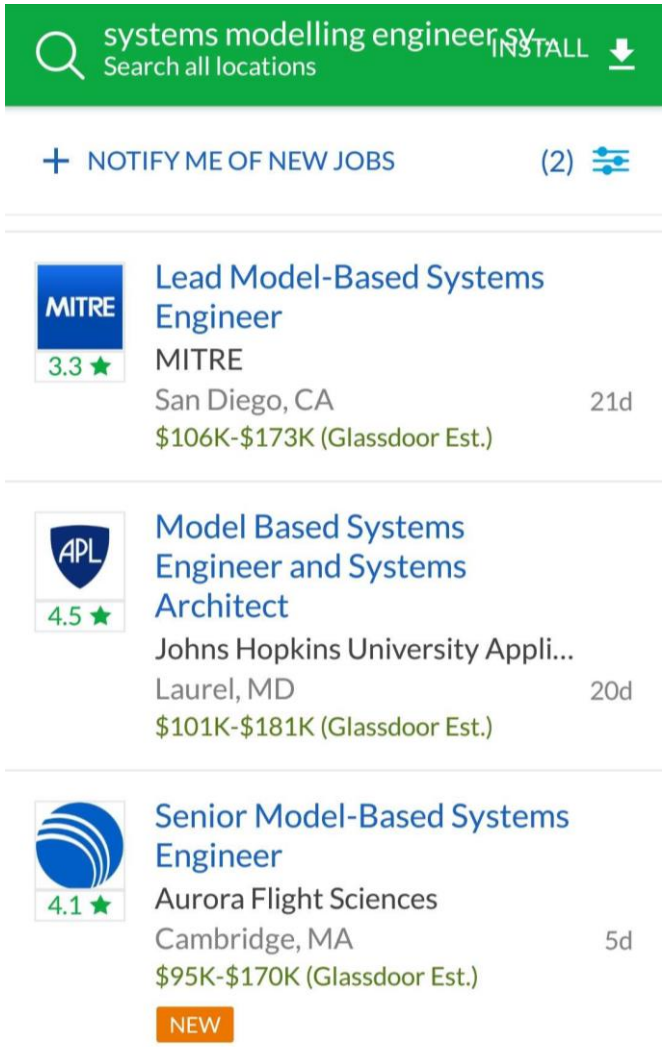


ReTe tárgy

Tréning piaci ára: 500-5000 EUR

https://www.omg.org/ocsmp/

Megéri ezt megtanulni?



- Rendszerbiztonsági Mérnök
- Hardver és Szoftver Integrátor
- Szoftverintegrációs Mérnök
- Applikációs Szoftverfejlesztő Mérnök (MATLAB/Simulink)
- Rendszer Integrációs Mérnök
- FPGA és SW fejlesztőmérnök - Hardware-in-the-loop
- Rendszerteszt Automatizáló Mérnök (Motor Tesztpad)
- Rendszerteszt Automatizáló Mérnök (Rendszer Tesztpad)

Informatikai rendszertervezés (áttekintés)

- Követelmények rögzítése
- Használati esetek

Követelmény analízis

- Funkcionális dekompozíció
- Komponens + Interfészek

Komponens tervezés

- Állapotgépek
- Adatfolyam
- Jellegzetes futási utak (szekvencia)

Viselkedés modellezés

- Platform modellezés
- Nemfunkcionális analízis
- Allokáció

Architektúra tervezés

- Biztonság (safety) alapok
- Hibatűrő rendszer-architektúrák

Biztonságra tervezés

- Specifikáció alapú, modellalapú tesztelés
- Tesztfedettség
- Szimuláció

Verifikáció és validáció

- Modell-transzformáció
- Kódgenerálás

Automatizálási módszerek

Összegzés: Informatikai rendszertervezés