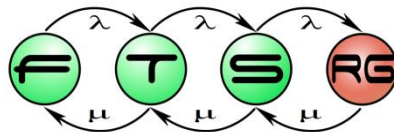


# Informatikai rendszertervezés

Dr. Micskei Zoltán

(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

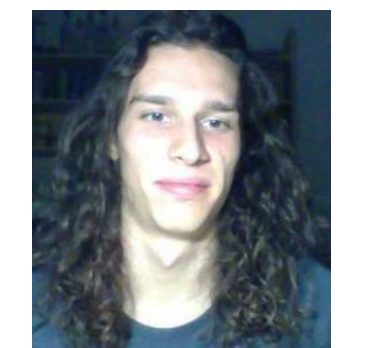
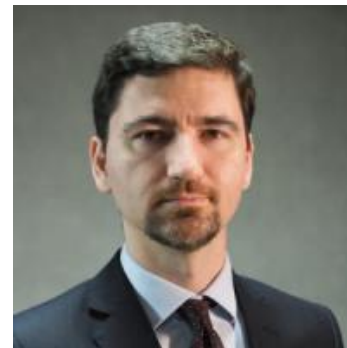
## MSc szakirány Kritikus rendszerek

- Modellalapú rendszertervezés
- Szoftver- és rendszerellenőrzés
- Kiberfizikai rendszerek

# A tárgy oktatói

## ■ Előadók

- Dr. Bergmann Gábor
- Farkas Rebeka
- Graics Bence
- Dr. Horváth Ákos
- Dr. Micskei Zoltán
- Molnár Vince



## ■ Gyakorlat / házi feladat:

- demonstrátorok

# 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)

## ■ Írásbeli vizsga

- Elméleti kiskérdések és gyakorlati feladatok

# IMSc pontok

- Legfeljebb 20 pont szerezhető
- IMSc pontok
  - IMSc rész a házi feladatokban: max. 12 pont
  - Extra pont: max. 12 pont
  - Opcionális, egyedi feladat: max. 10 pont
- Nem csak IMSc hallgatóknak
- DE: csak jelest elért hallgatóknak

# Weboldalak

## ■ <https://inf.mit.bme.hu/edu/courses/rete>

- Hírek, naptár
- Segédanyagok
- HF feladatok



The screenshot shows the website for the 'Hibatűrő Rendszerek Kutatócsoport' (Fault-Tolerant Systems Research Group) at BME. The page is titled 'Informatikai rendszertervezés' (Information Systems Design). It features a navigation menu with options like 'Kezdőlap', 'Események', 'Oktatás', 'Kutatás', 'Hallgatóink sikerei', and 'Magunkról'. The main content area includes a sidebar with 'Oktatás' (Education) and 'Informatikai rendszertervezés' (Information Systems Design) sections. The main content area has tabs for 'Megtekintés' (View) and 'Szerkesztés' (Edit). The page lists the course leader (Varró Dániel) and lecturers (Horváth Ákos, Micskei Zoltán, Imre Molnár, Vince Vörös, András Korábbi). It also includes a 'Célkitűzés' (Objective) section and a 'Felépítés' (Structure) section.

## ■ <http://q2a.inf.mit.bme.hu/questions/rete>

- Technikai kérdések
- HF segítség



The screenshot shows the 'Recent questions and answers in Rendszertervezés' (Recent questions and answers in Information Systems Design) section of the Q&A website. It displays three questions with their respective vote counts and answers:

| Question                              | Votes | Answers | Asked       | Points |
|---------------------------------------|-------|---------|-------------|--------|
| Trigger cannot be empty!              | 0     | 1       | Apr 30      | 510    |
| 4. HáziTopEvent FTA üres emailt küld. | +1    | 1       | Dec 9, 2017 | 113    |
| 4. házi: voter evaluation             | 0     | 0       | Nov 9, 2017 | 22     |

## ■ [YouTube csatorna](#): HF eszköz használata

# Teendő a héten

- Csapatalakítás
- Határidő: szerda 12:00
  - Nem jelentkező hallgatókat automatikusan beosztjuk
- Űrlap linkje: hírben publikáljuk

# MOTIVÁCIÓ

Miért van szükség rendszertervezésre?





# Hol fontos a rendszertervezés?



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

Continental



PROLAN

evopro

NATIONAL INSTRUMENTS

ThyssenKrupp



BOSCH

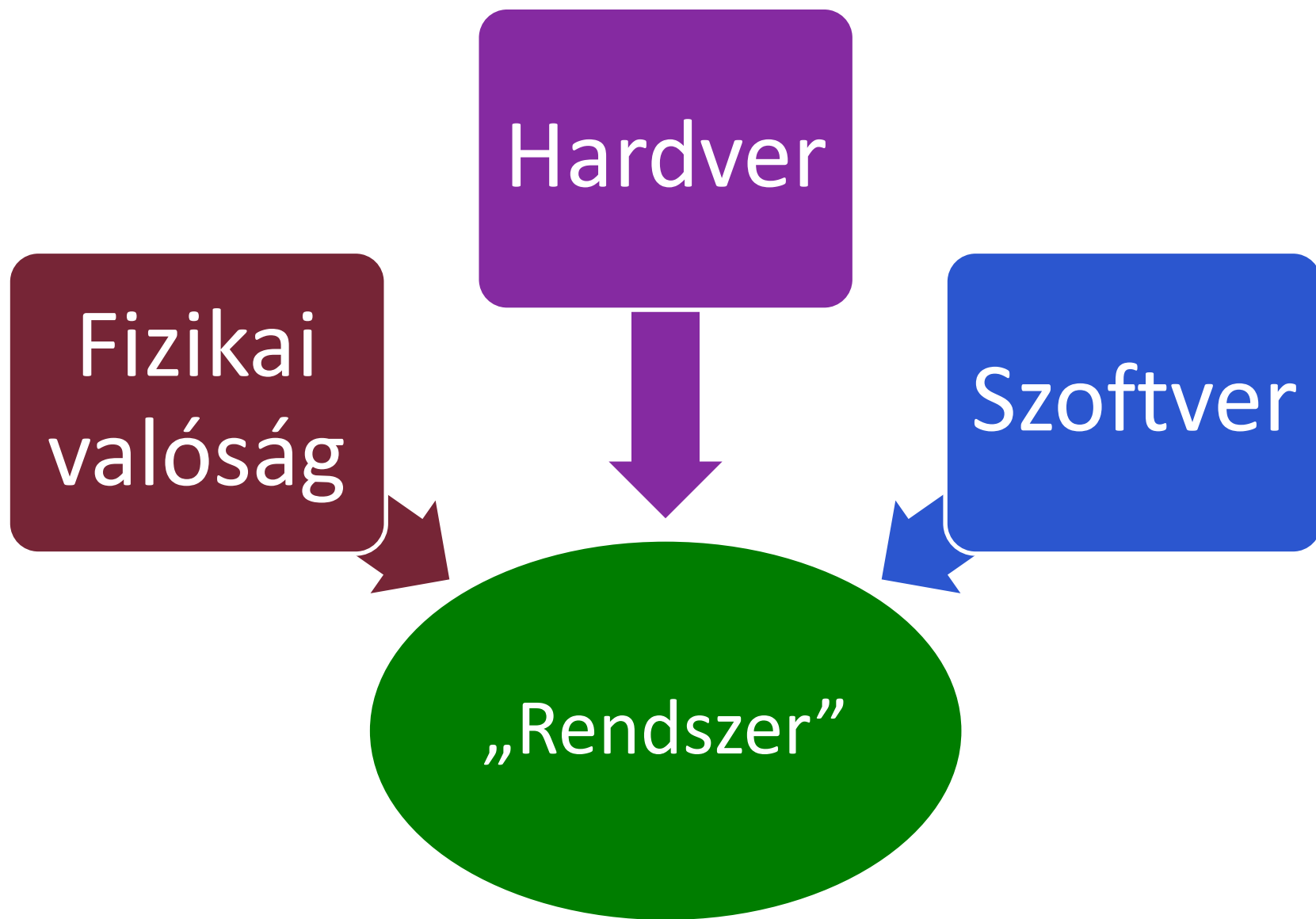


SIEMENS

KNORR-BREMSE

KUKA

# 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

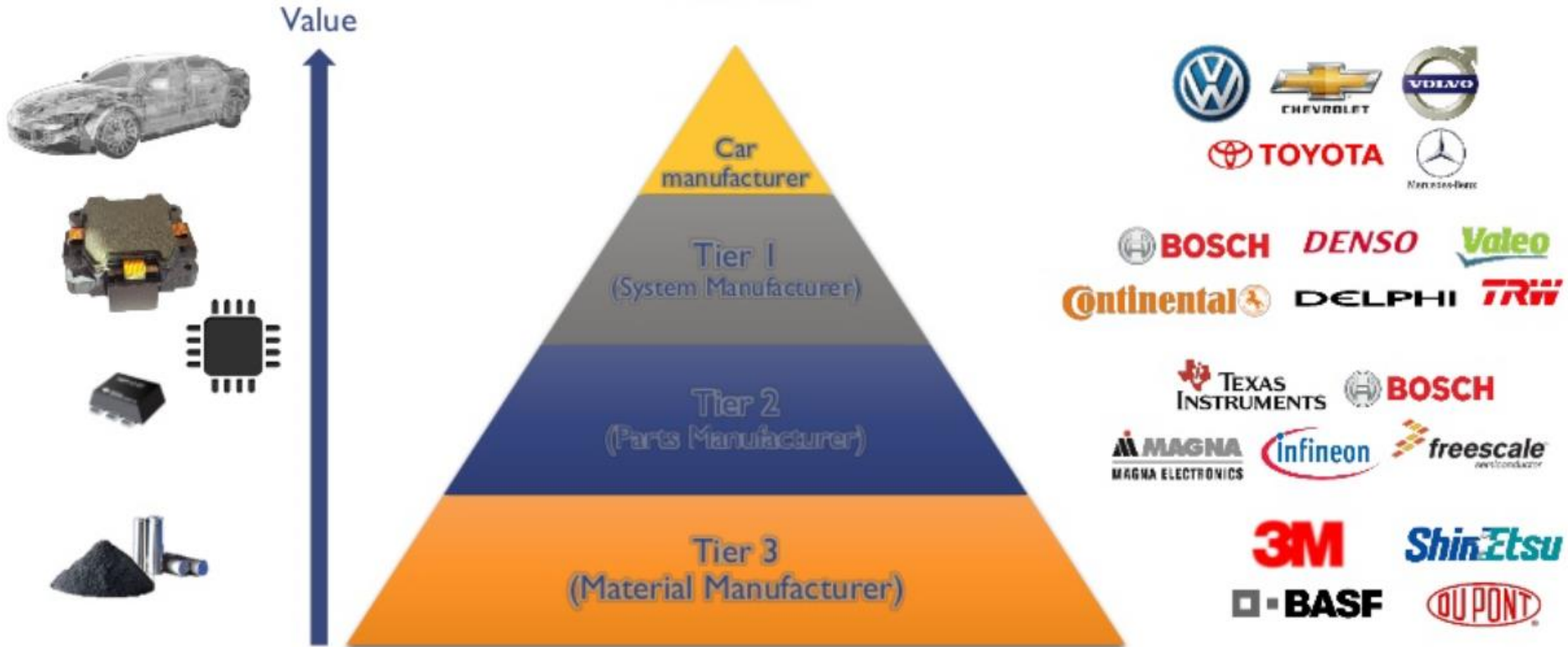
- (Biztonság)kritikus rendszerek
- Engedélyezés, tanúsítás

# Példa: Egy mai modern autóban...



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

# Példa: Egy mai modern autóban...



## Autógyártó feladata

- Követelmények megadása
- Komponensek integrálása

# Példa: Egy mai modern autóban...



## Drive-by-wire: Nincs mechanikus kapcsolat

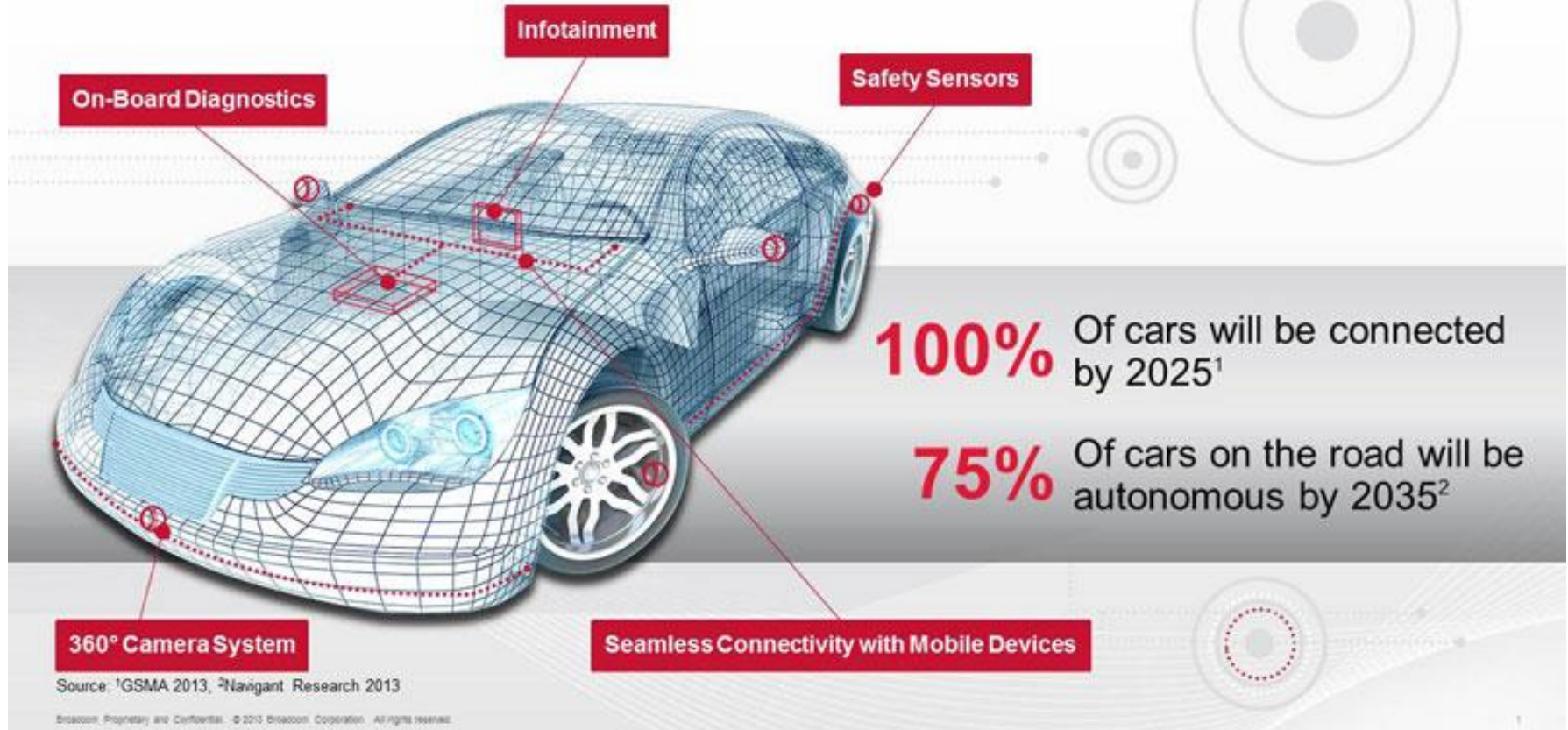
- Kormánykerék ⇔ kormányzott kerék
- Fékpedál ⇔ fékbetétek
- Gázpedál ⇔ motor

## Van viszont helyette

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

# ... és a jövő autójában

## THE CONNECTED CAR



## Kiber-fizikai rendszerek



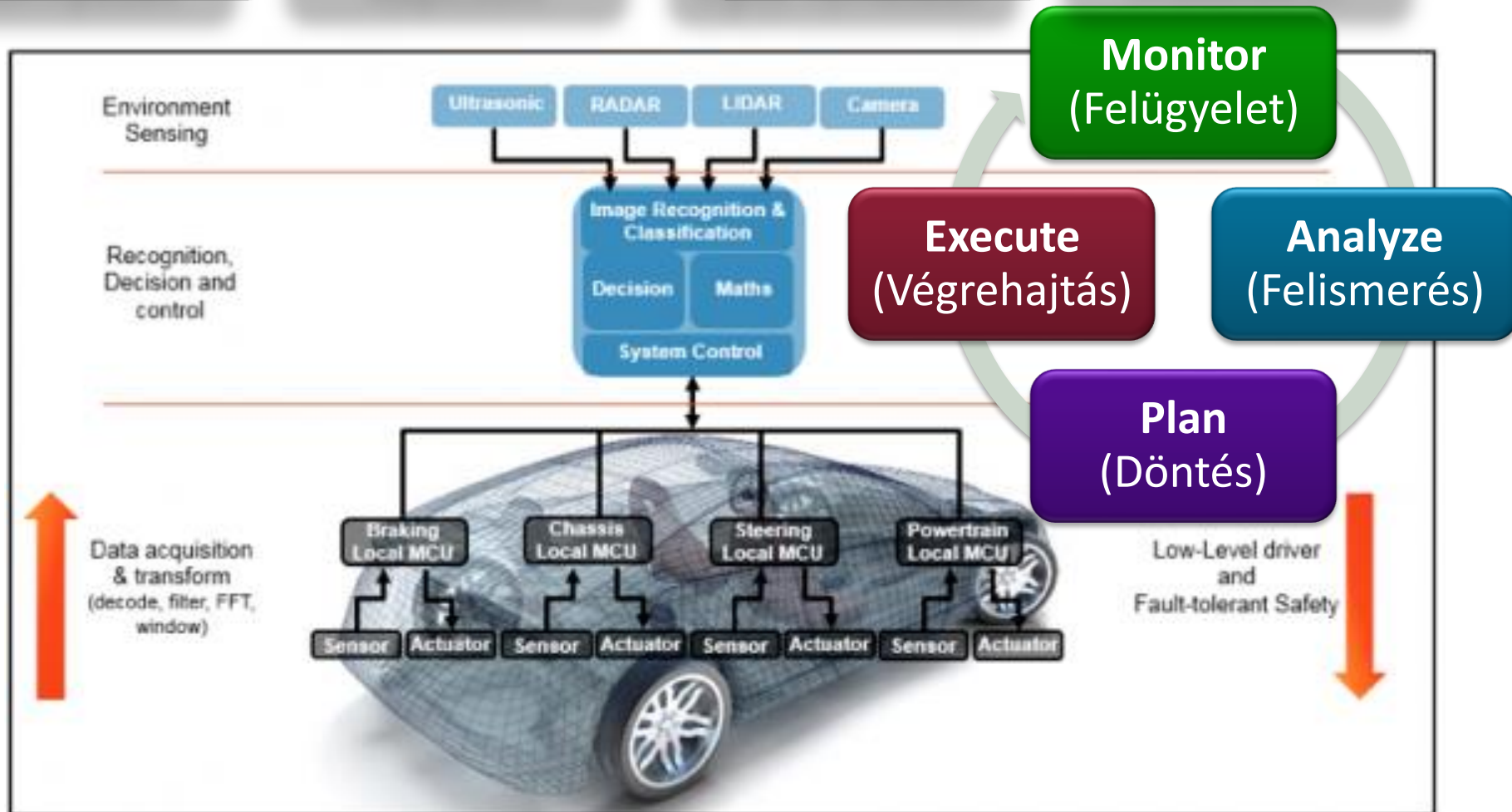
# ... és a jövő autójában

Változó fizikai környezet

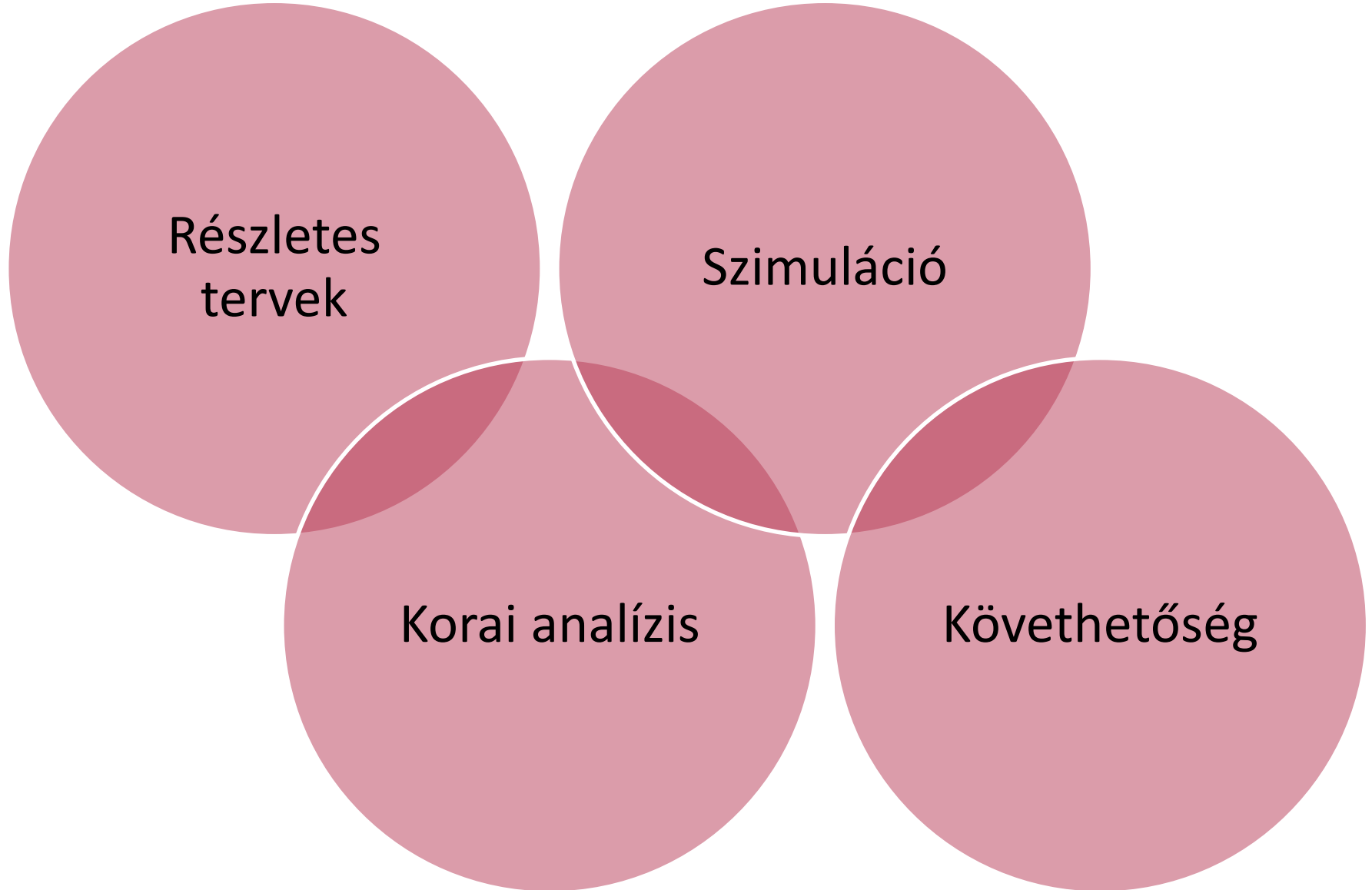
Hálózatba kapcsolt

Dinamikus nyílt rendszer

Biztonságos működés?



# Következmény: rendszerTERVEZÉS



# MODELLEK A RENDSZERTERVEZÉSBEN

Hol és miért használunk modelleket?

# Különböző absztrakciós szinteken...

Rendszer

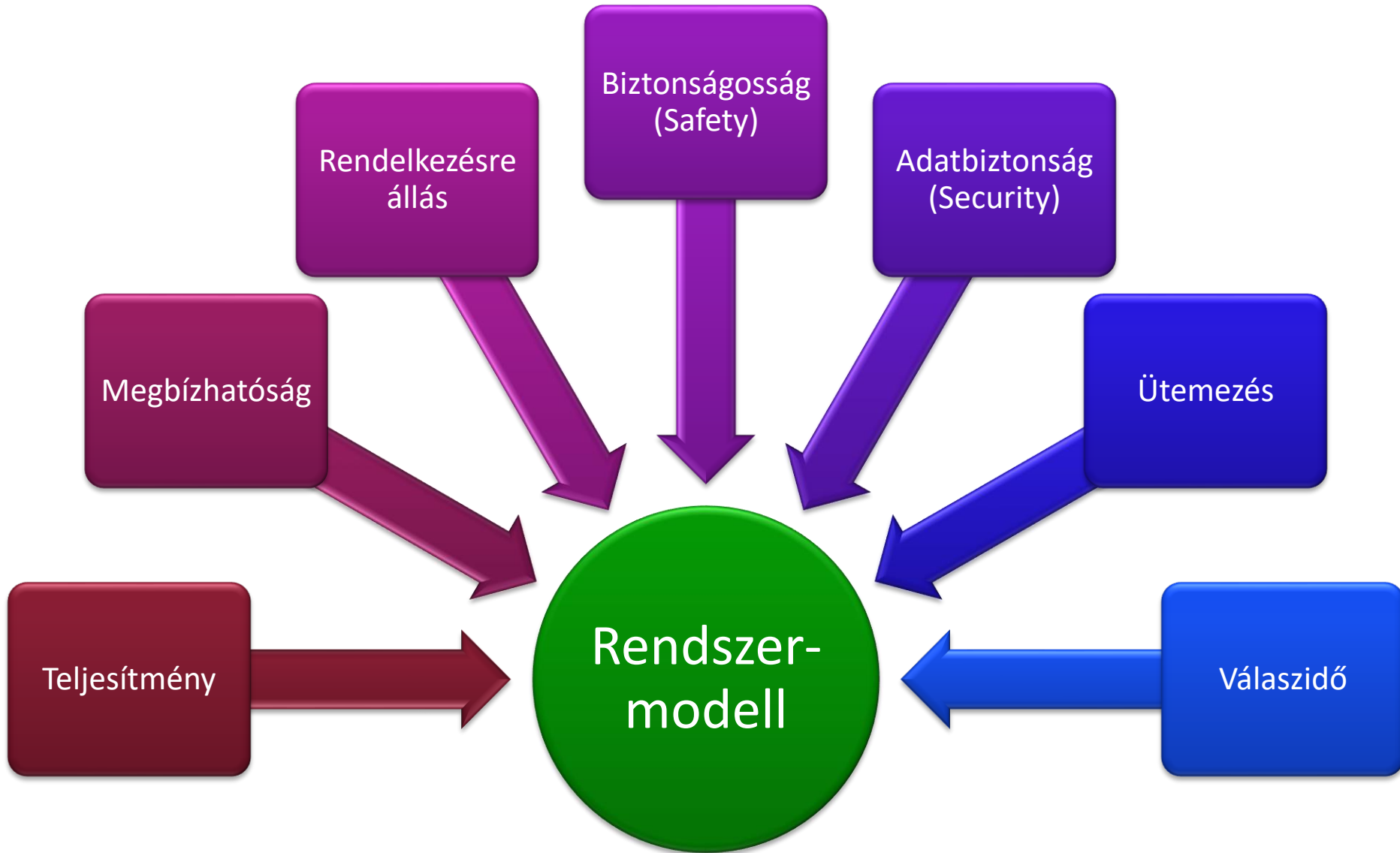
Architektúra

Komponens

# Különböző tervezési fázisokban...



# Többféle nézőpontból...



# Többféle célból...

Statikus  
modellezés

Dinamikus  
modellezés

Tervezési  
folyamat

Tervezési-  
bejárás,  
Optimalizáció

Architektúra-  
tervezés

Platform-  
modellezés

Allokáció,  
Telepítés

Tesztelés,  
V&V

Szimuláció

Kódgenerálás

Dokumentáció-  
generálás

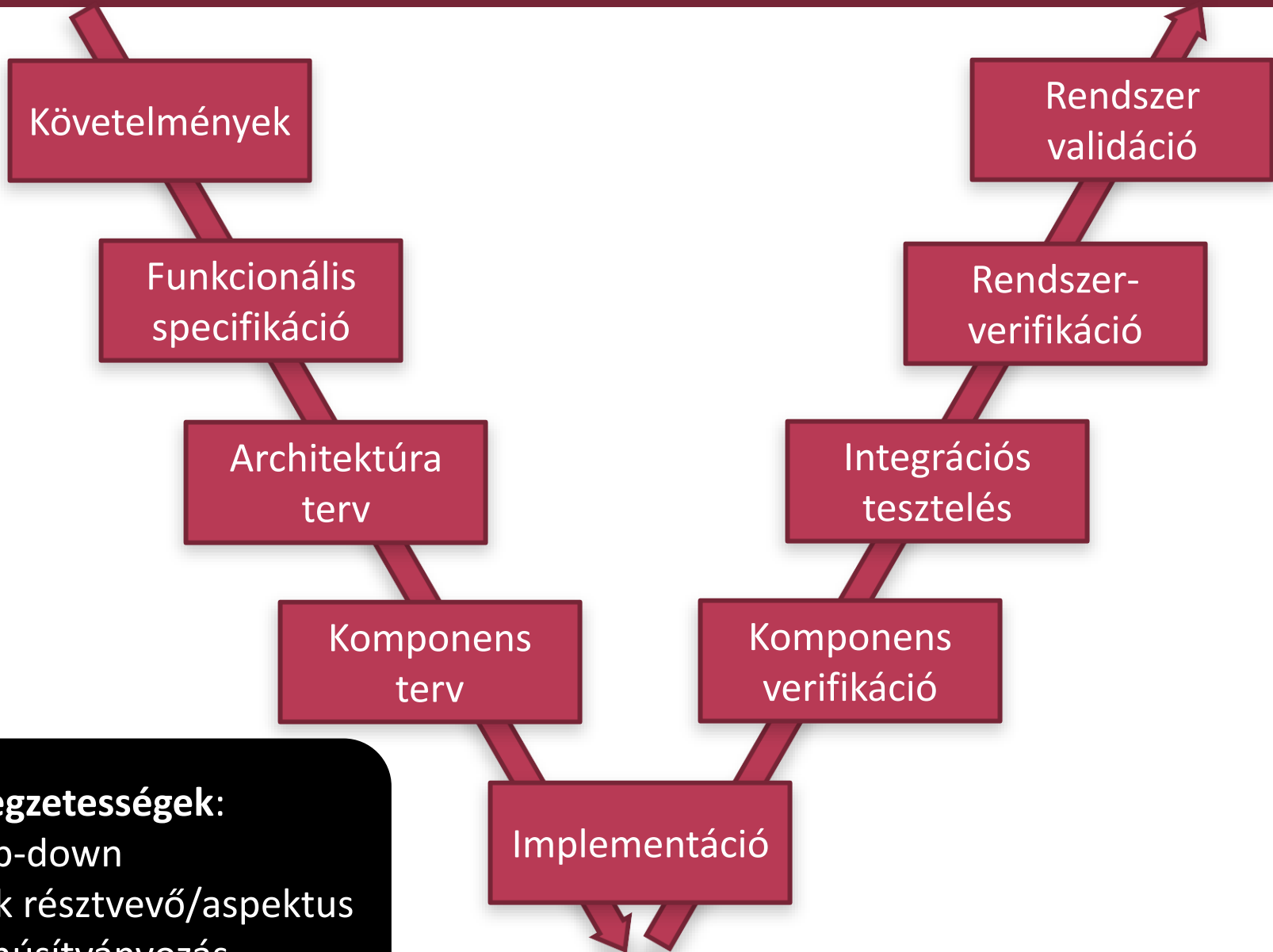
Fizikai és  
mérnöki  
modellek

# A RENDSZERTERVEZÉS FOLYAMATA

Milyen tipikus lépésekből áll a rendszertervezés?



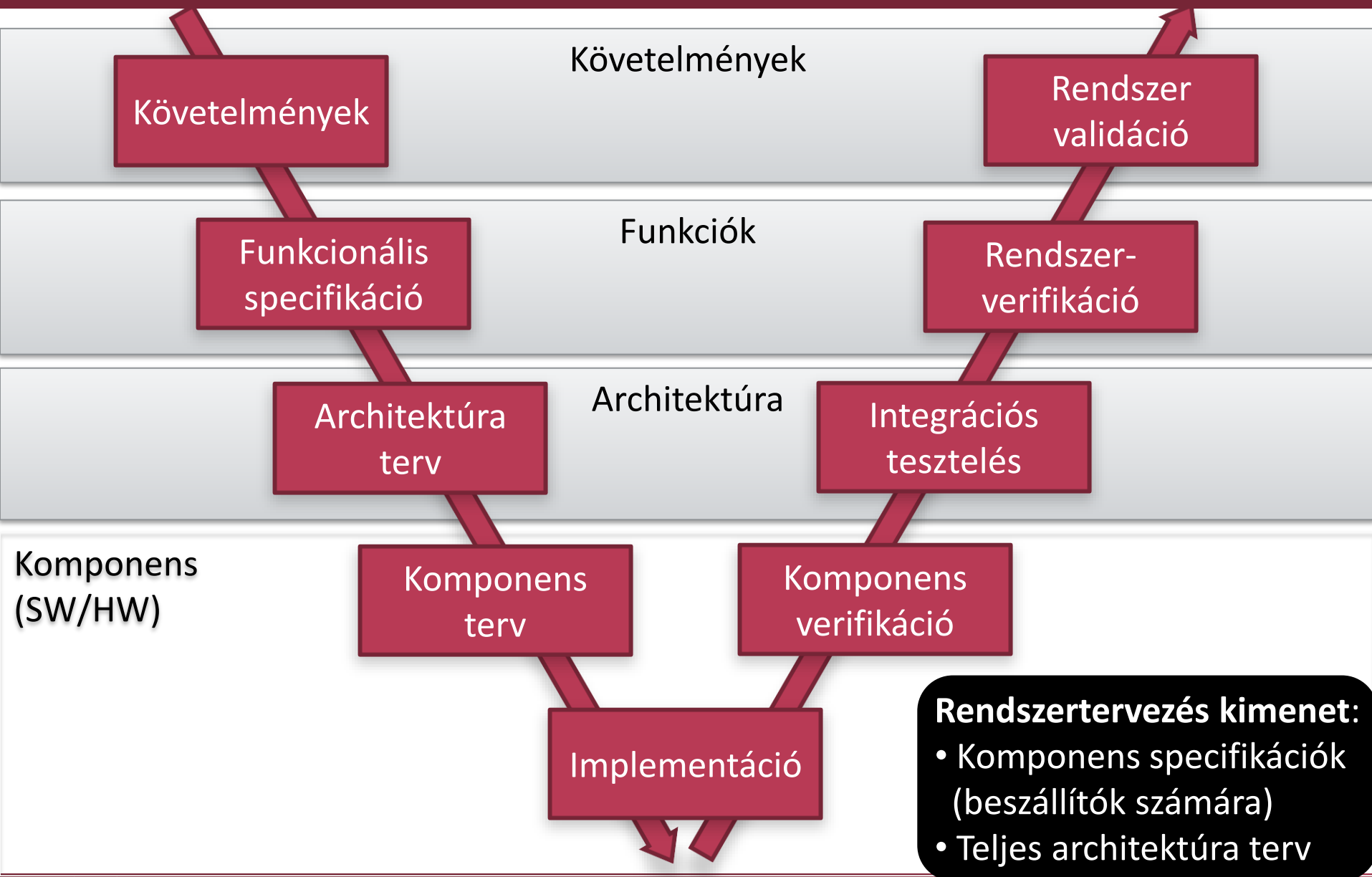
# V-modell: Kritikus rendszerek



## Jellegzetességek:

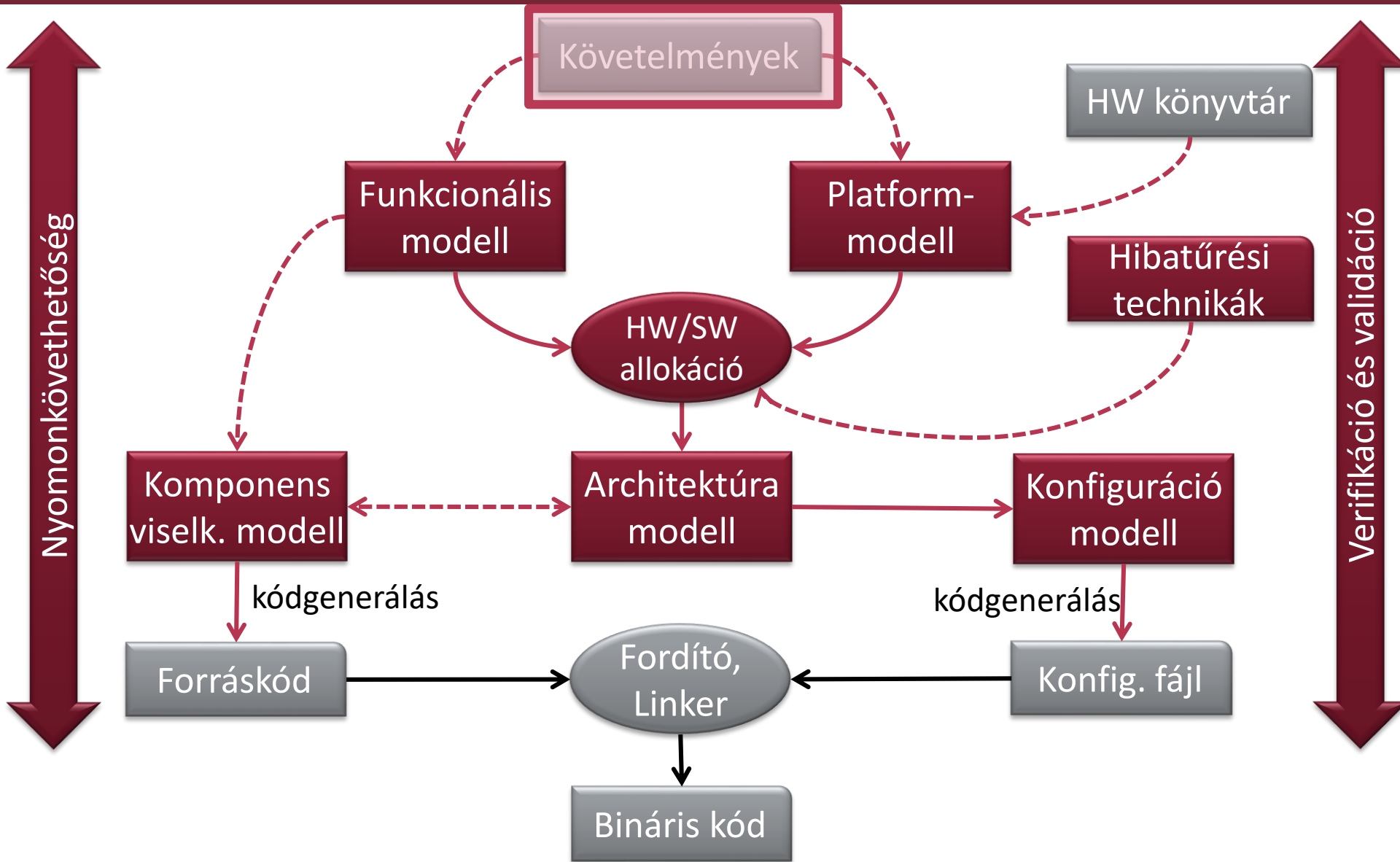
- Top-down
- Sok résztvevő/aspektus
- Tanúsítványozás

# A rendszertervezés feladata

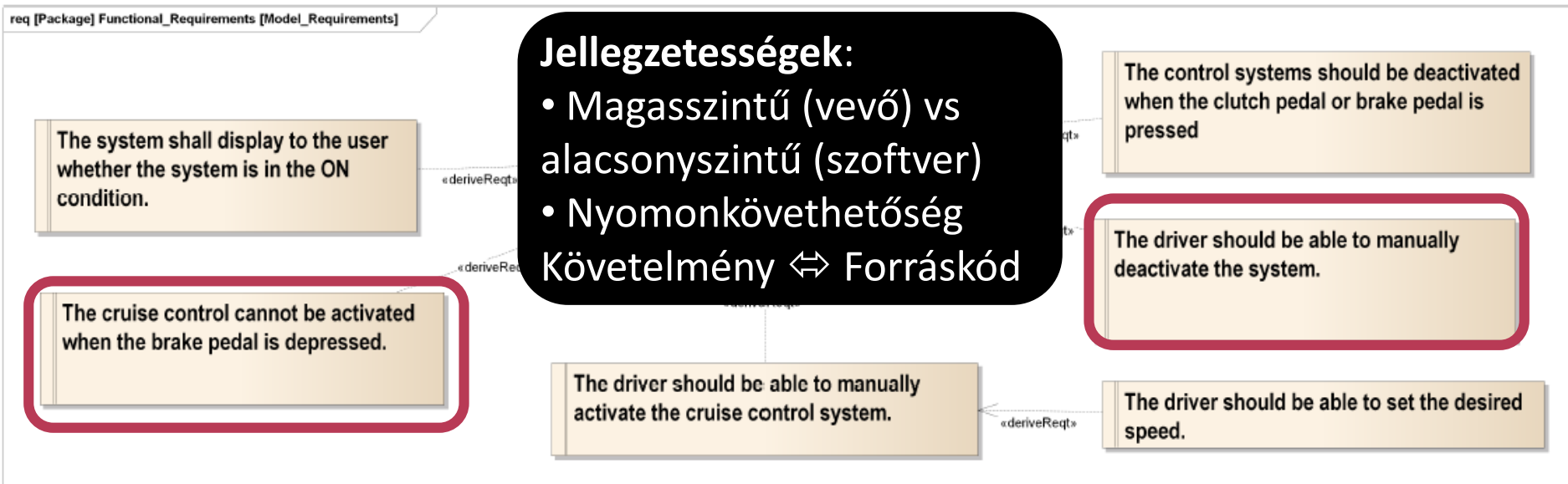


- Rendszertervezés kimenet:**
- Komponens specifikációk (beszállítók számára)
  - Teljes architektúra terv

# Platform-alapú rendszertervezés



# Követelmények



## Példa

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

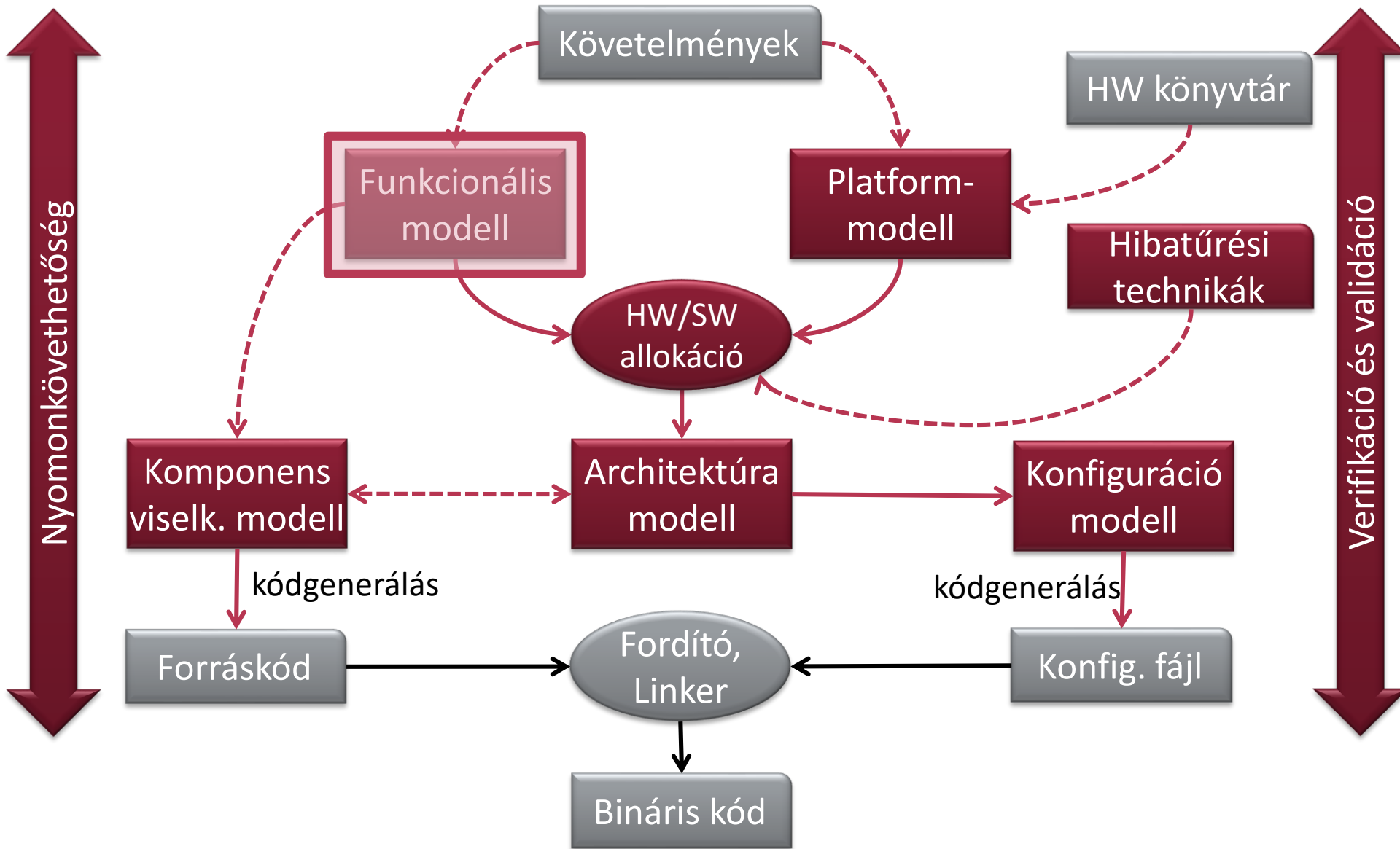
## REMO:

- Követelmények modellezése
- Funkcionális / nemfunkcionális
- Finomítás / Konfliktus

## RETE (UML / SysML):

- Requirements diagram
- Use case diagram

# Platform-alapú rendszertervezés



# Funkcionális specifikáció

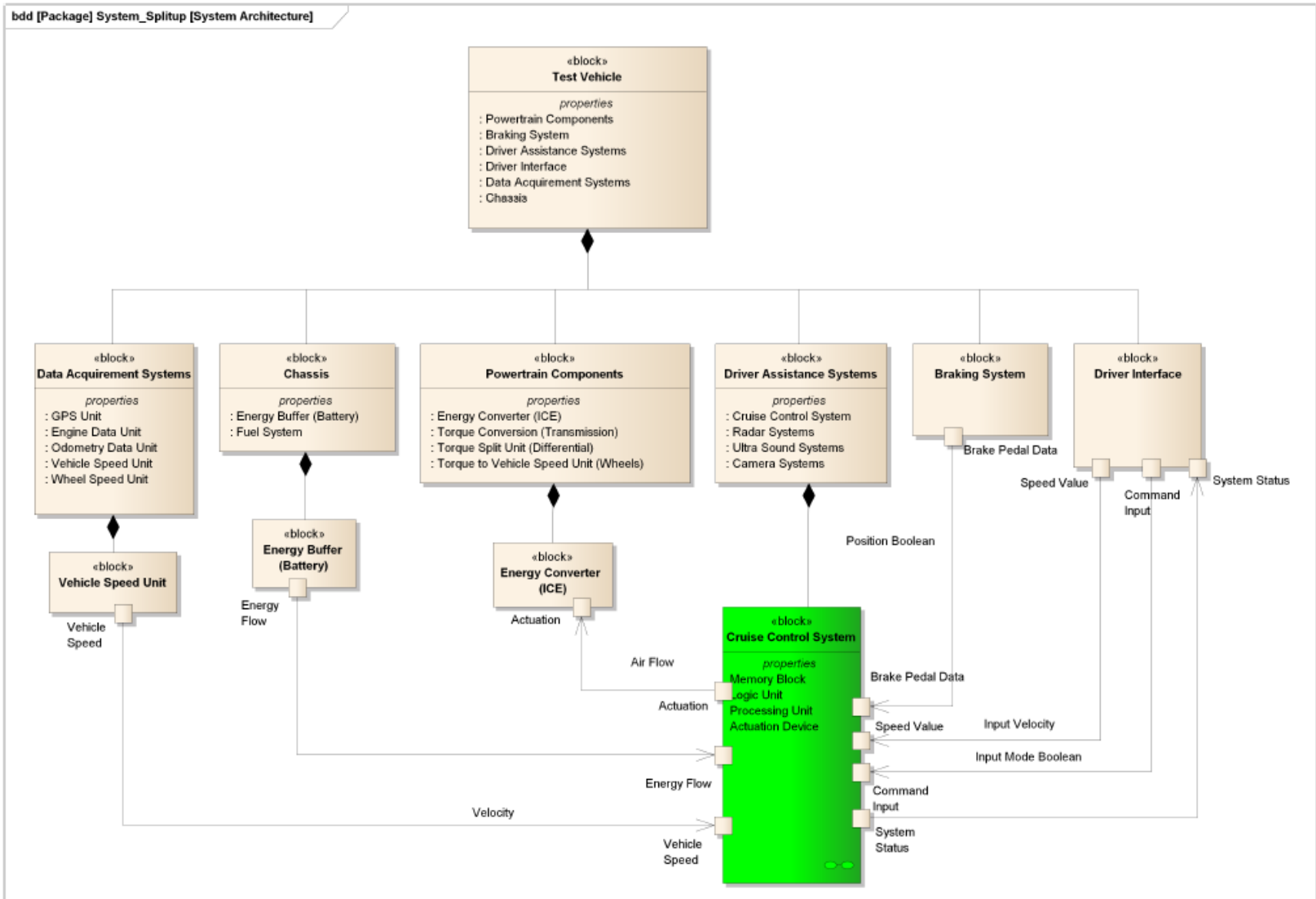
- 1 Adaptive Cruise Control
- 2 Electronic Brake System MK60E
- 3 Sensor Cluster
- 4 Gateway Data Transmitter
- 5 Force Feedback  
Accelerator Pedal
- 6 Door Control Unit
- 7 Sunroof  
Control Unit

**Funkcionális specifikáció =**  
Funkciók / szolgáltatások +  
interfészek + kapcsolatok +  
+ kapcsolódó követelmények

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

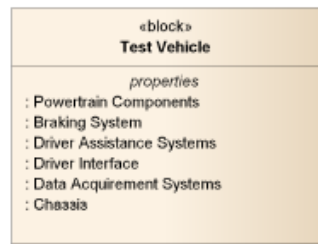


# Példa: Funkcionális specifikáció



# Példa: Funkcionális specifikáció

bdd [Package] System\_Splitup [System Architecture]



## ■ Tempomat bemenete:

- Aktuális sebesség
- Elvárt sebesség
- Fékpedál állapota
- Vezető parancsa
- Energia

## ■ Tempomat kimenete:

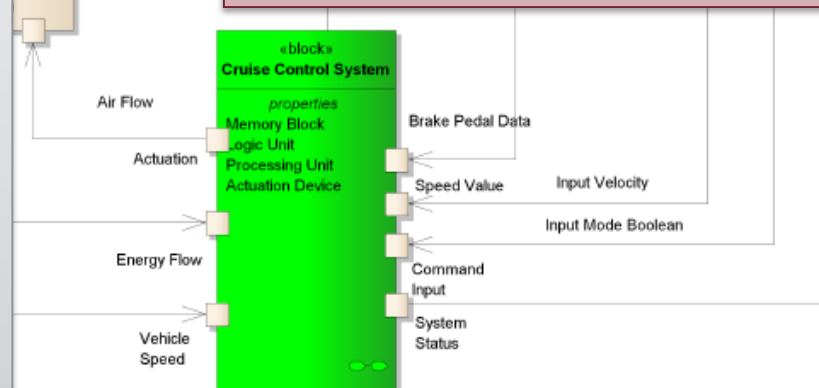
- Vezérlőjel
- Tempomat ki/be

## ■ REMO:

- Funkcionális dekompozíció
- Strukturális modellek (pl. példány- és típusgráf)

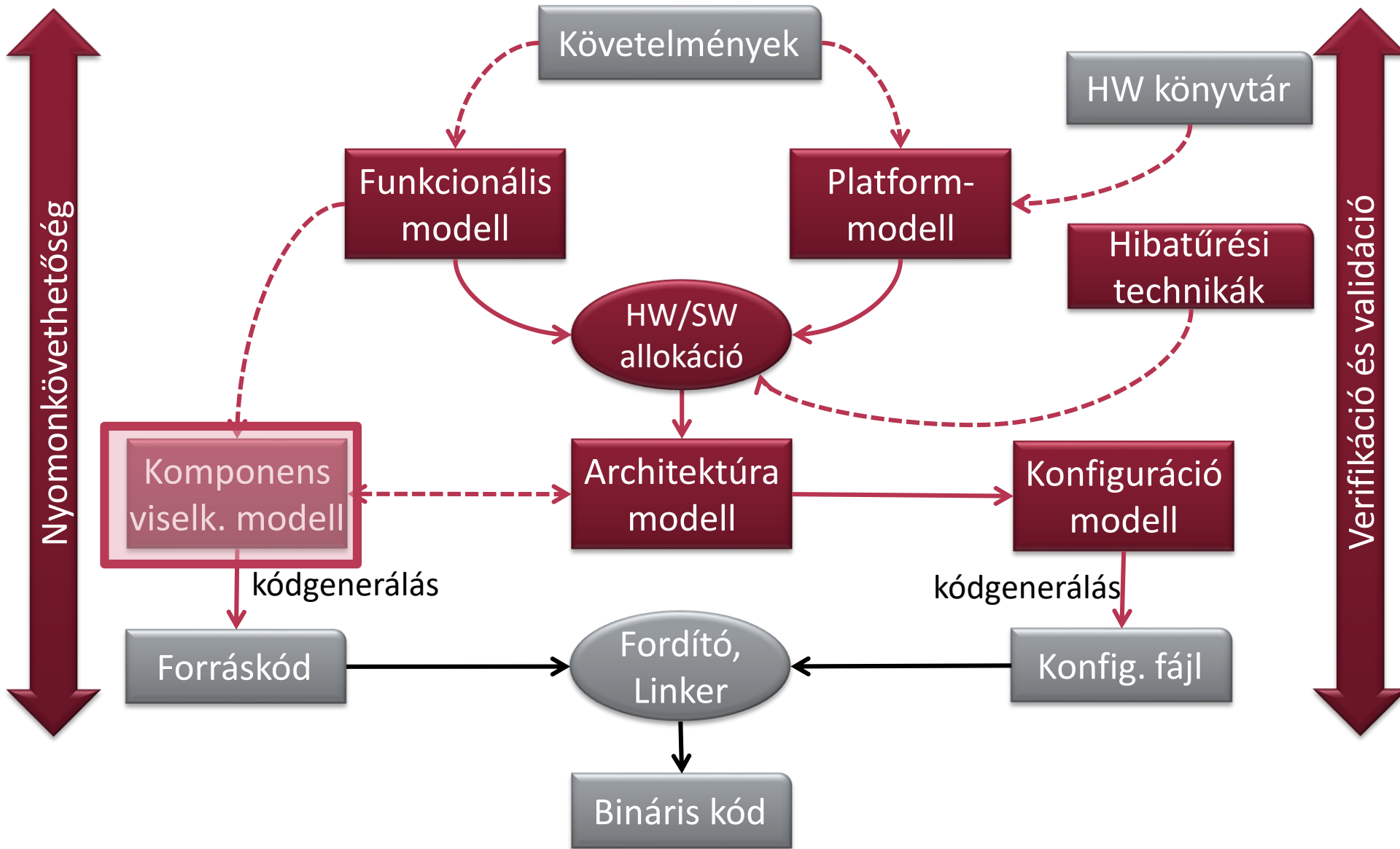
## ■ RETE (SysML/UML):

- Osztály diagram
- Komponens diagram
- (Internal) Block diagram





# Platform-alapú rendszertervezés

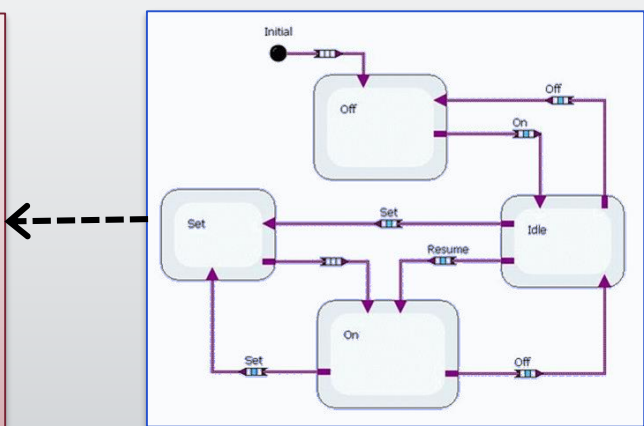
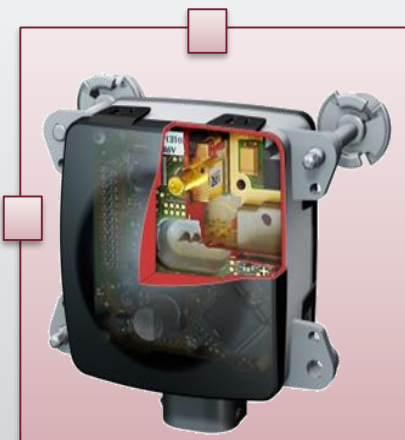
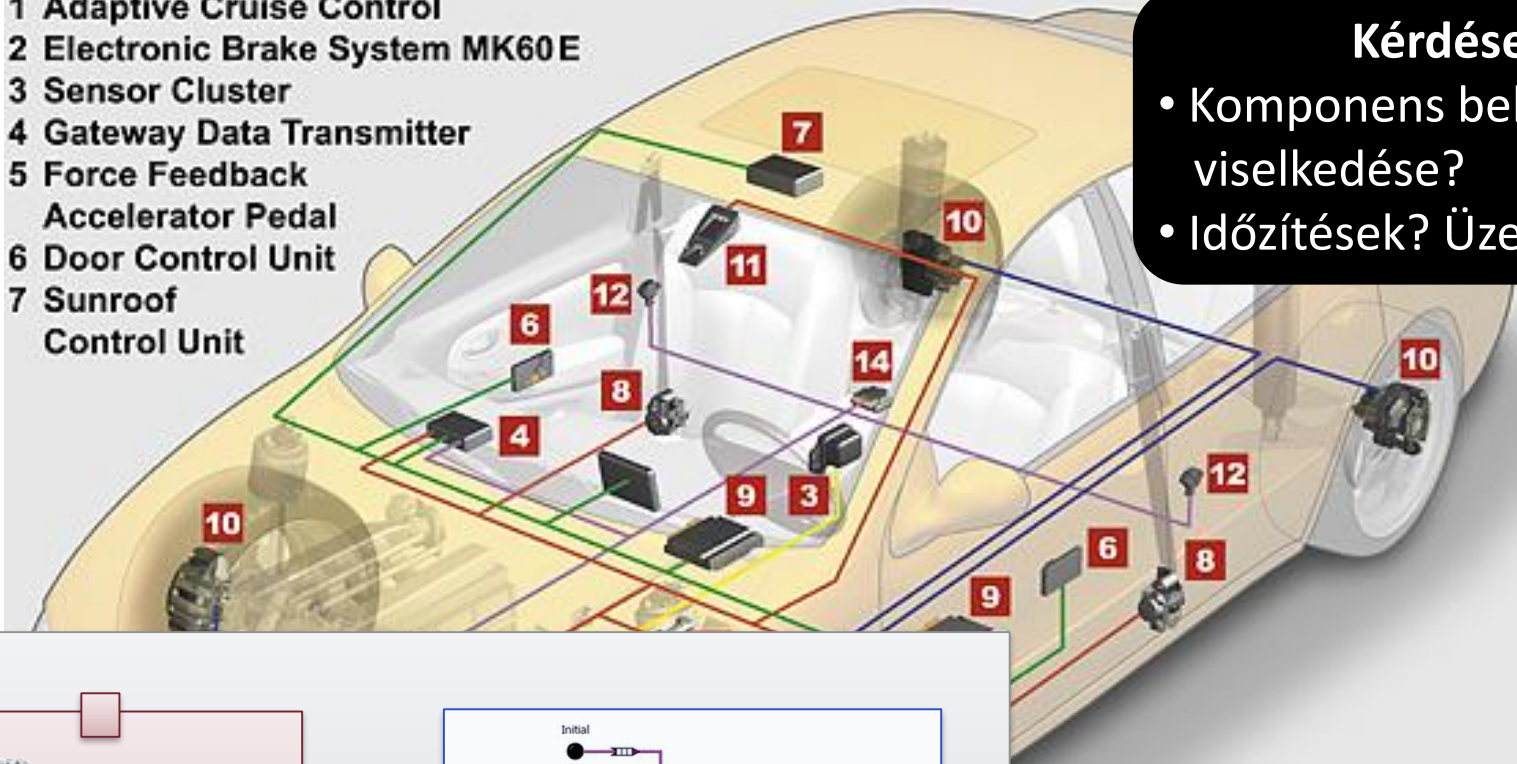


# Komponens terv

- 1 Adaptive Cruise Control
- 2 Electronic Brake System MK60 E
- 3 Sensor Cluster
- 4 Gateway Data Transmitter
- 5 Force Feedback Accelerator Pedal
- 6 Door Control Unit
- 7 Sunroof Control Unit

**Kérdések:**

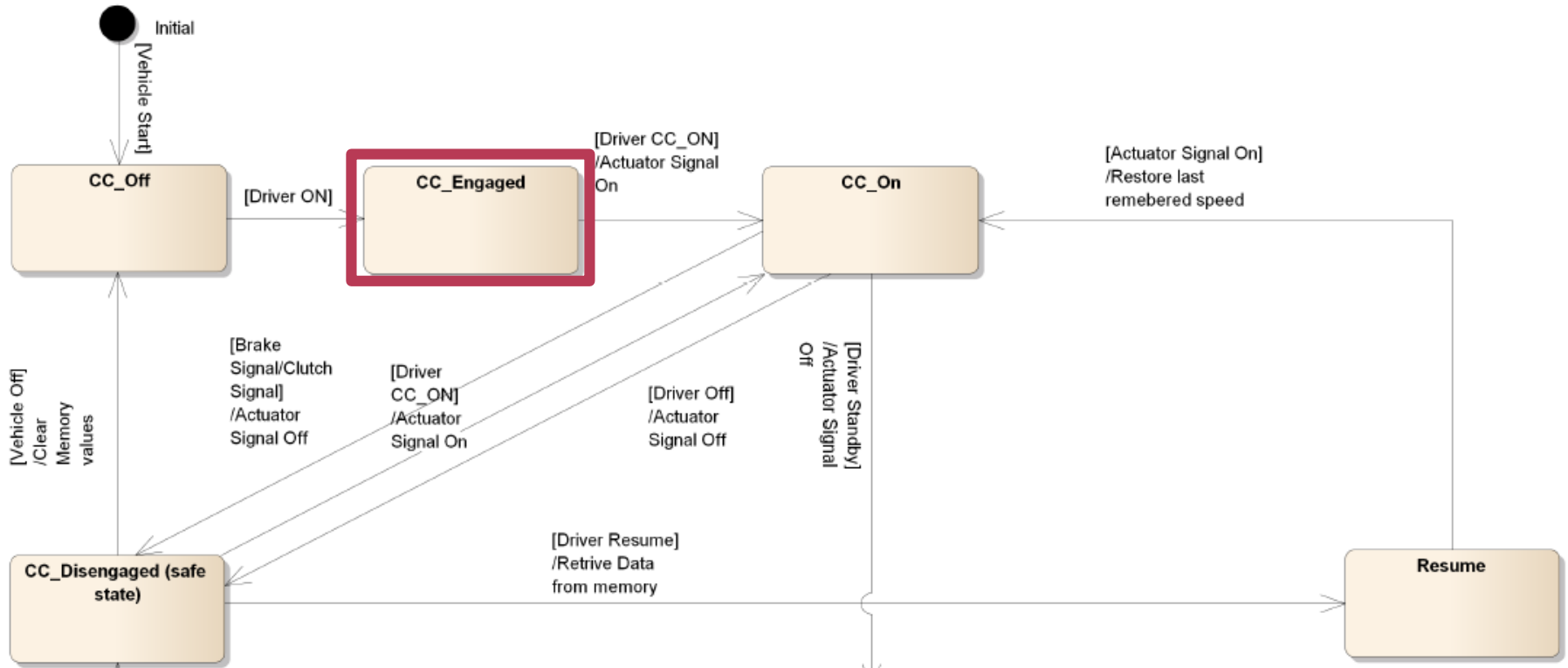
- Komponens belső viselkedése?
- Időzítések? Üzenetküldés?



- 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

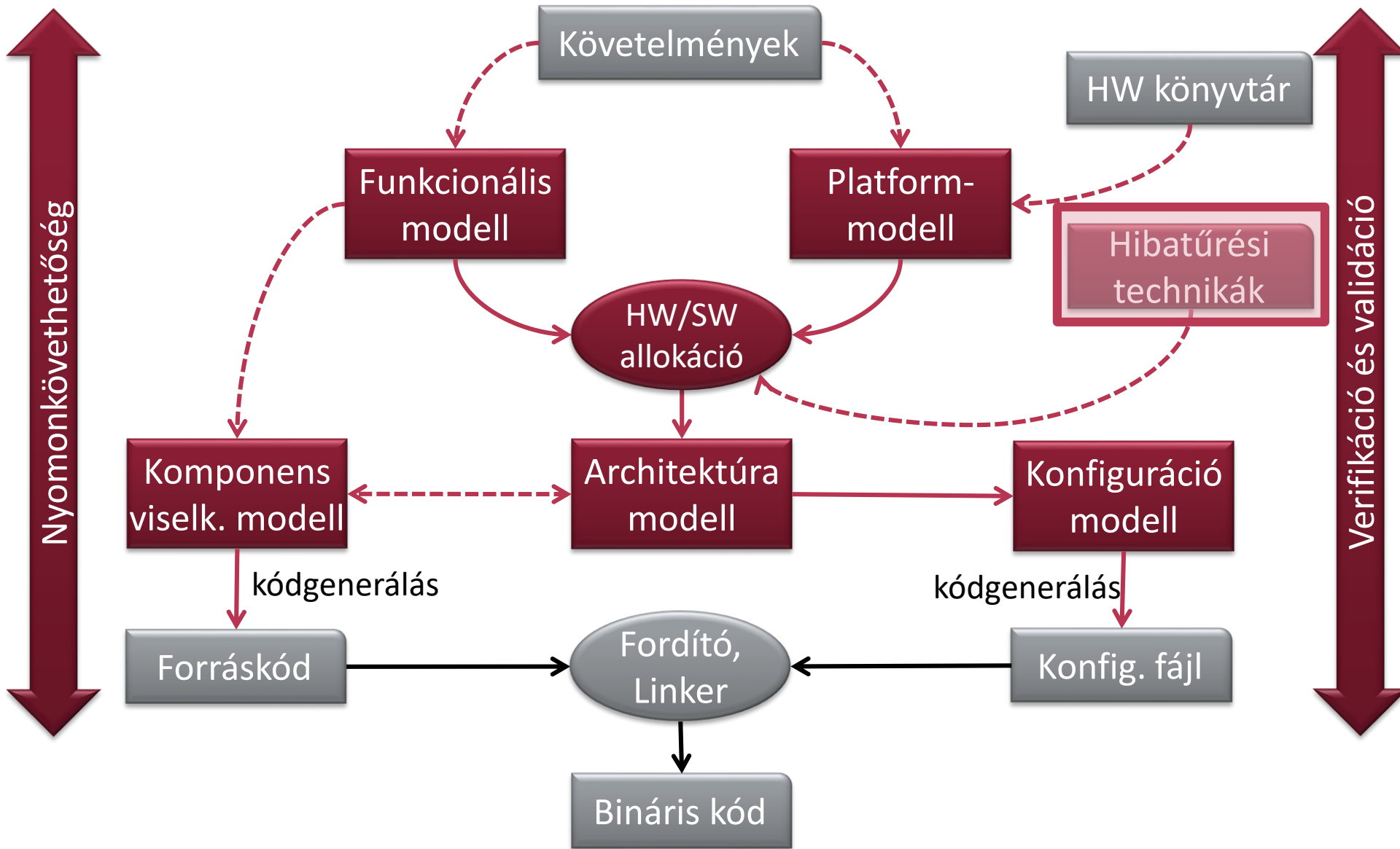
stm [StateMachine] StateMachine [StateMachine]



- 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

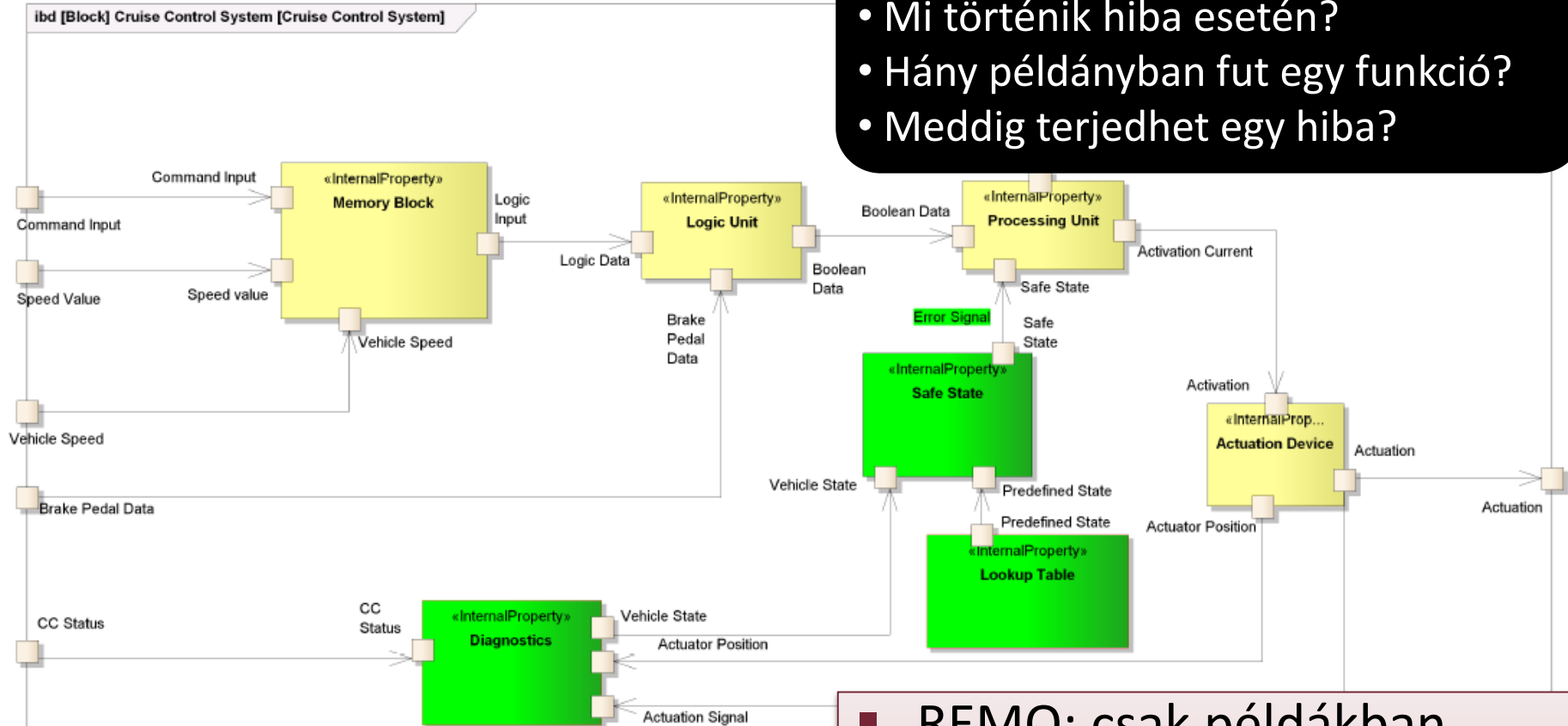
# Platform-alapú rendszertervezés



# Biztonságra tervezés / Hibatűrés

## Kérdések:

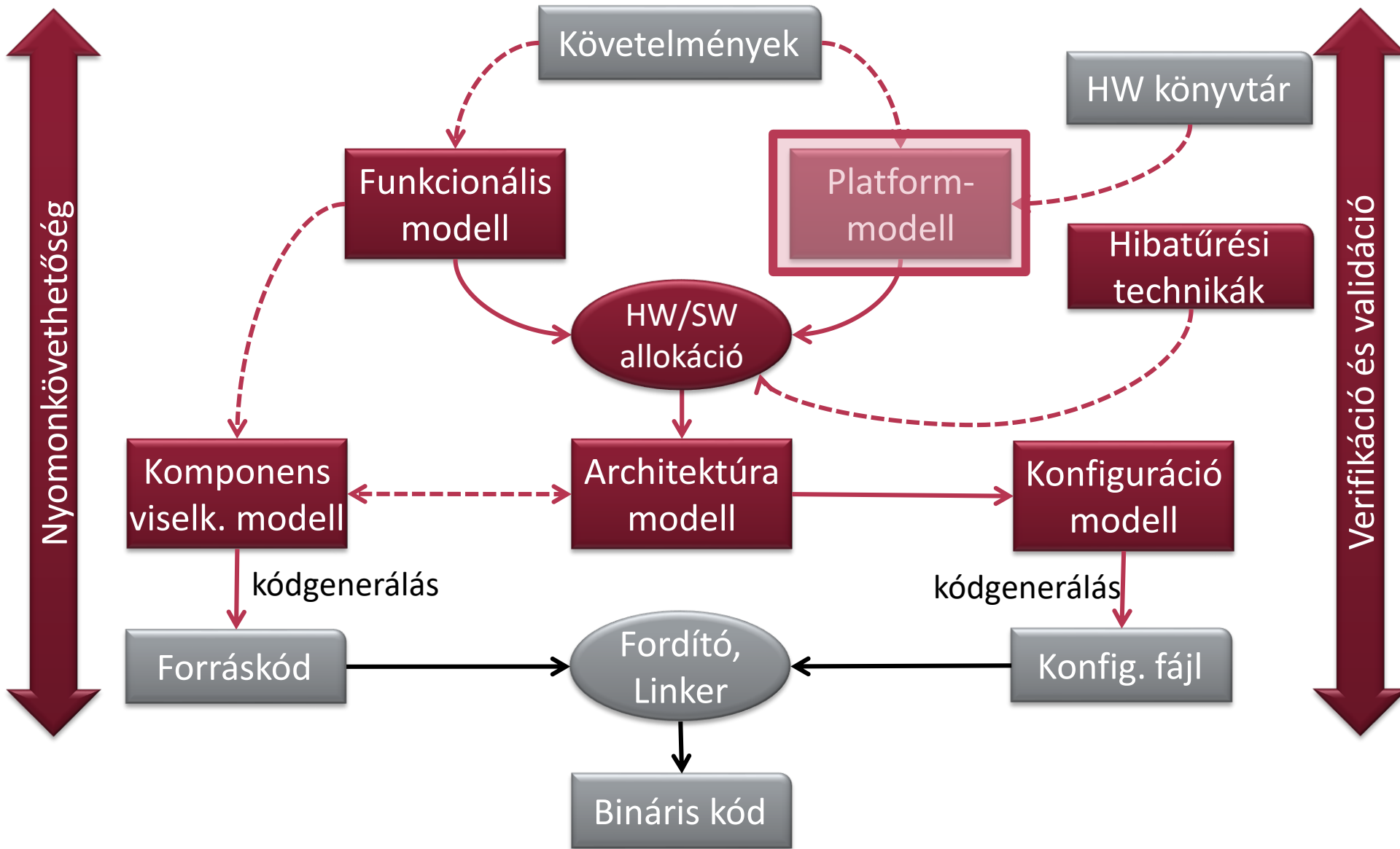
- Mi történik hiba esetén?
- Hány példányban fut egy funkció?
- Meddig terjedhet egy hiba?



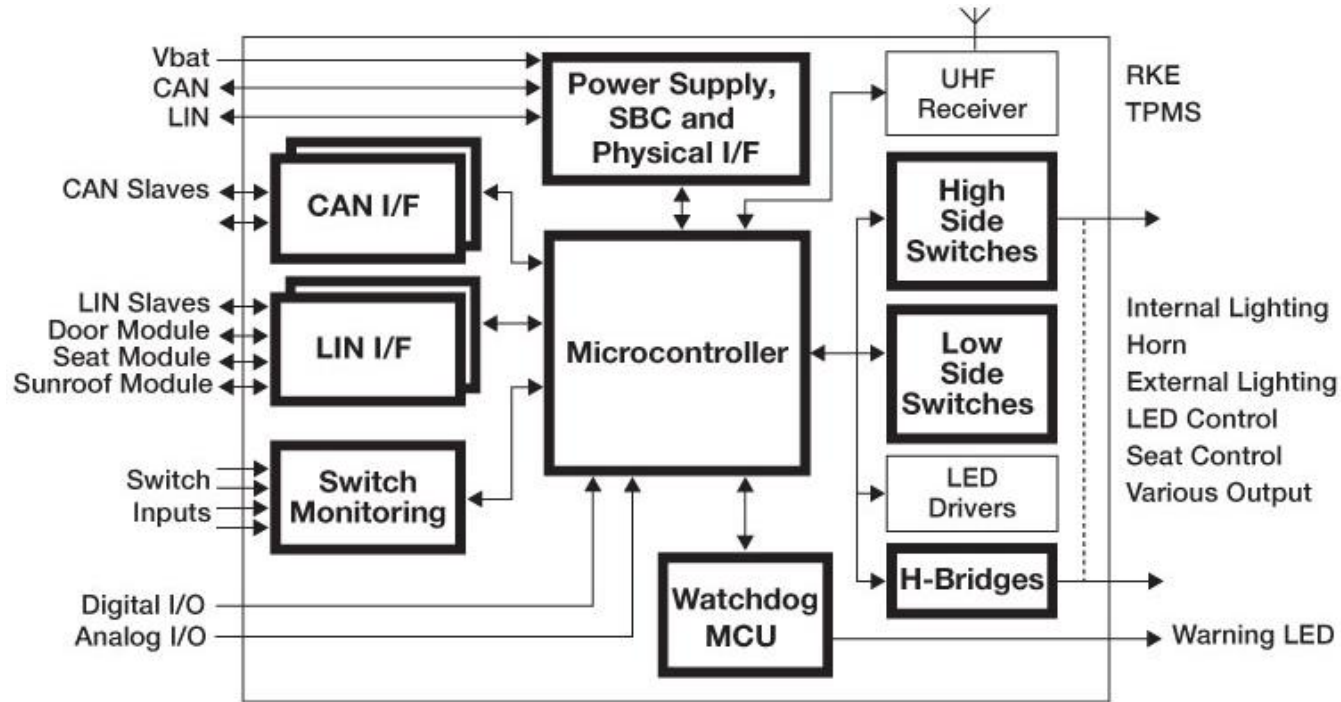
- Tempomat-kimenet monitorozása
- Összehasonlítás tárolt adatokkal
- Jelentős eltérés esetén hibajelzés
- Hibajelzés esetén deaktiválás

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

# Platform-alapú rendszertervezés



# Platform modellezés

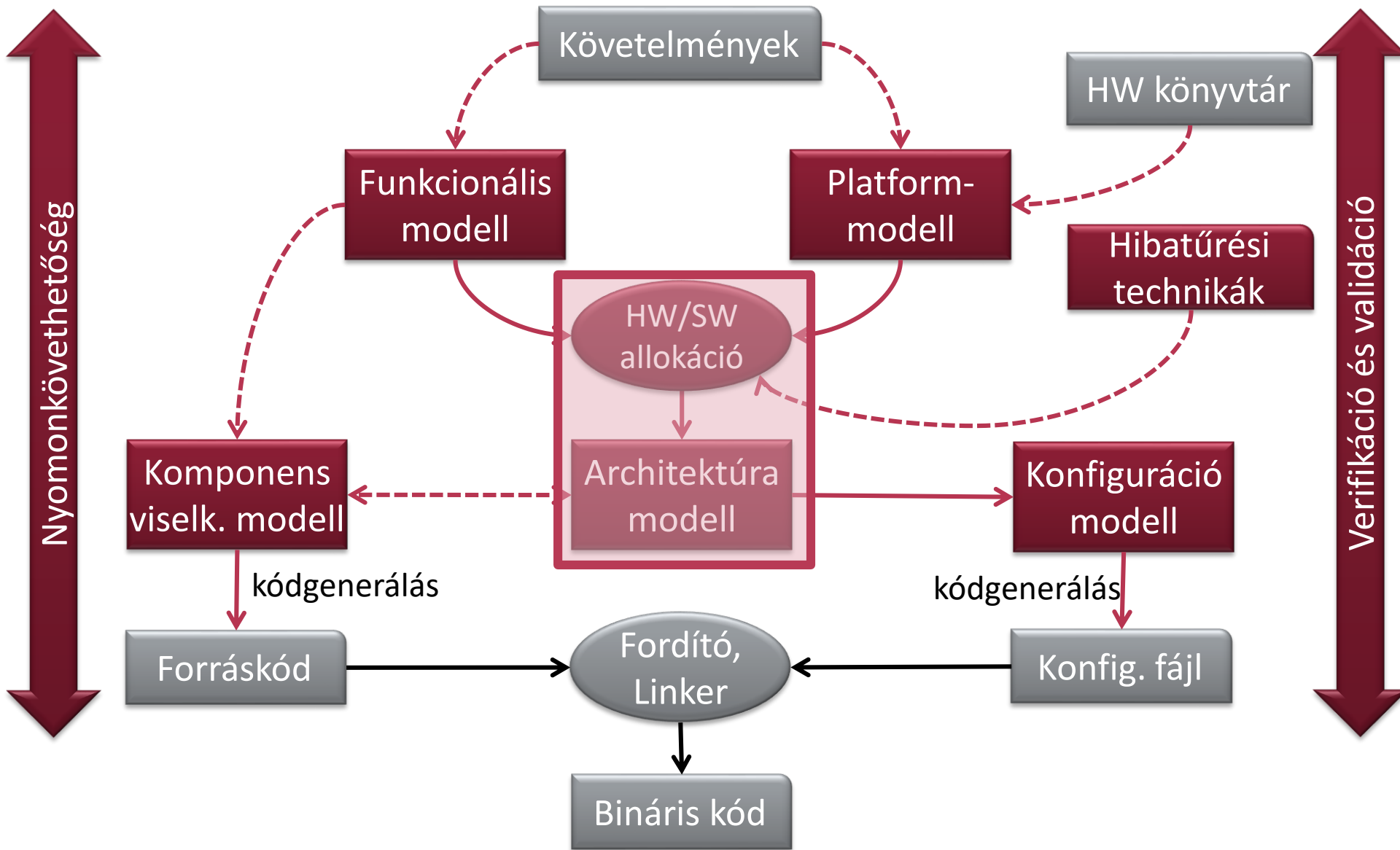


## Példa

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

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

# Platform-alapú rendszertervezés





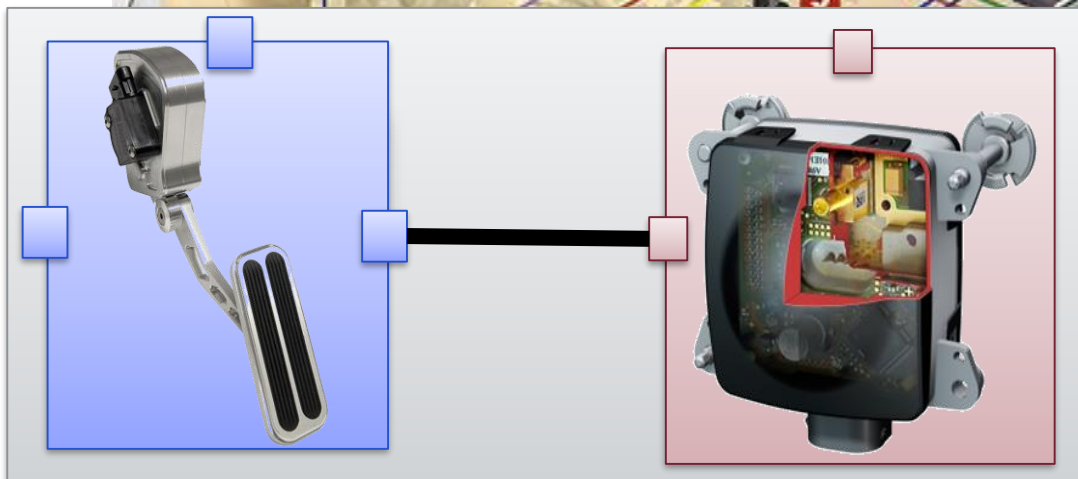
# Architektúra terv (aka. Rendszermodell)

- 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:

A funkciók példányai

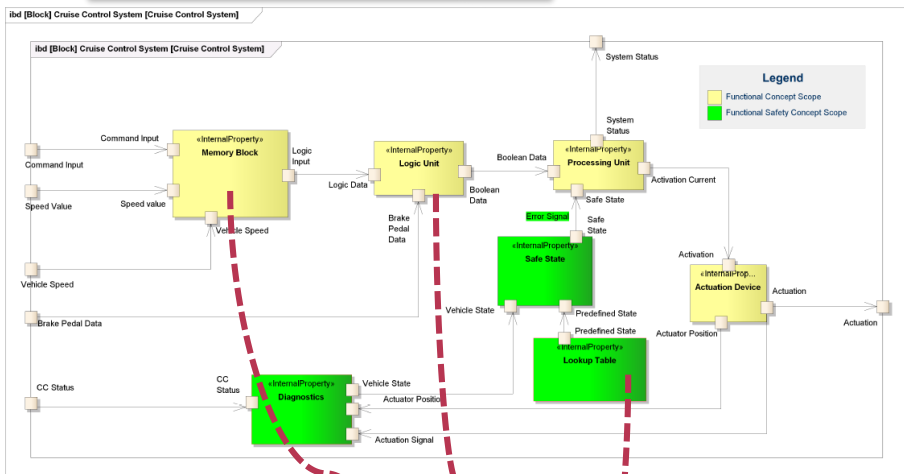
- Hol / mikor futnak?
- Mikor kommunikálnak?
- Melyik buszon?
- Mivel áll kapcsolatban?



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

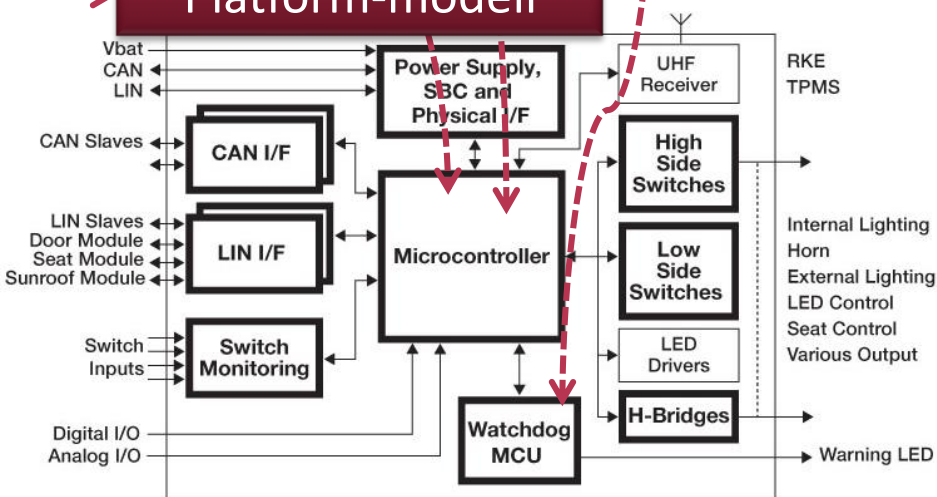
# Példa: Architektúra terv (Rendszermodell)

## Funkcionális modell



HW/SW  
allokáció

## Platform-modell



## REMO

- Nemfunkcionális követelmények
- Teljesítménymodellezés

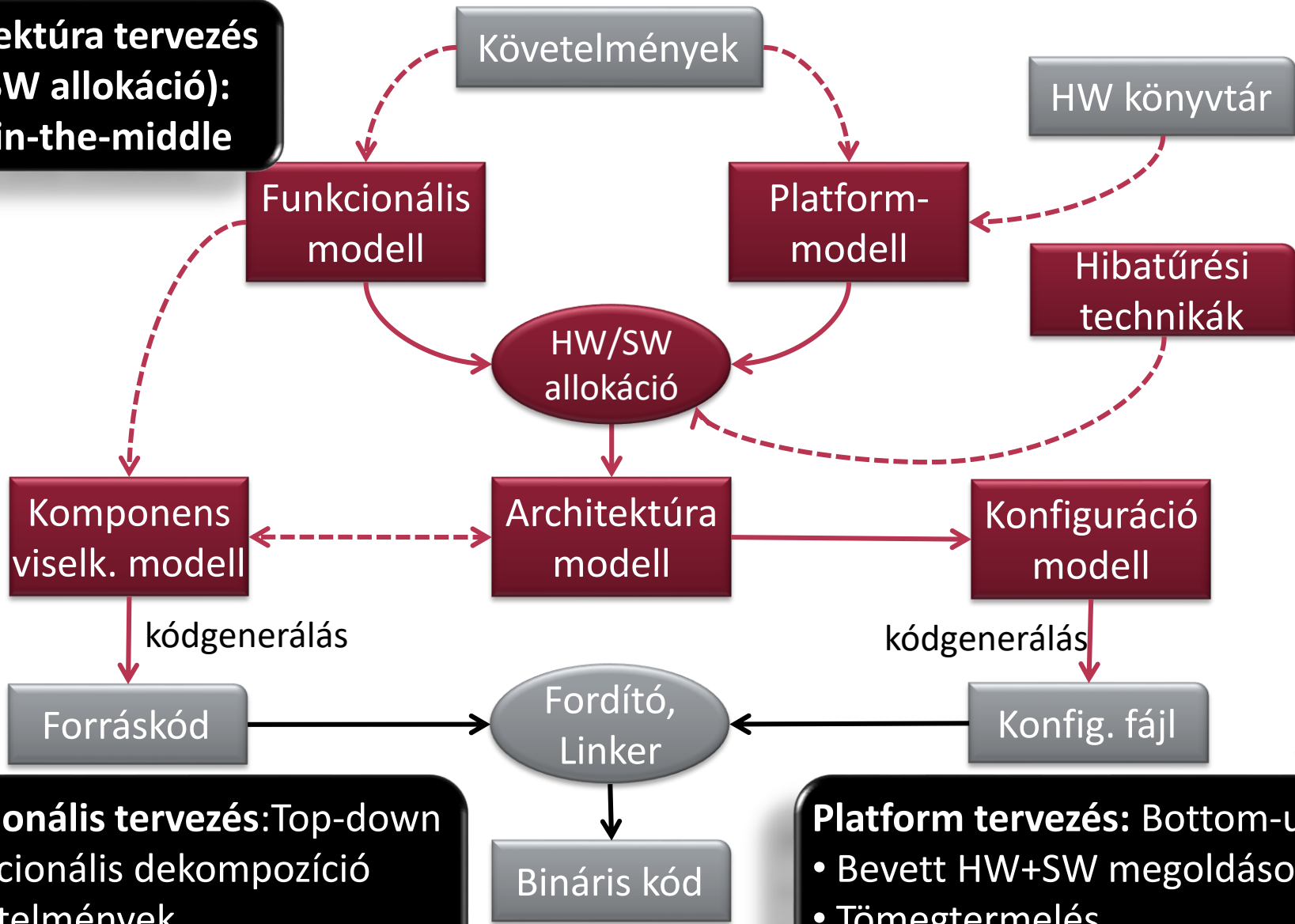
## RETE

- Nemfunkcionális követelmények analízise
  - Ütemezés
  - Rendelkezésre állás
- Allokáció és telepítés

# Platform-alapú rendszertervezés

**Architektúra tervezés (HW/SW allokáció): Meet-in-the-middle**

Nyomonkövethetőség



Verifikáció és validáció

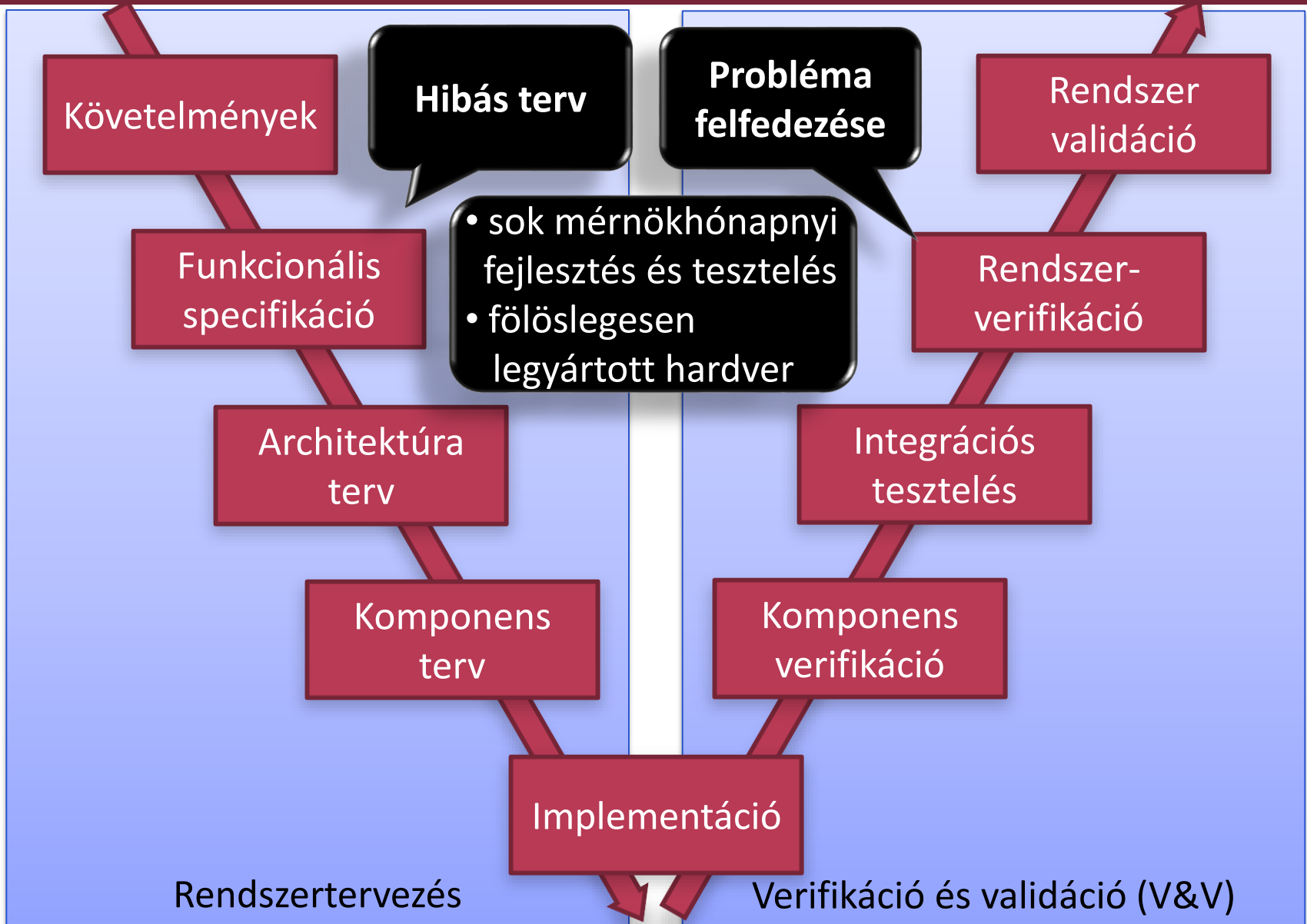
**Funkcionális tervezés: Top-down**  
• Funkcionális dekompozíció  
• Követelmények nyomonkövethetősége

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

# VERIFIKÁCIÓ ÉS VALIDÁCIÓ A RENDSZERTERVEZÉSBEN

Miért működik mégis egy ennyire komplex rendszer?

# Motiváció



# V&V technikák a képzésben

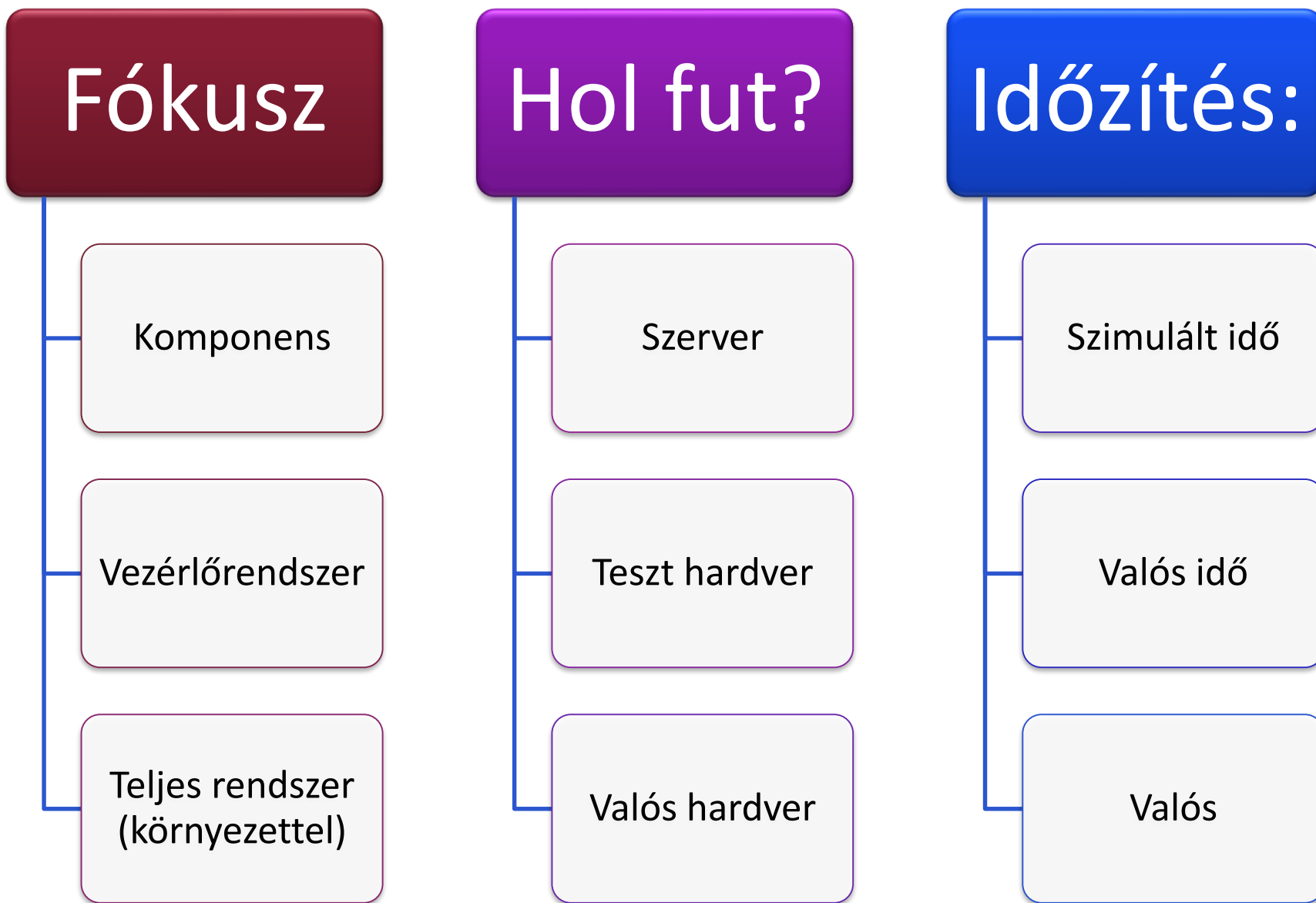
- REMO
  - Szimuláció (folyamat)
  - Tesztelés (orákulum / fedettség / öntesztelés)
  - Modellellenőrzés alapok
- RETE
  - Követelmény alapú tesztelés
  - Modellalapú tesztelés
- Ipari Informatika
  - HIL / SIL
  - Szimuláció
- Szoftver- és rendszerellenőrzés (MSc)
  - Számos további módszer

Implementáció

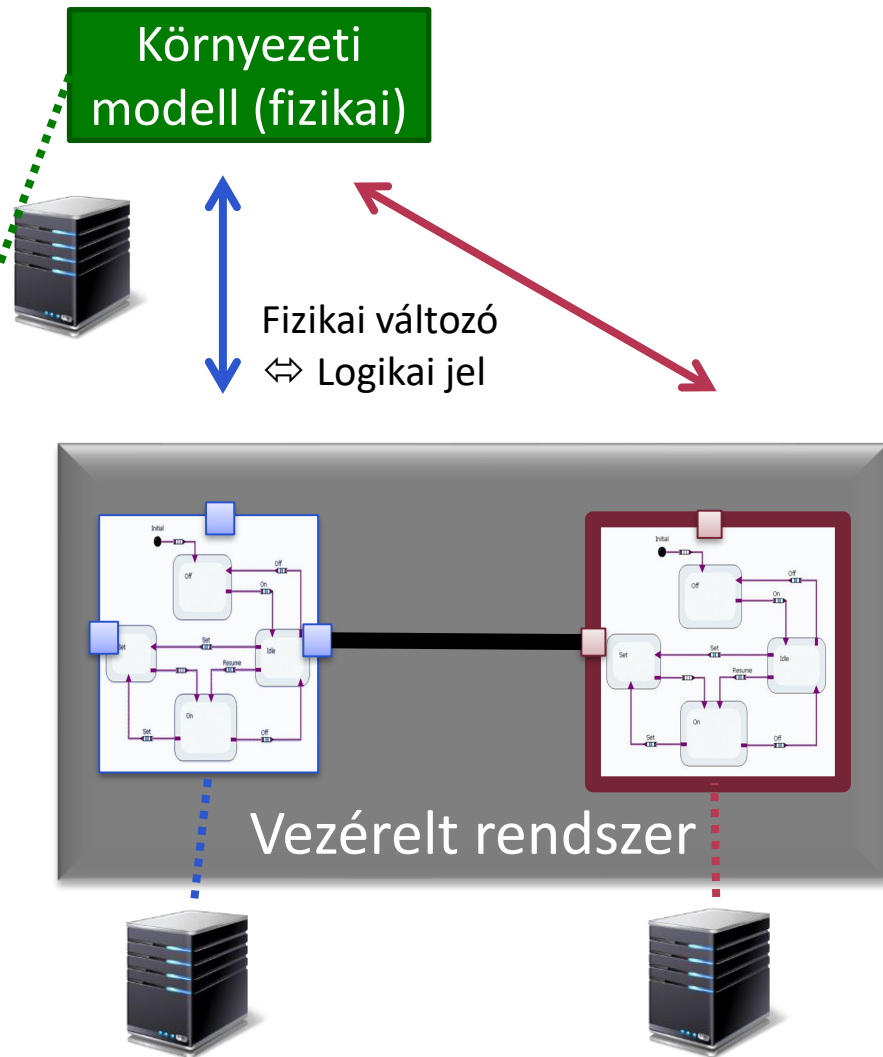
Verifikáció és validáció (V&V)



# Szimuláció/tesztelés alapú verifikáció és validáció



# Komponens verifikáció

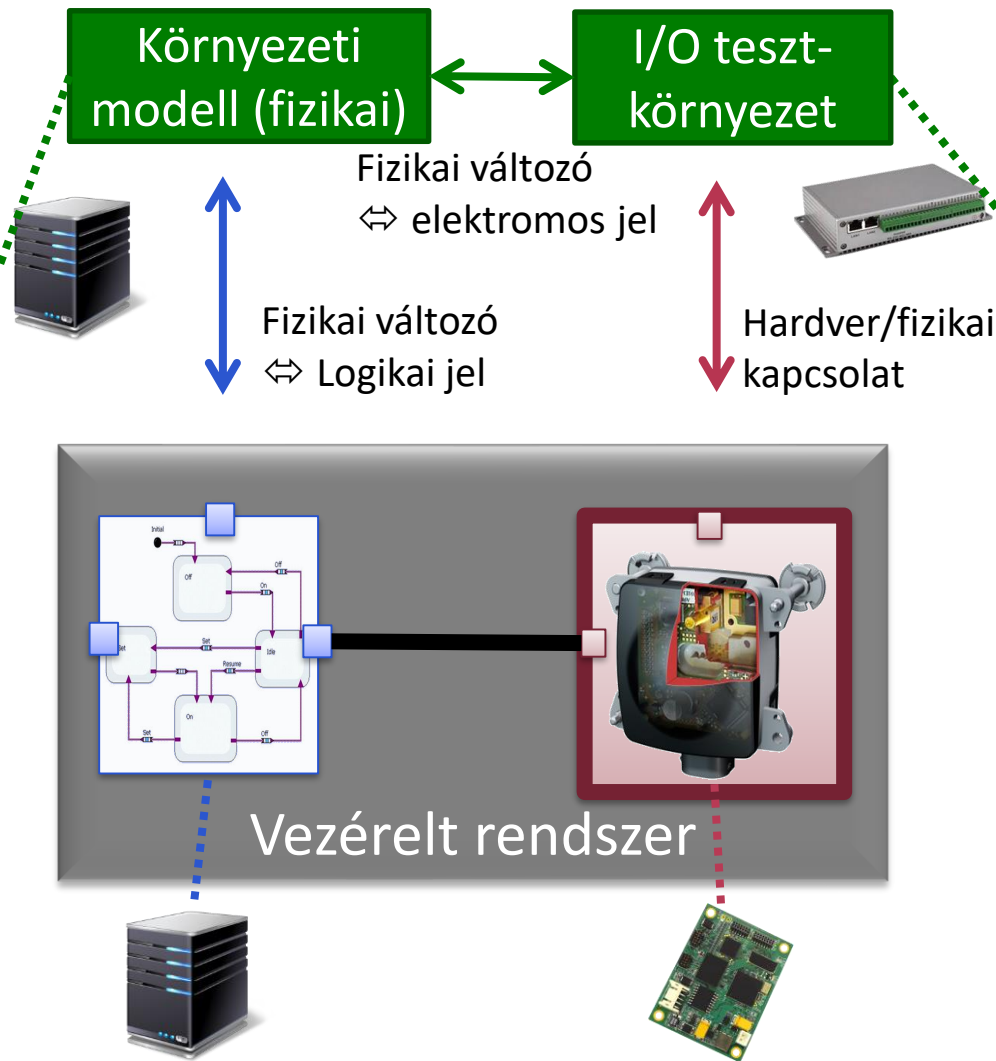


## Software-in-the-loop

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



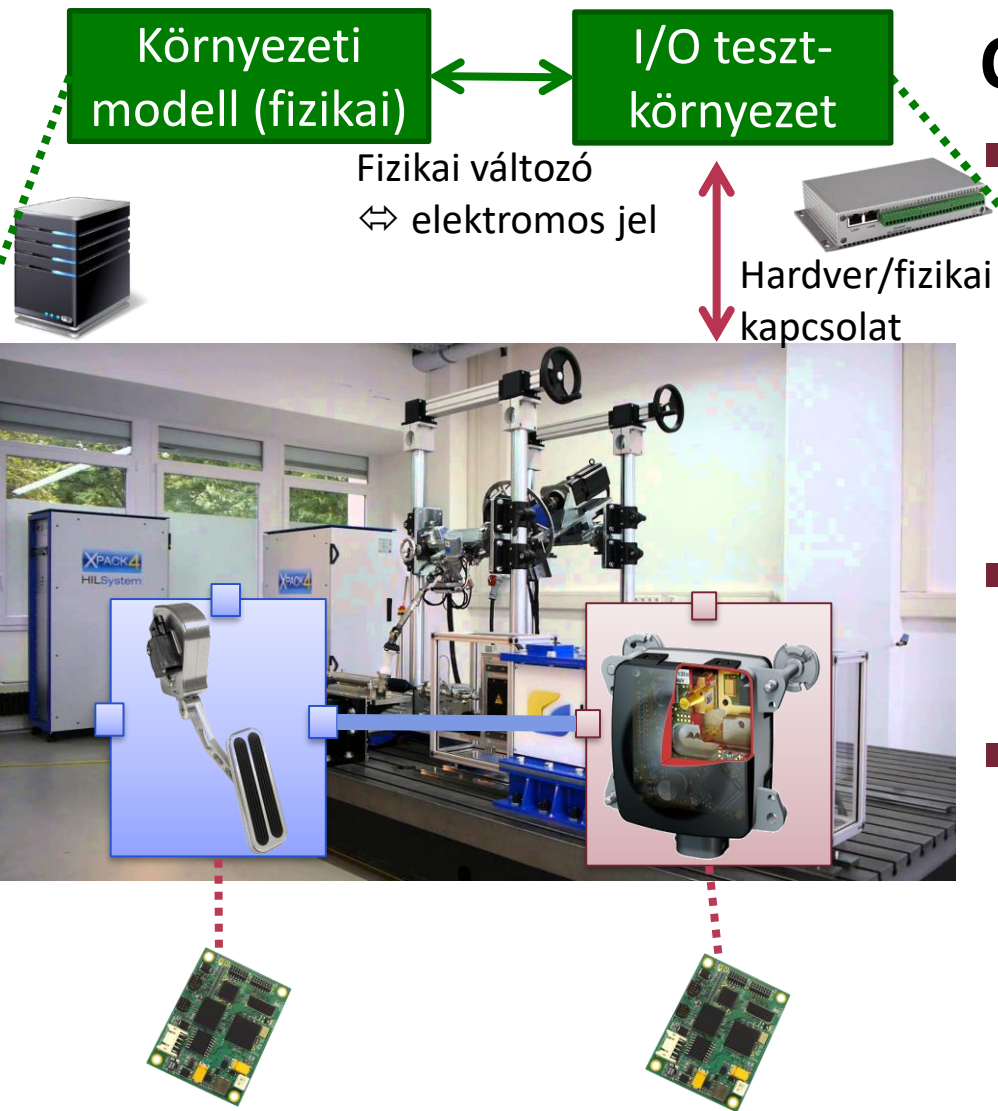
# Integrációs tesztelés



## 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

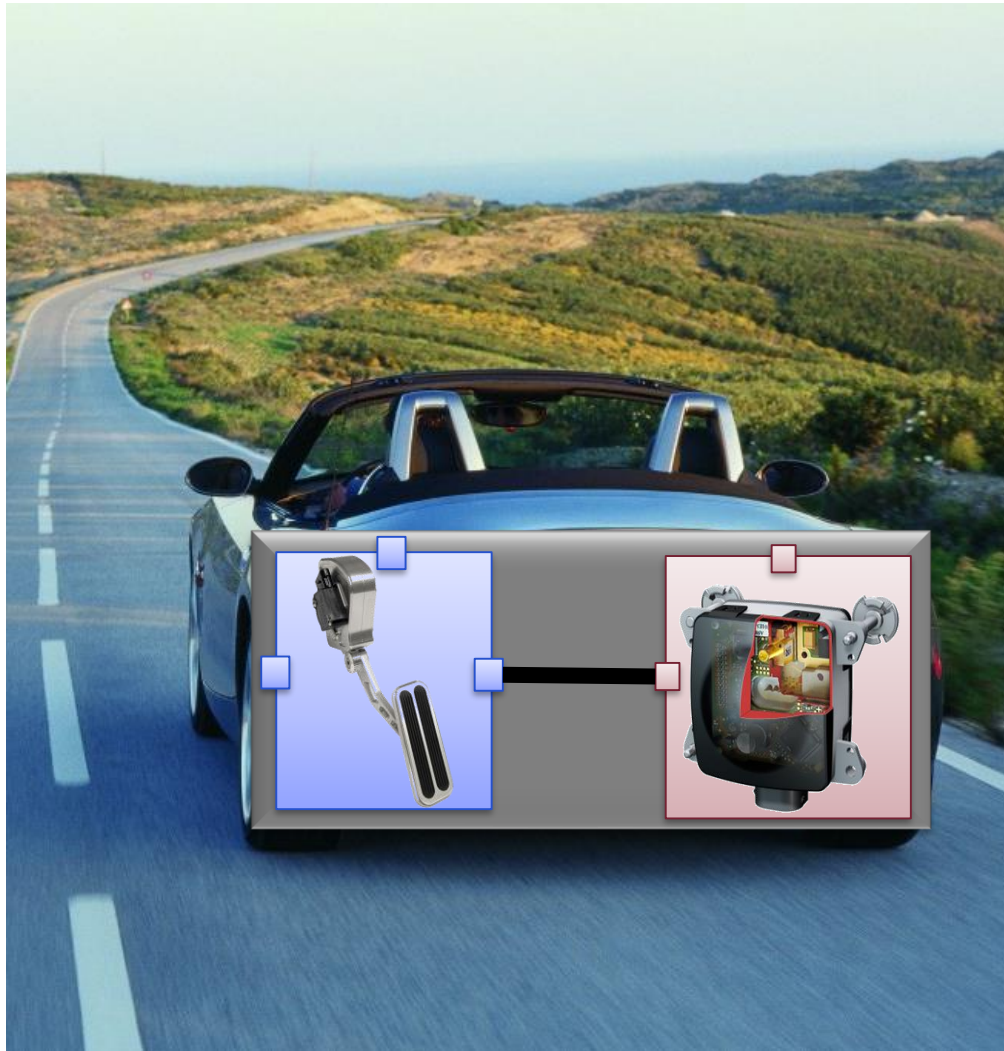
# Rendszerverifikáció



## Component-in-the-loop

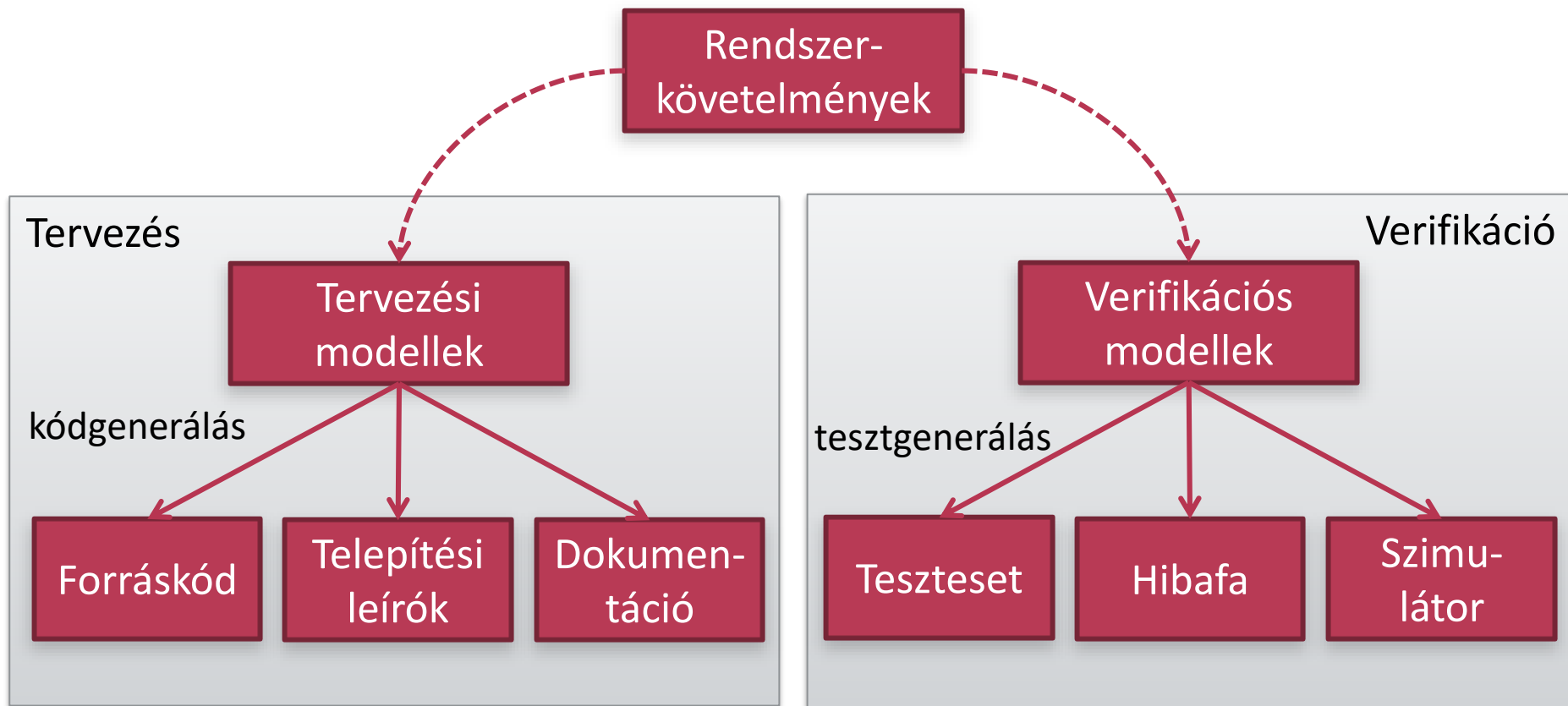
- **Rendszer: Integrált**
  - Valós hardverre telepített komponensek
  - Elektromos integráció (vezérlőjelek, tápellátás)
  - Valós működés
- **Fizikai környezet:**
  - Valós idejű, szimulált
- **Ellenőrzés:**
  - Korábbi mérési adatok (benchmark)
  - Virtuális törésteszt, stb.

# 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

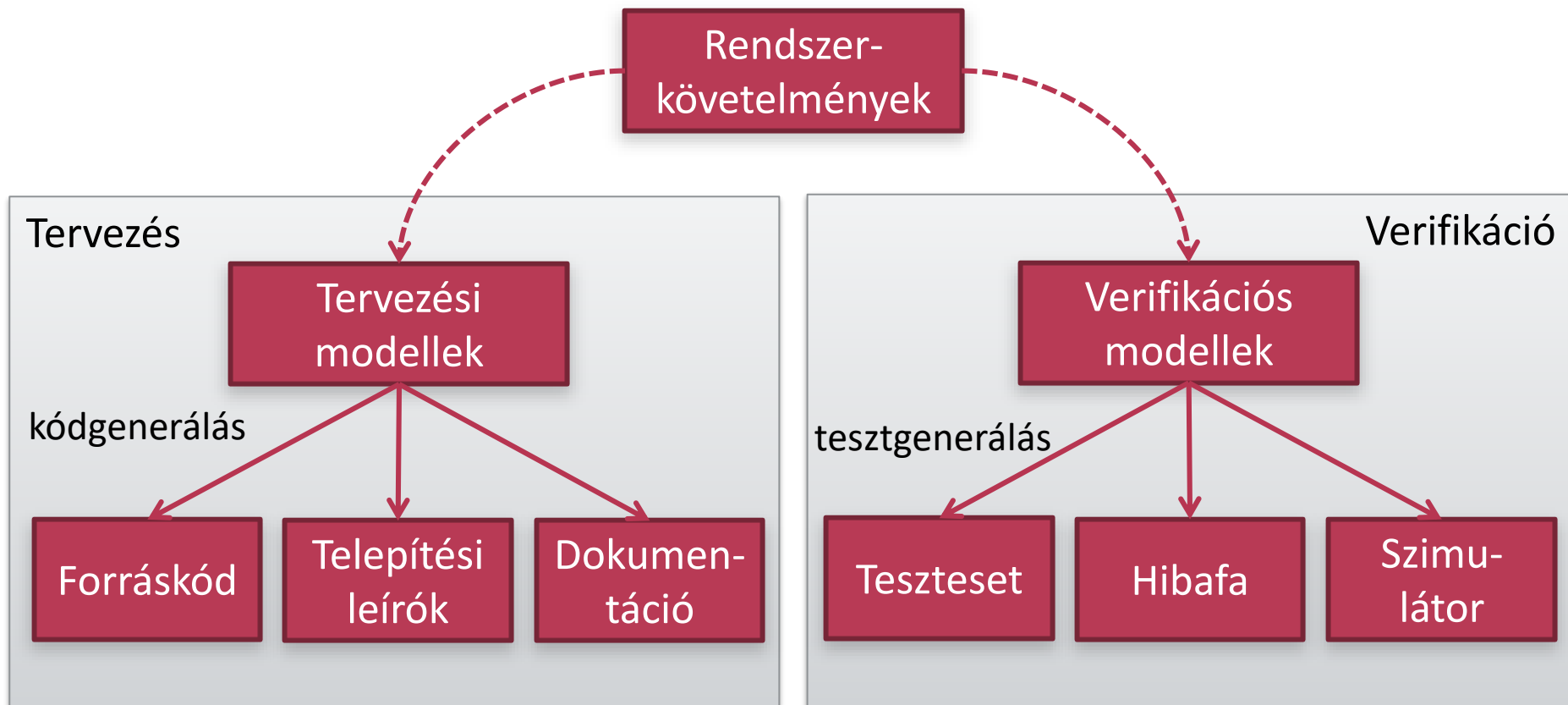
# Modellek felhasználási célja



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

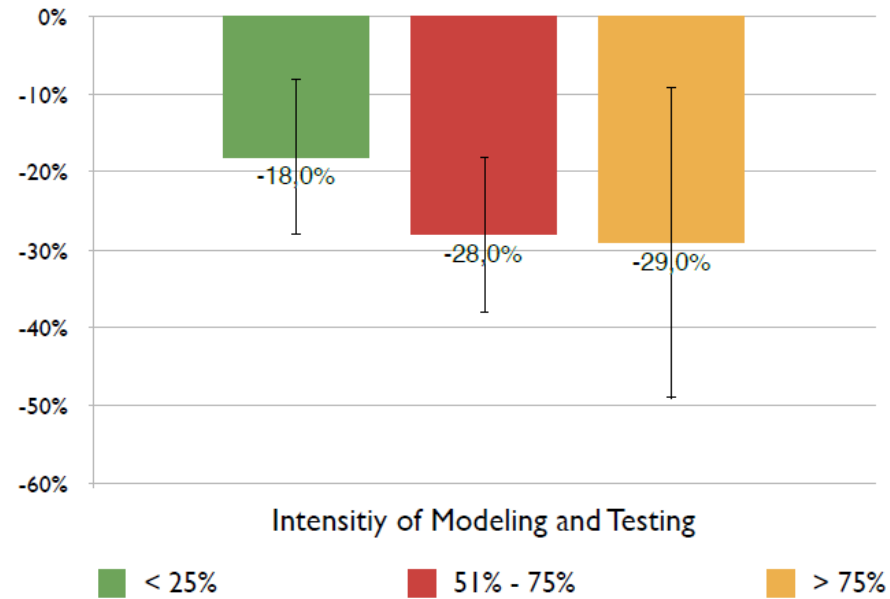
# A modell alapú tervezés előnyei

## ■ Jellegzetességek:

- Tervezés:
  - 30-40%-kal több idő/költség
- Ellenőrzés:
  - Átlagosan 40%-kal kevesebb
- Kódgenerálás:
  - >90% a résztvevők 40%-nál!
  - 40-50%-os megtakarítás
- 3 éves megtérülés

## ■ Miért?

- Tervezési hibák 60%-a korai fázisban felderíthető
- Virtuális prototípusok

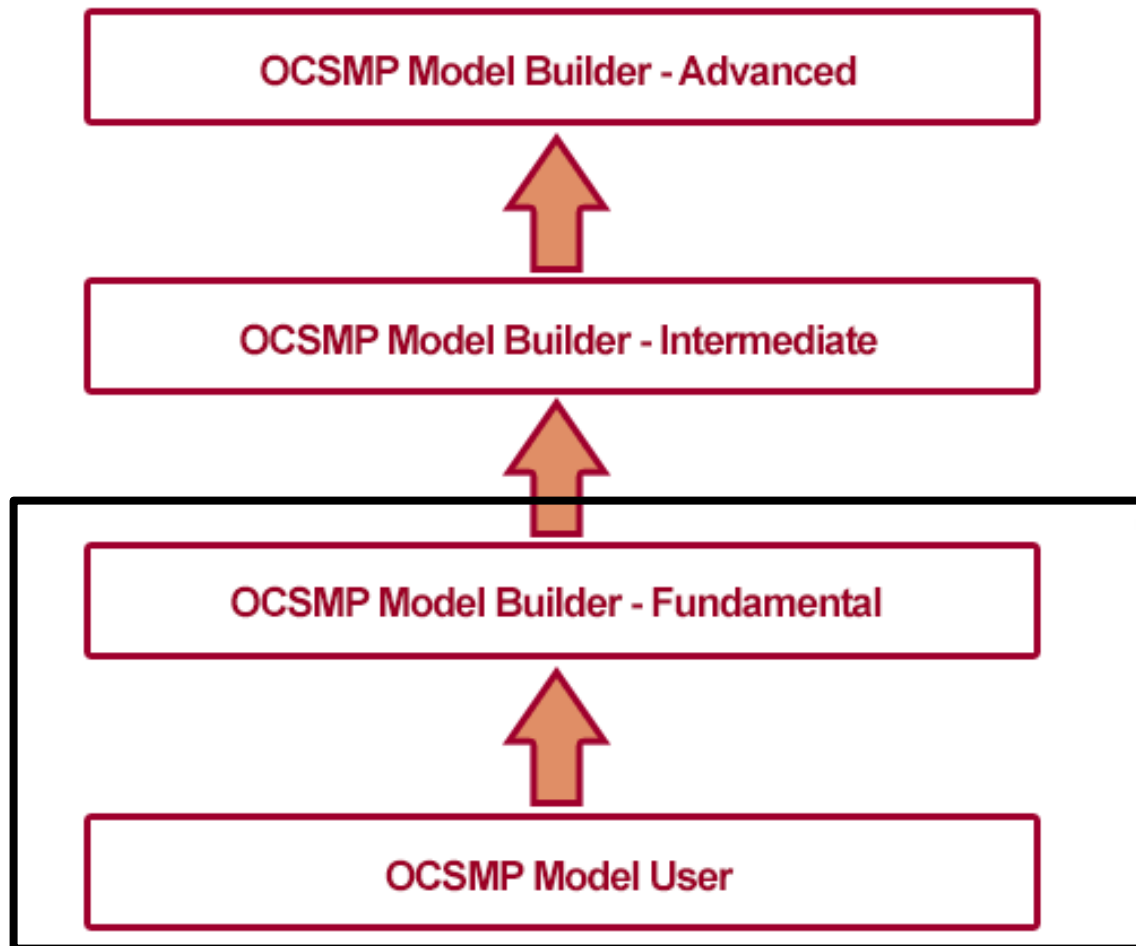


### Felmérés:

- autóiipari szereplők
- 180 ember (14 országból)
- menedzserek, fejlesztők, R&D

# Mit tanulhatok itt?

## OMG-Certified Systems Modeling Professional



ReTe tárgy

Tréning piaci ára:  
500-5000 EUR

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



# Megéri ezt megtanulni?

systems modelling engineer, sy...  
Search all locations

+ NOTIFY ME OF NEW JOBS (2)

**Lead Model-Based Systems Engineer**  
MITRE  
San Diego, CA 21d  
\$106K-\$173K (Glassdoor Est.)

**Model Based Systems Engineer and Systems Architect**  
Johns Hopkins University Appli...  
Laurel, MD 20d  
\$101K-\$181K (Glassdoor Est.)

**Senior Model-Based Systems Engineer**  
Aurora Flight Sciences  
Cambridge, MA 5d  
\$95K-\$170K (Glassdoor Est.)  
**NEW**

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

- Biztonság (safety) alapok
- Hibatűrő rendszer-architektúrák

Biztonságra  
tervezés

- Platform modellezés
- Nemfunkcionális analízis
- Allokáció

Architektúra  
tervezés

- Specifikáció alapú, modellalapú tesztelés
- Tesztfedettség
- Szimuláció

Verifikáció és  
validáció

- Modell-transzformáció
- Kódgenerálás

Automatizálási  
módszerek

# Összegzés: Informatikai rendszertervezés

