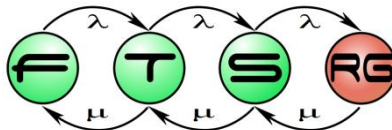
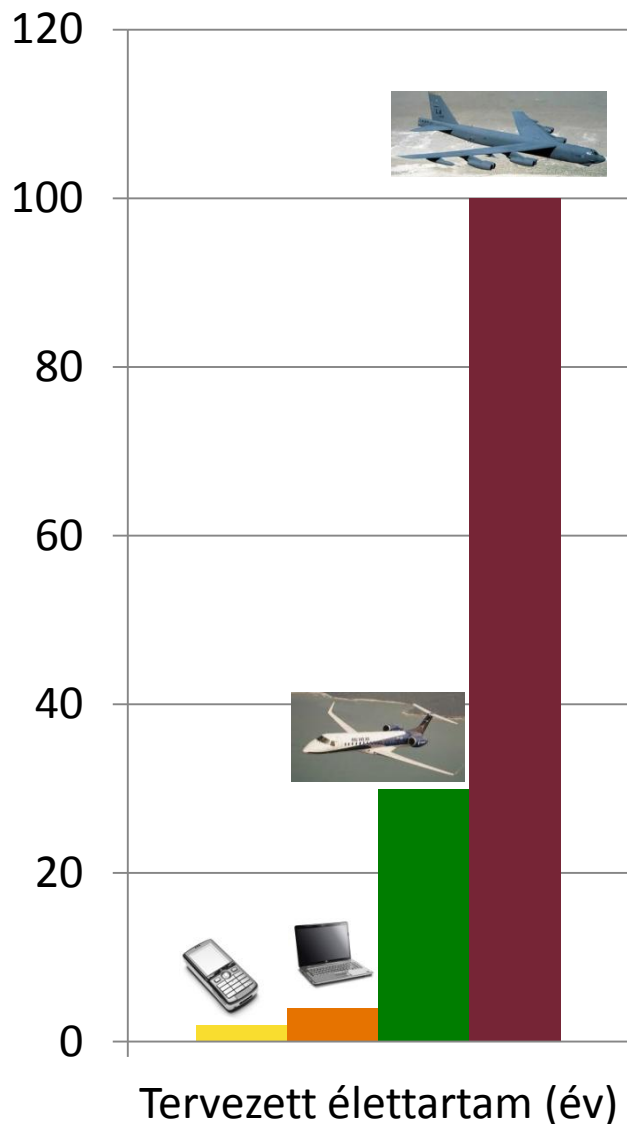


Szakterület-specifikus modellezés kritikus rendszerekben

Varró Dániel
Rendszermodellezés



Kritikus rendszerek jellemzői



Egy repülőgép várható élettartama: 30-100 év

■ Mobiltelefon

■ Laptop

■ Polgári repülőgép

■ Katonai repülőgép

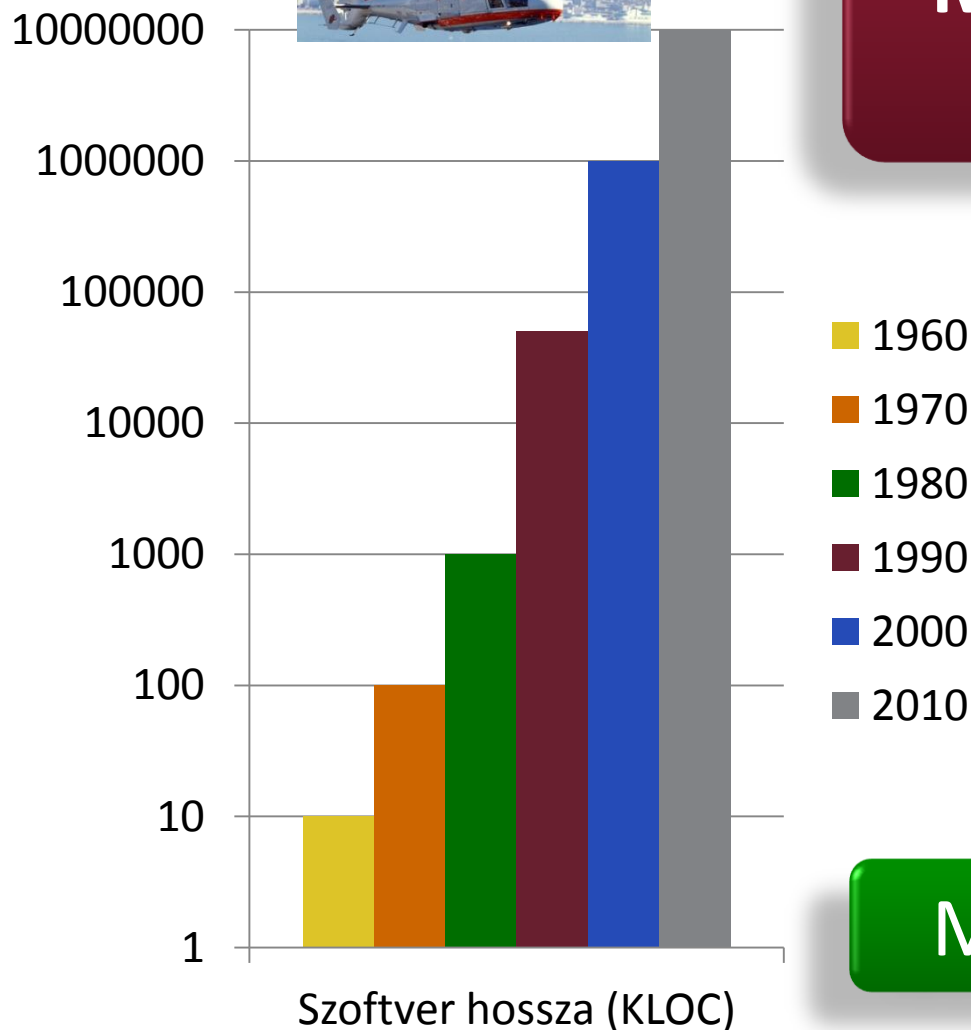
Független bizottság előtt kell igazolni, hogy repülni is fog

30 év alatt nem fordulhat elő veszélyt okozó meghibásodás!

Fő tervezési szempontok:

- kiemelt minőség
- gazdaságos gyártás
- biztonságos üzemeltetés

Kritikus rendszerek jellemzői



**Ma egy kritikus rendszer
70-80%-a szoftver!**

Minden fontos
szoftverkomponens
> 1 millió programsor

Egy átlagos programozó
1000 kódsoronként
10-12 hibát vét

Mitől működnek akkor?

Kritikus rendszerek tervezése

Modellvezérelt tervezés

- Korai hibadetekció
- Tervezési alternatívák felderítése
- Automatikus kódgenerálás
- Eszközintegráció

Előnyök:

- Minőség++, Produktivitás++
- Fejlesztési költség --
- Ellenőrzési költség --

Verifikáció és validáció

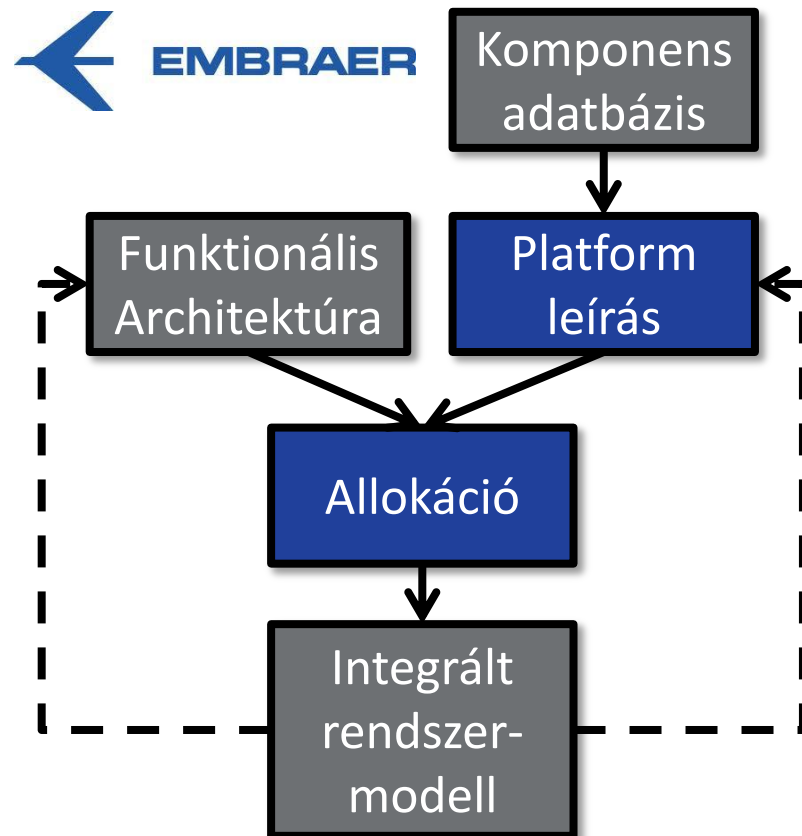
- Formális módszerek:
 - Matematikai alapú specifikációs nyelvek
 - Helyességbizonyítási algoritmusok
- Tesztelés
 - Előírt tesztlefedettség
 - Automatikus tesztgenerálás
 - Statikus kódanalízis

ARINC653 konfigurációs táblák modellvezérelt tervezése

Esettanulmány

Futó kollaborációs projekt

Cél: SW komponensek allokációja
ARINC653 alapú IMA platformra



DECOS



indexys
INControl: Exploitation of the
genesYS cross-domain architecture



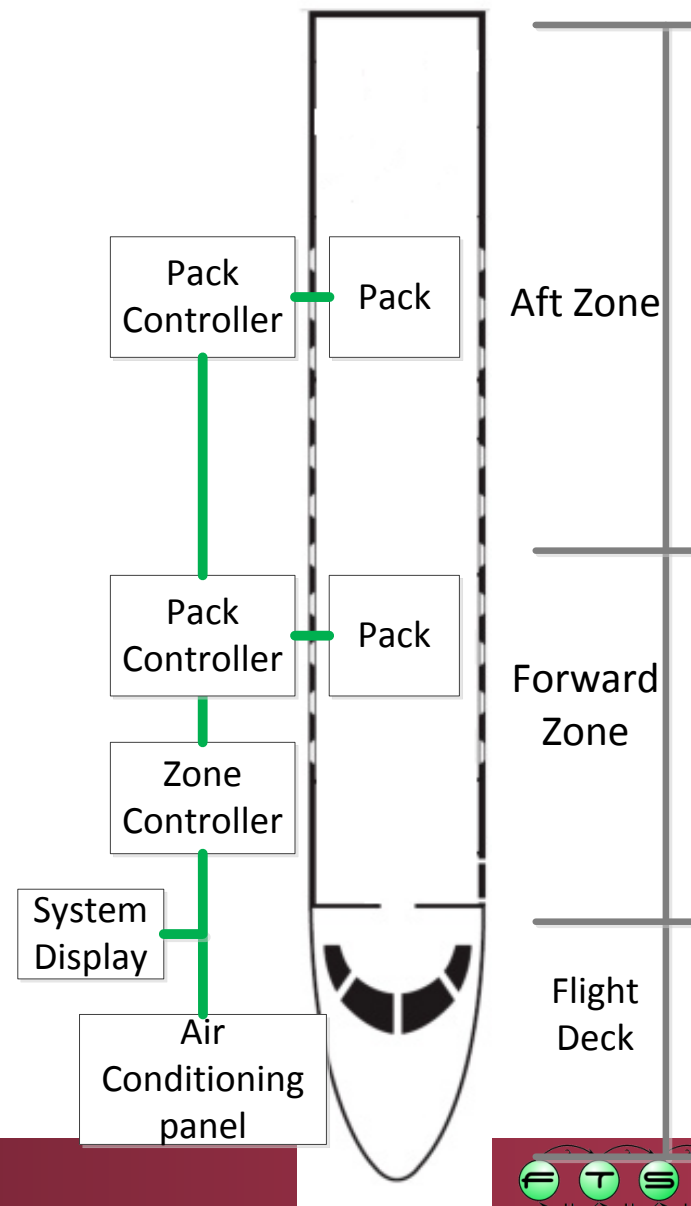
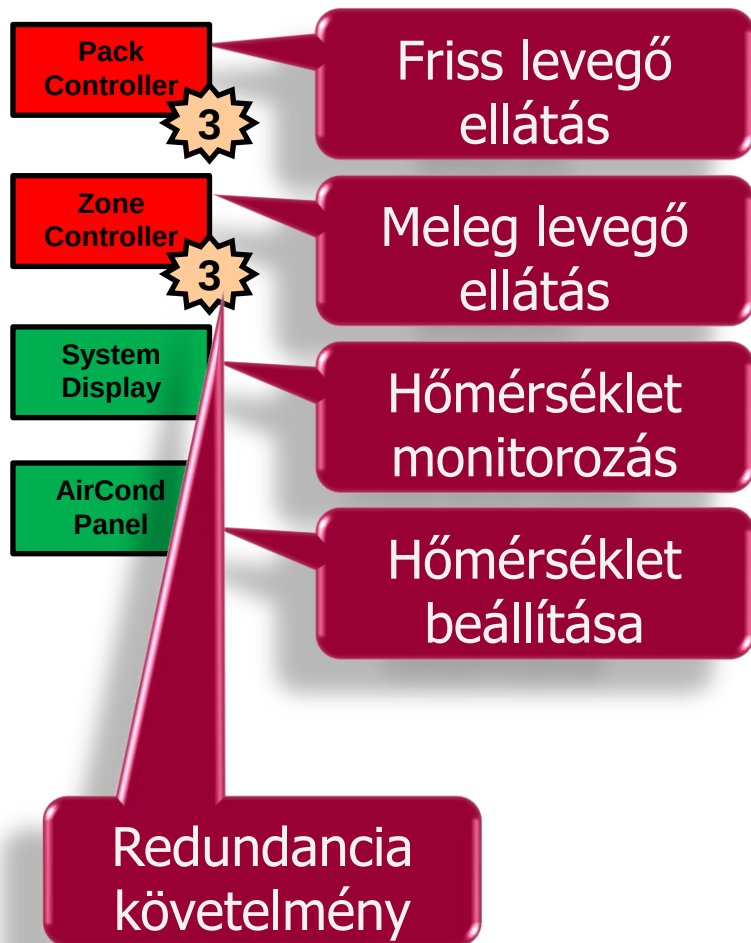
MOGENTES

secure
CHANGE



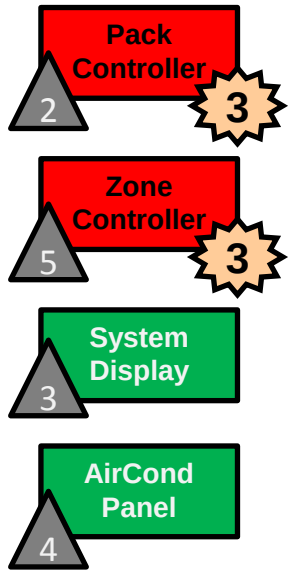
ARINC653 konfigurációk tervezése

SW funkcionalitás
(kritikus + nem kritikus)

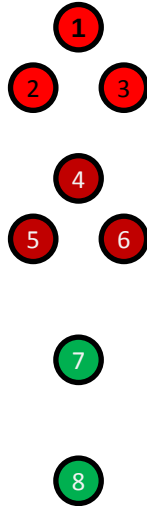


Funkciók, Példányok, Partíciók, Modulok

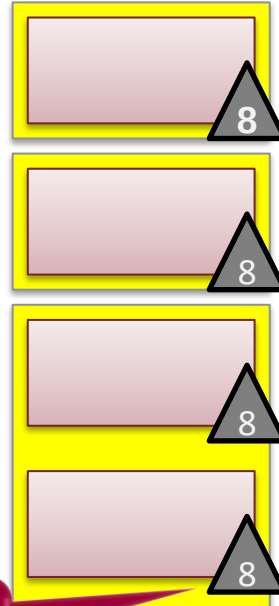
SW funkcionalitás
(kritikus + nem kritikus)



Futó példányok



Partíciók

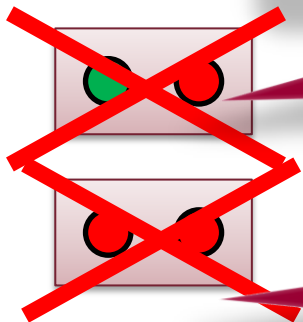


Modulok

További megkötések

- WCET,
- ütemezés, stb.
- interfészek
- adattípusok

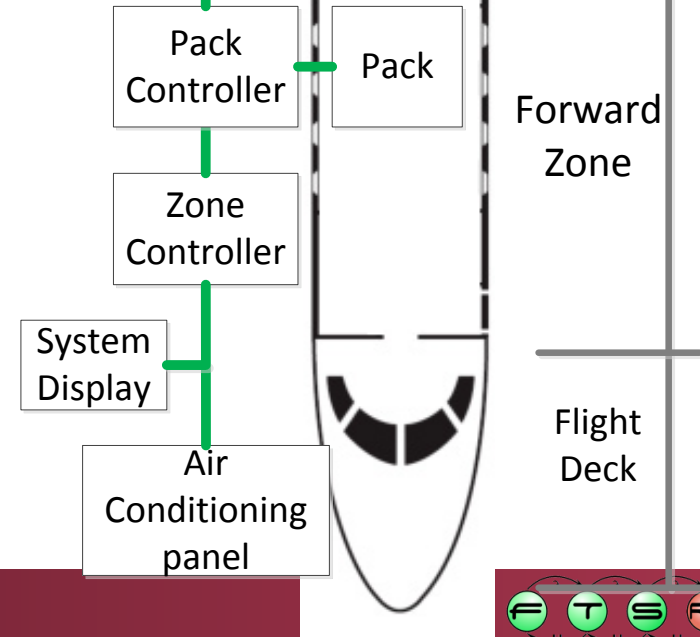
Megkötések



Memória
korlátok

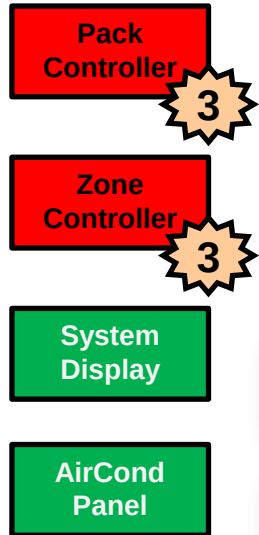
Kritikus és nem-
kritikus feladat
nem keverhető

Kritikus feladatok
példányai nem
keverhetők

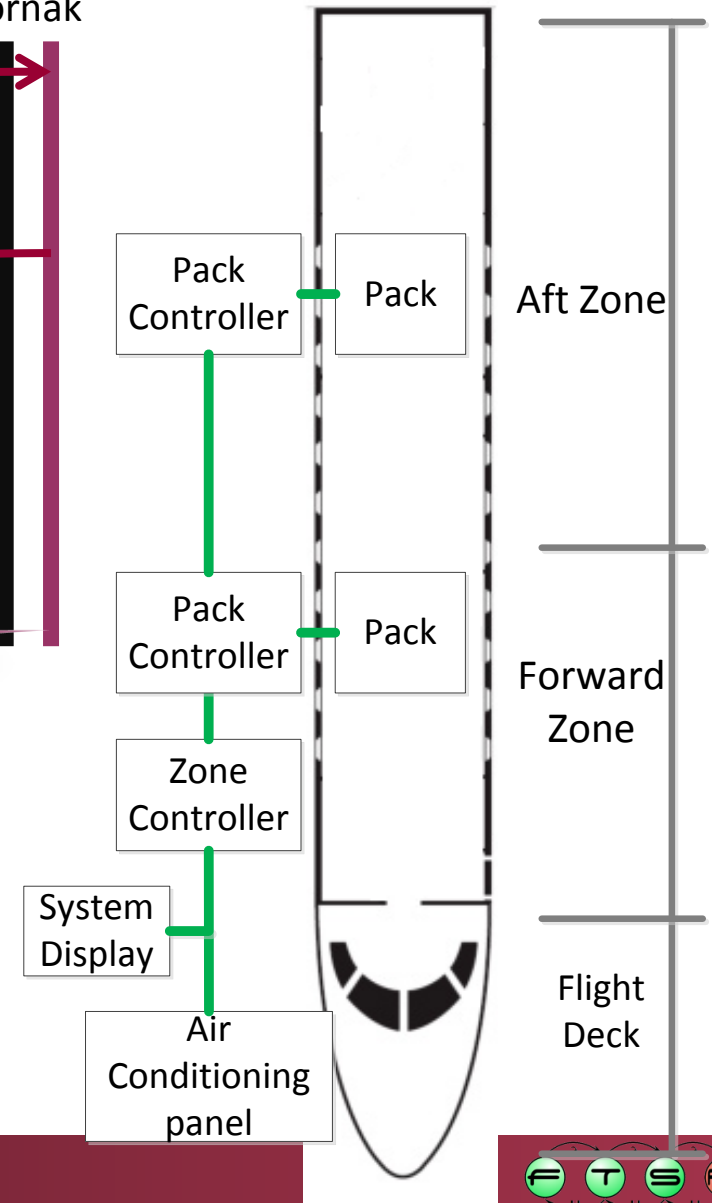
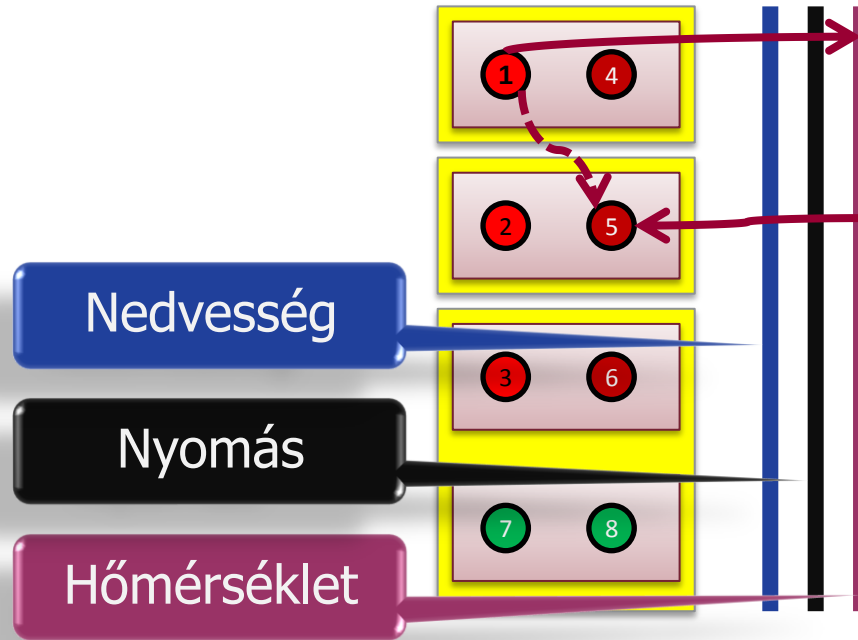


Kommunikációs csatornák allokációja

SW funkcionalitás



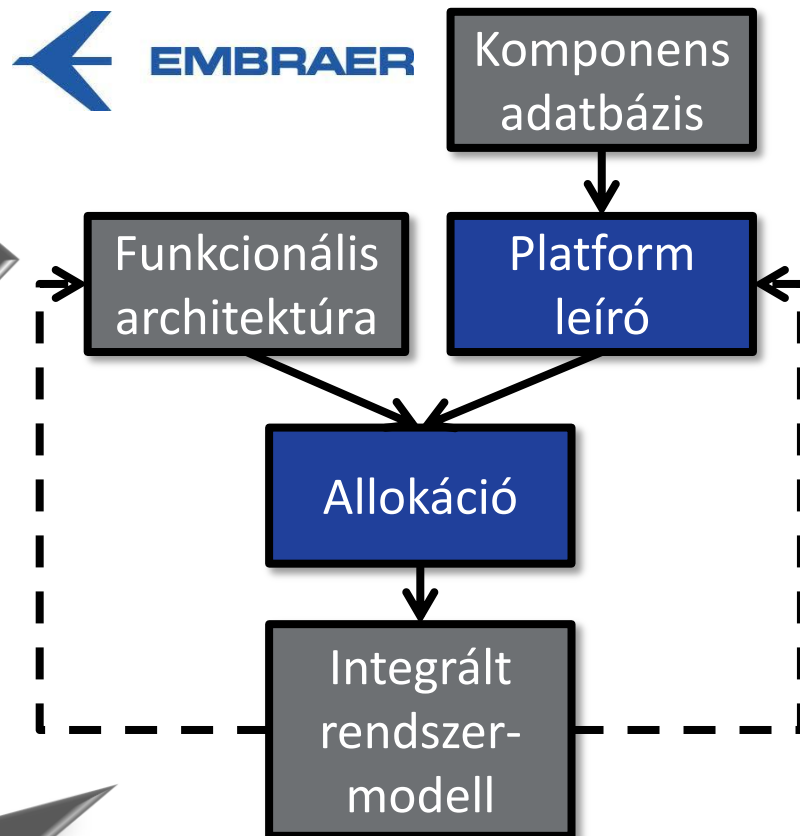
Kommunikációs csatornák



IMA konfigurációk modellvezérelt tervezése

Bemenetek:

- SW funkció architektúra modell (funkcionális + extrafunkc. követelm.)
- Platform leíró modell (ARINC 653 szakterületi modell)

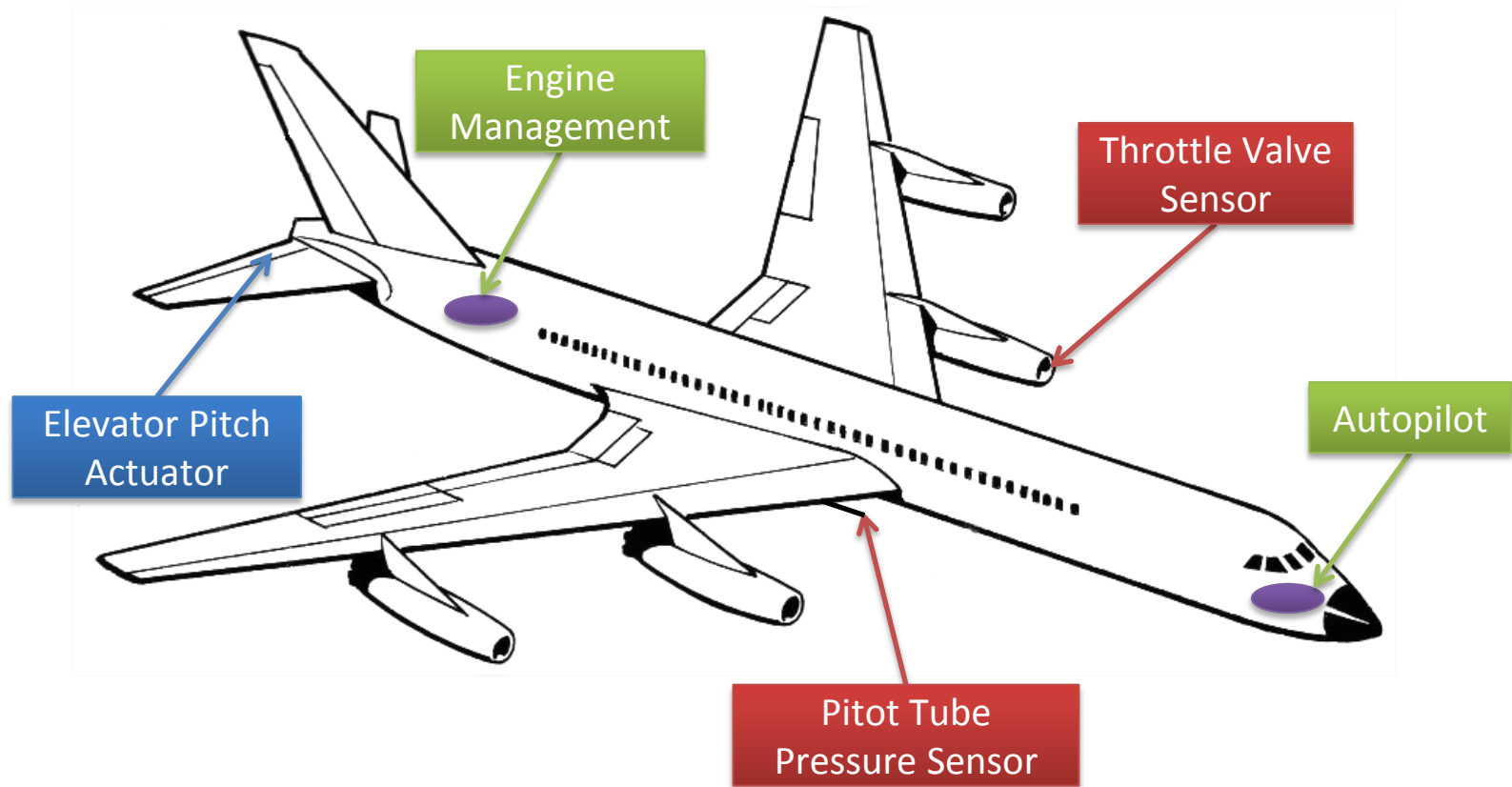


Kimenet:

- Integrált rendszermodell
- Szimulációra készen
- Teljes nyomonkövethetőség



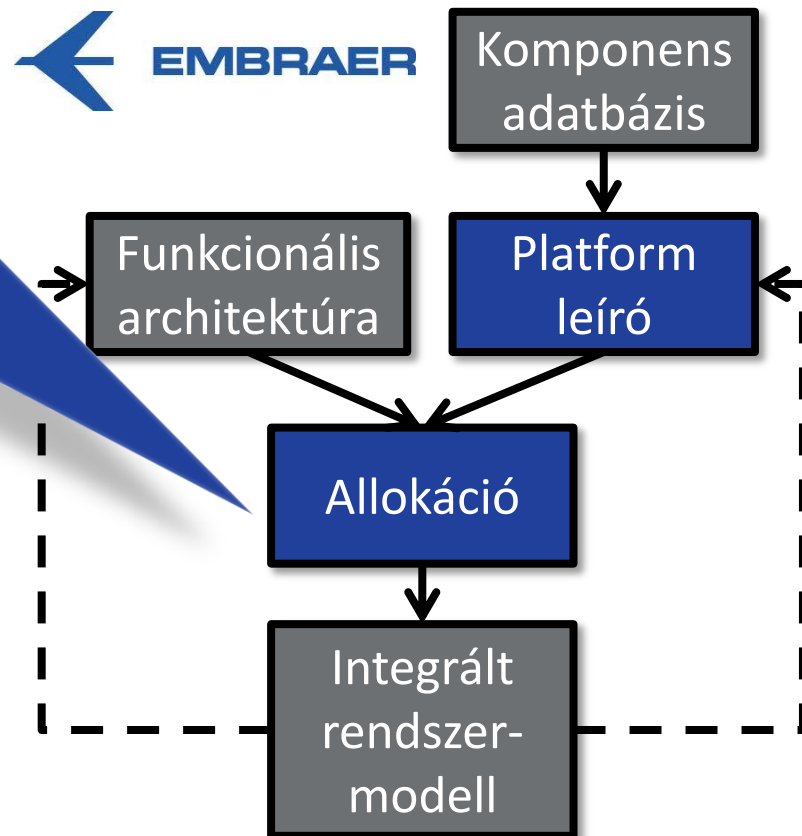
ÉIŐ DEMO



IMA konfigurációk modellvezérelt tervezése

Tervezőeszköz működési elve:

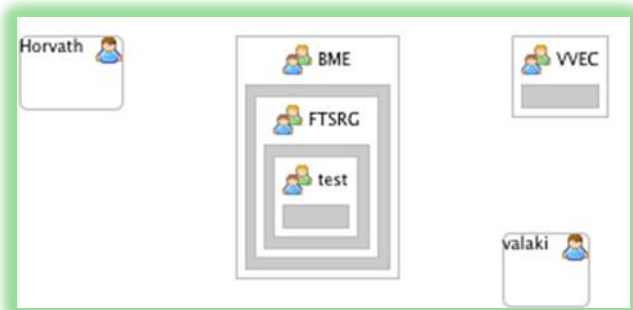
- Mérnökök által vezérelt manuális lépések
- Automatikus lépések
 - tervezési tér felderítés
 - optimalizáció
 - kódgenerálás
- Megkötések folyamatos ellenőrzése



Szakterület-specifikus modellező nyelvek

Szakterület-specifikus nyelvek felépítése

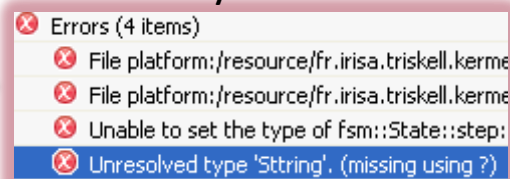
Grafikus szintakszis



Absztrakt szintakszis



Jólformáltsági
kényszerek

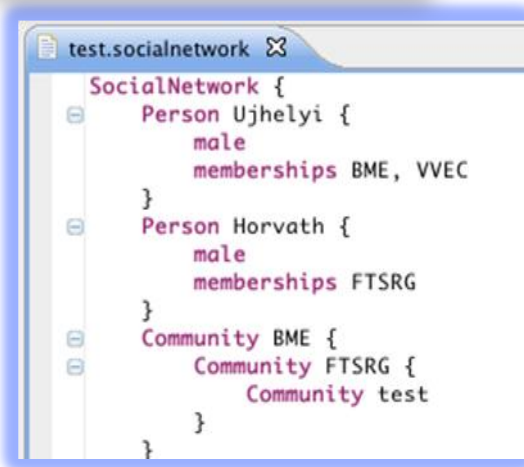


Viselkedési szemantika,
Szimuláció

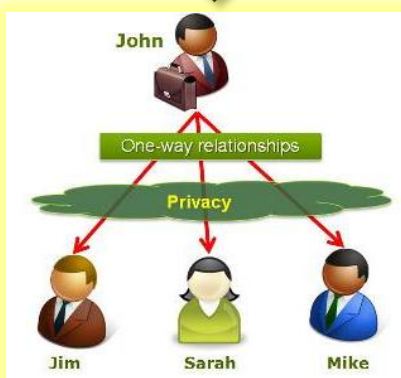
Kódgenerálás

Gráfmodellek!

Leképezés



Szöveges szintakszis



Nézet

```
</membership>
<profile defaultProvider="Sitefinity">
  <providers>
    <clear/>
    <add name="Sitefinity" connections
  </providers>
  <properties>
    <add name="FirstName"/>
    <add name="LastName"/>
    <!-- SNP specific properties -->
    <add name="NickName" />
    <add name="Gender" />
  </properties>
</profile>
```

Kód

(Dokumentáció,
Konfigurációs fájl)

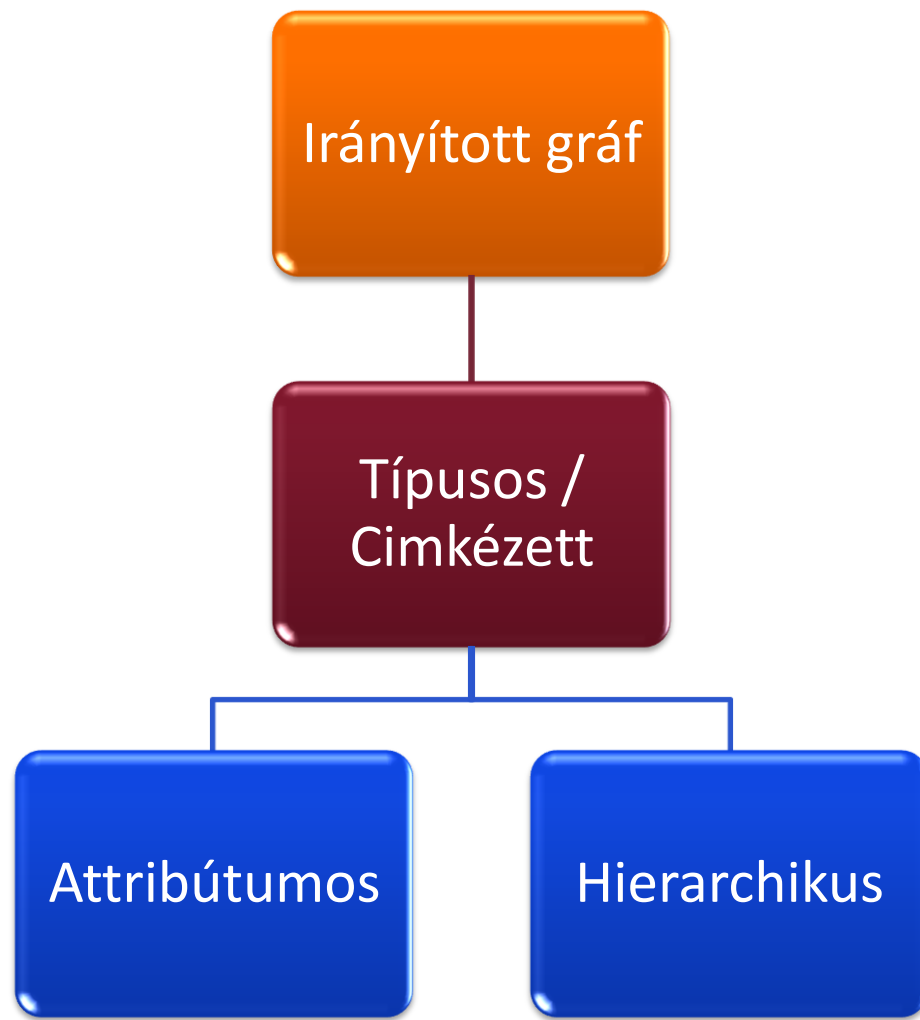
Szakterület-specifikus nyelvek aspektusai



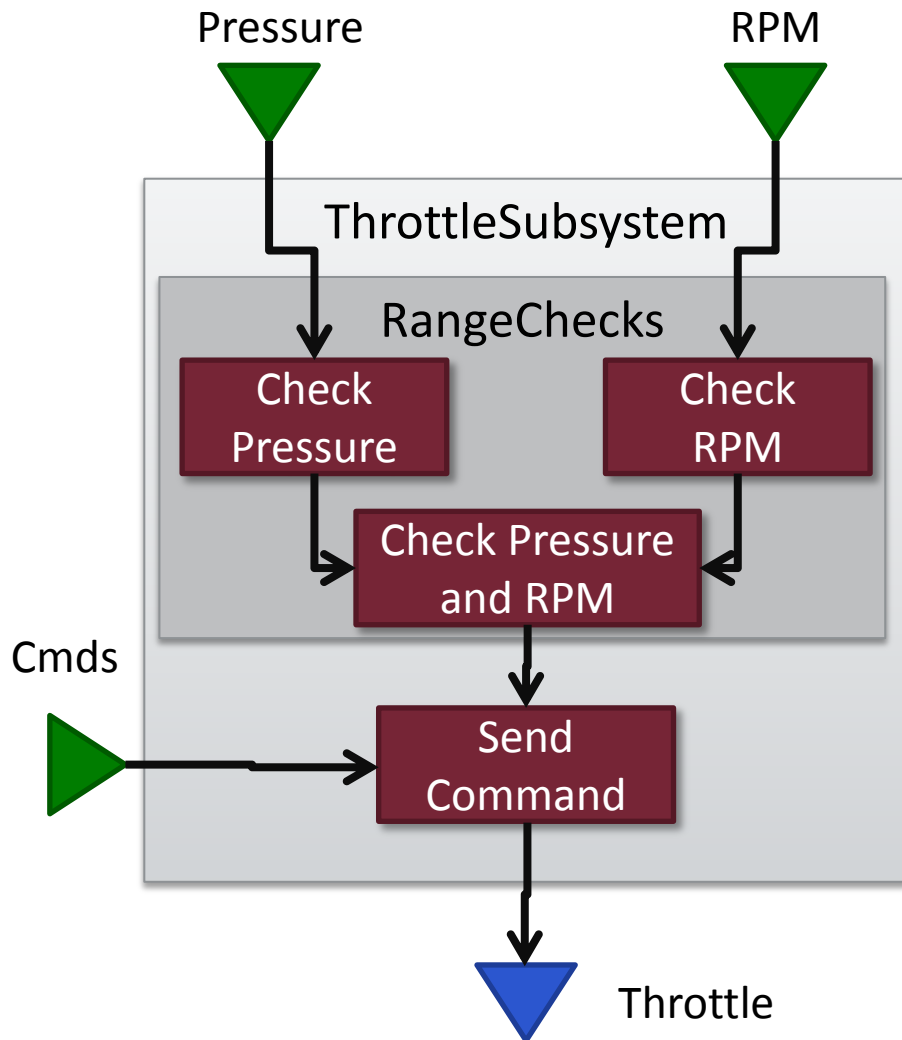
Gráfmodellek

Szabványos gráfmodellek az informatikában

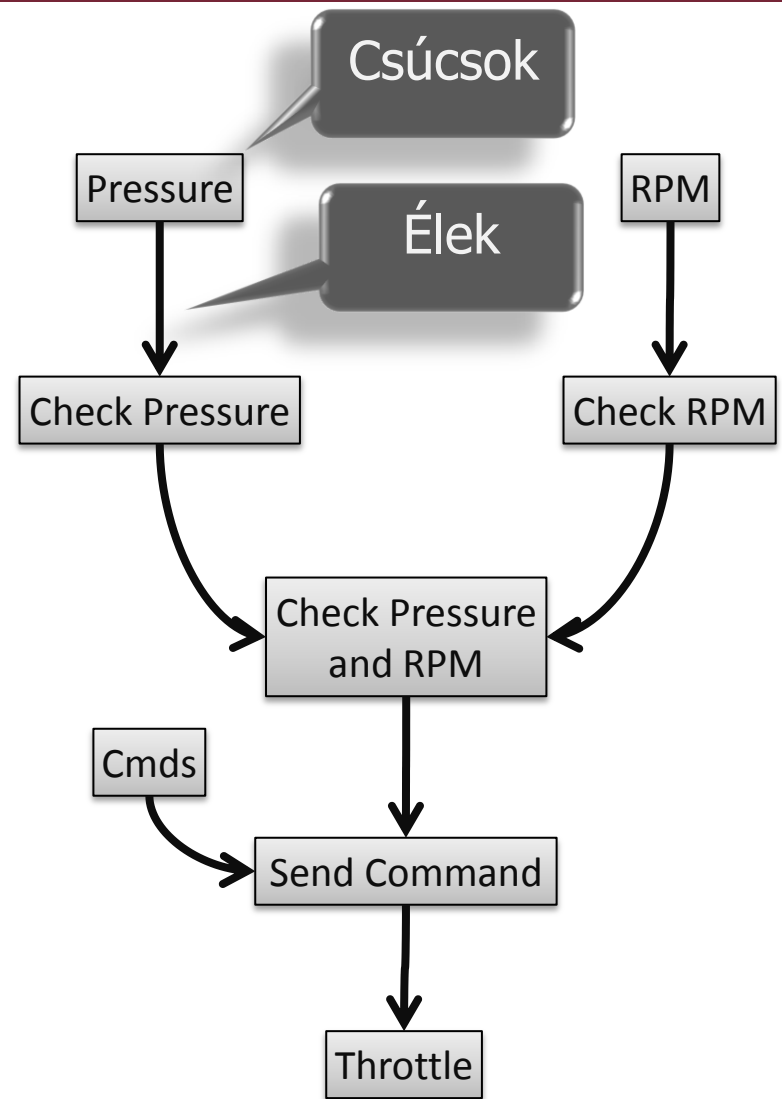
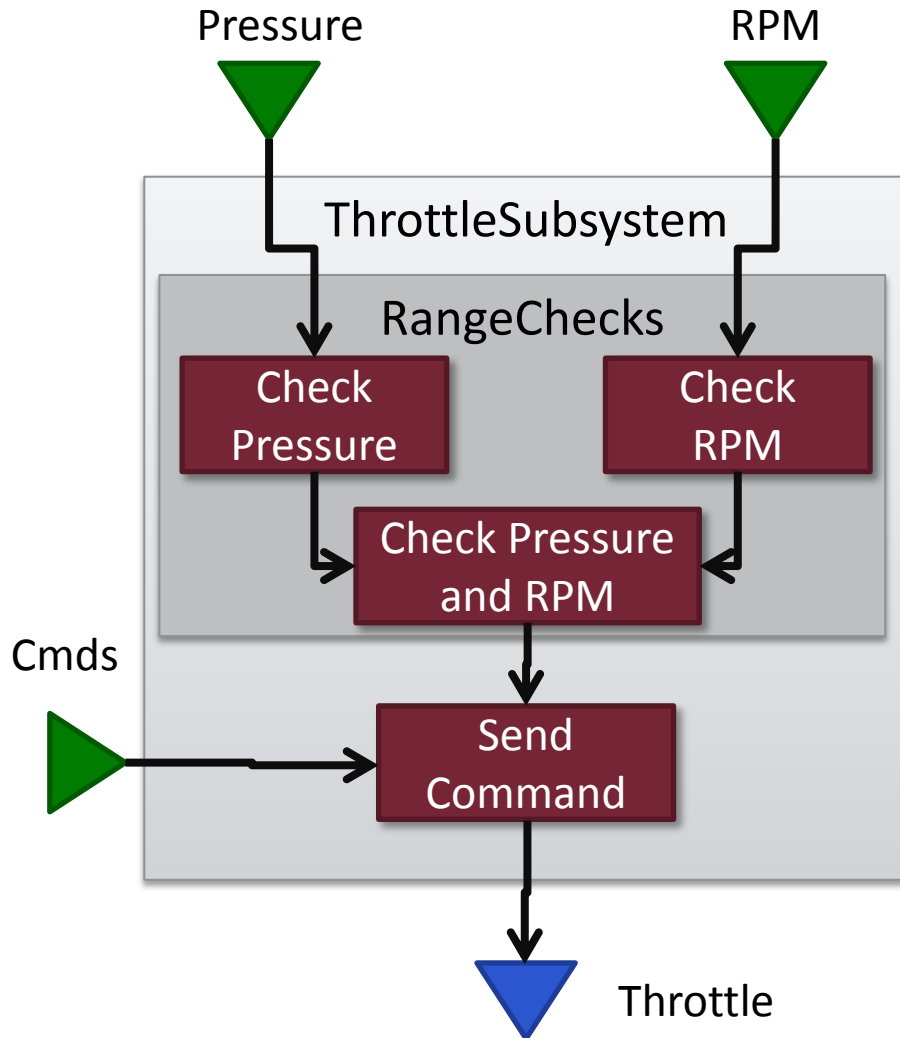
- **OMG: Meta Object Facility (MOF)**
 - Cél: Szakterület-specifikus modellezési nyelvek egységes megadása
 - Eclipse alapú fejlesztőeszközök szabványa
- **W3C: Resource Description Framework (RDF)**
 - Cél: Tudásreprezentáció a szemantikus weben
 - Gráfadatbázisok, Triple Store-ok (> 1 billió hármás)
- **IEEE: Conceptual Graphs (Common Logic)**
 - Cél: egységesített adatsereformátum logikai következtetőkhöz



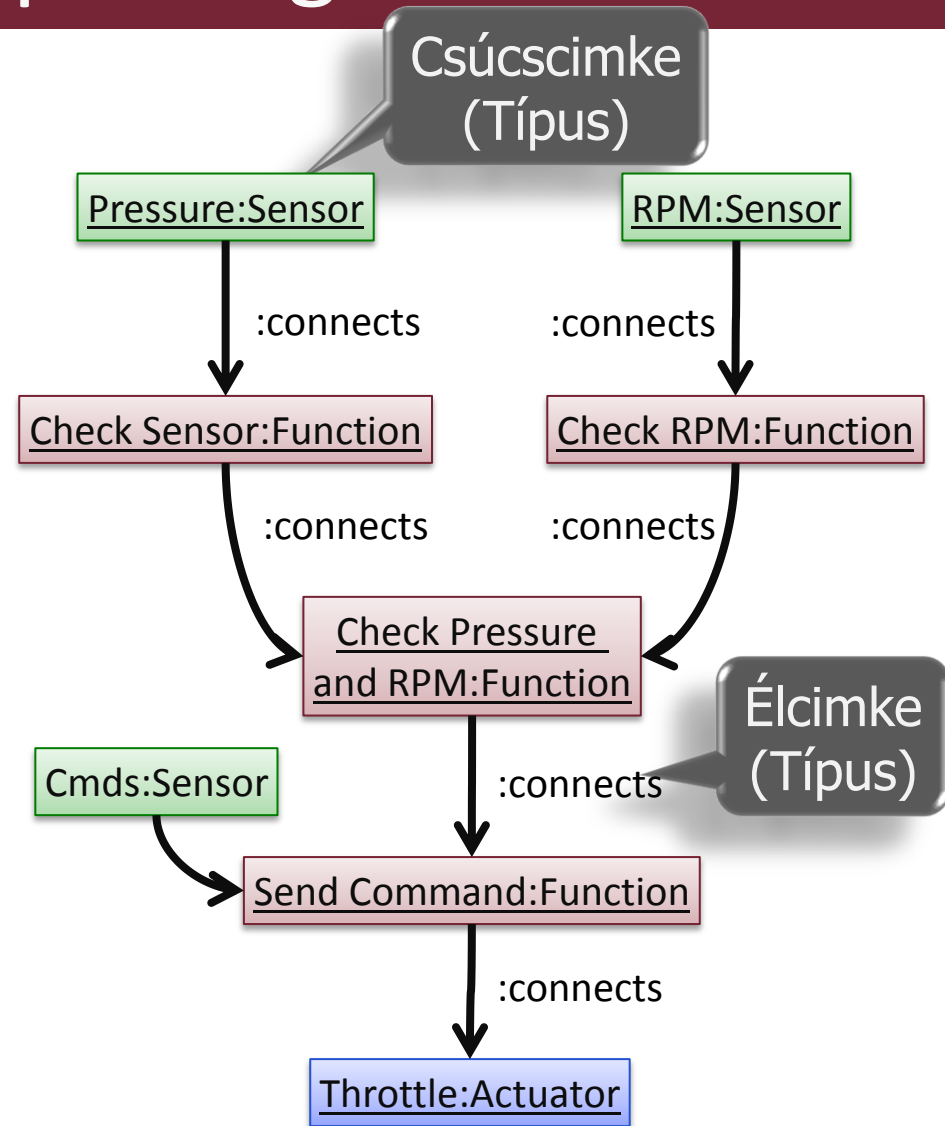
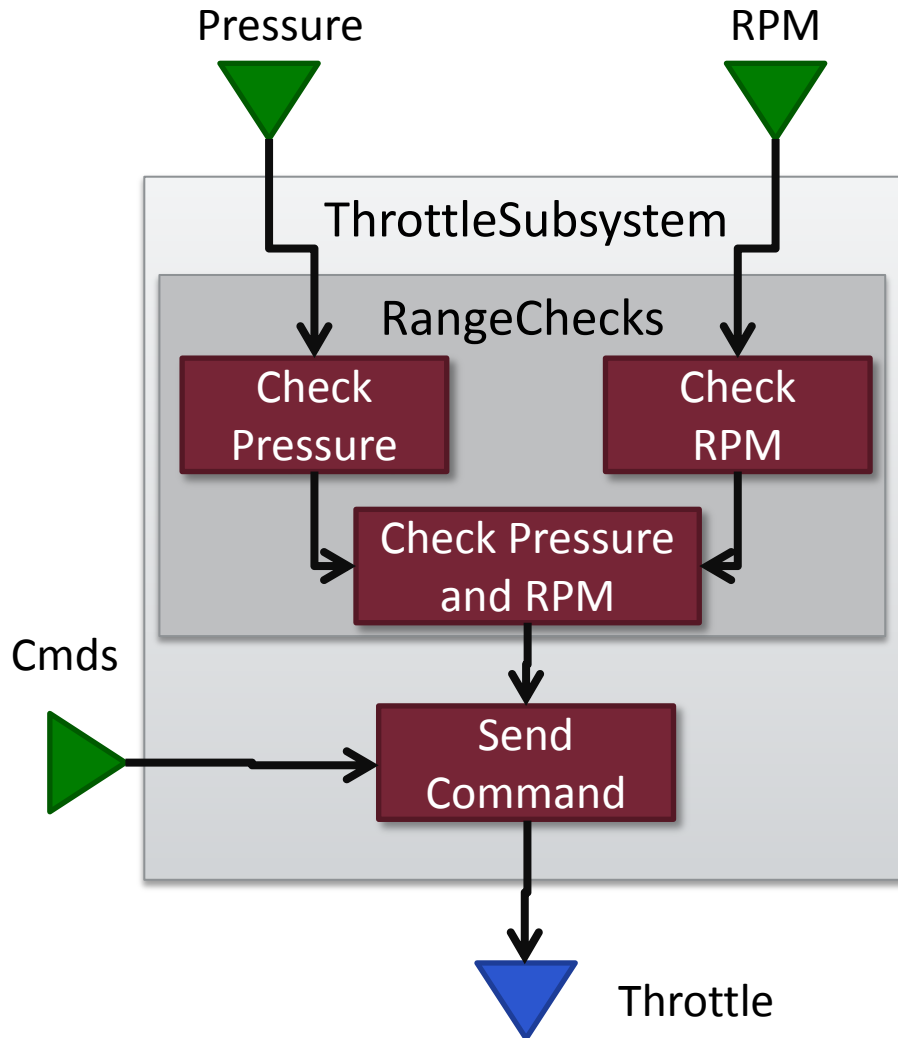
Gráfmodellek



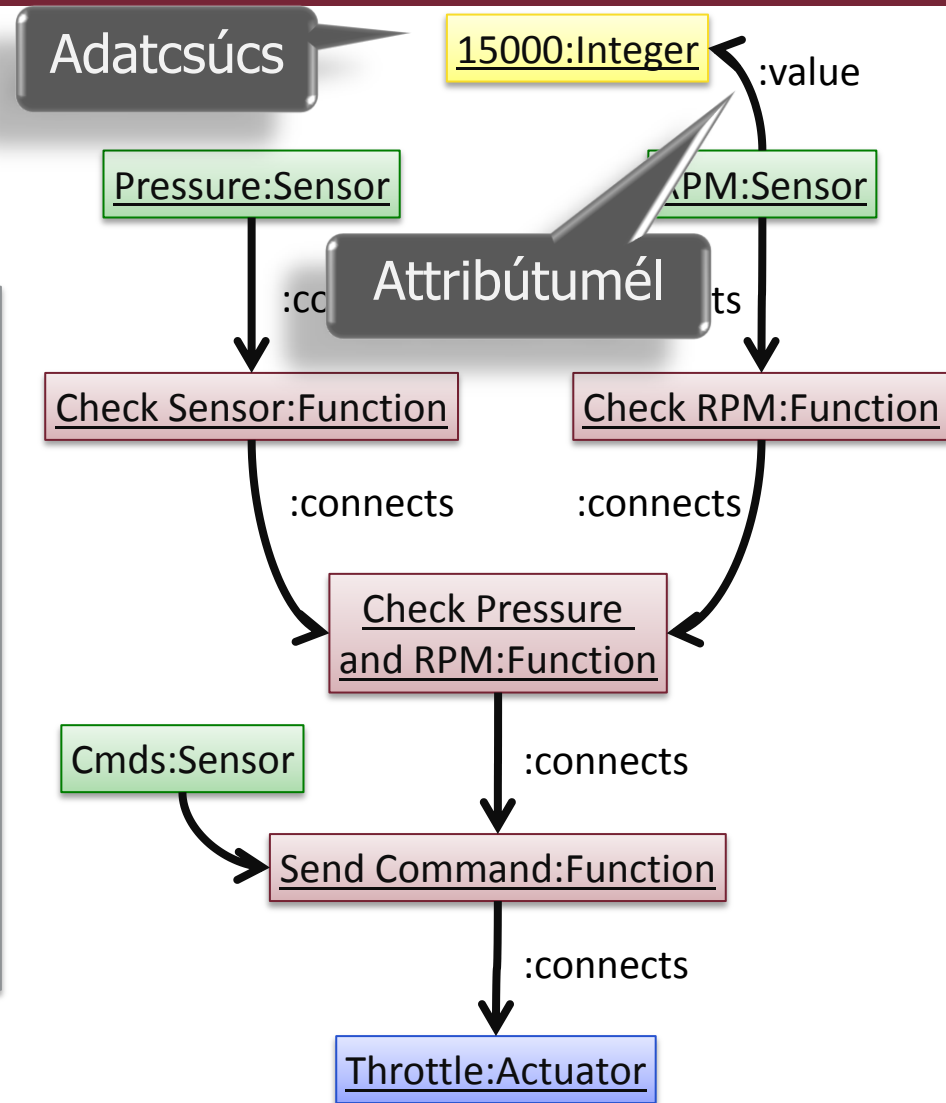
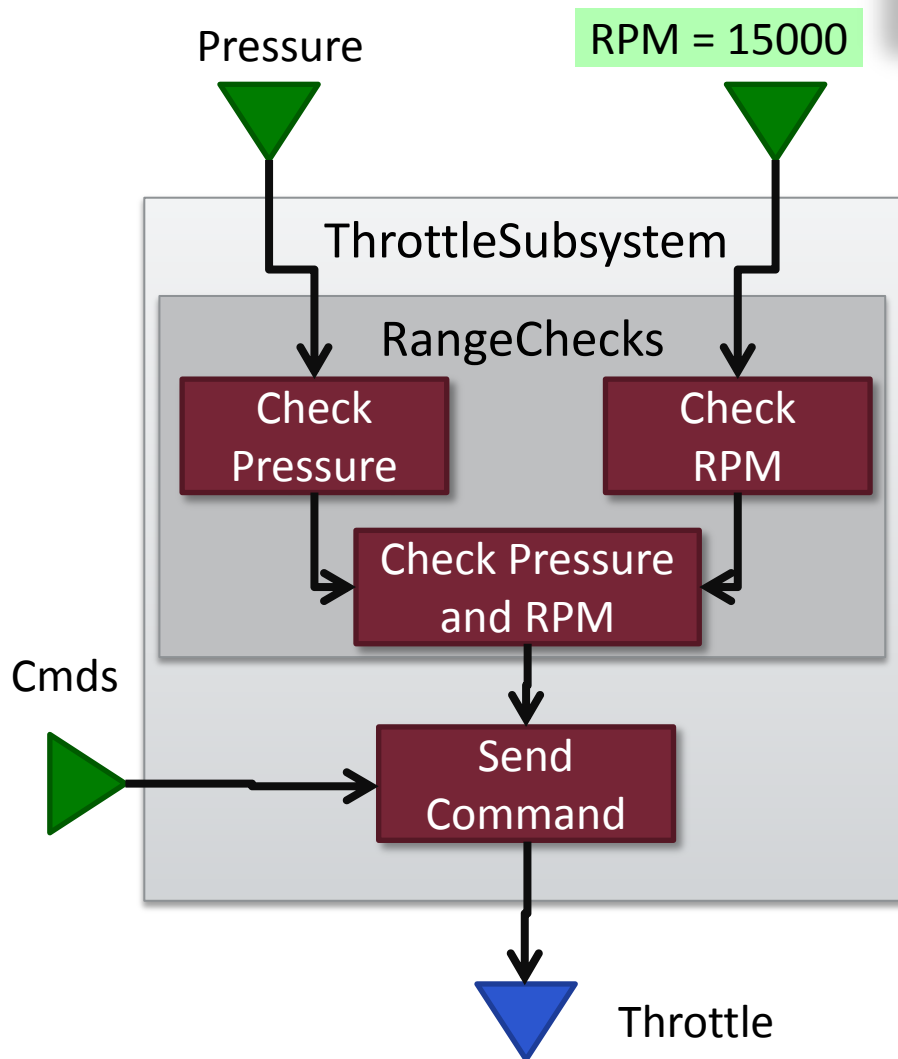
Gráfmodellek: Irányított gráf



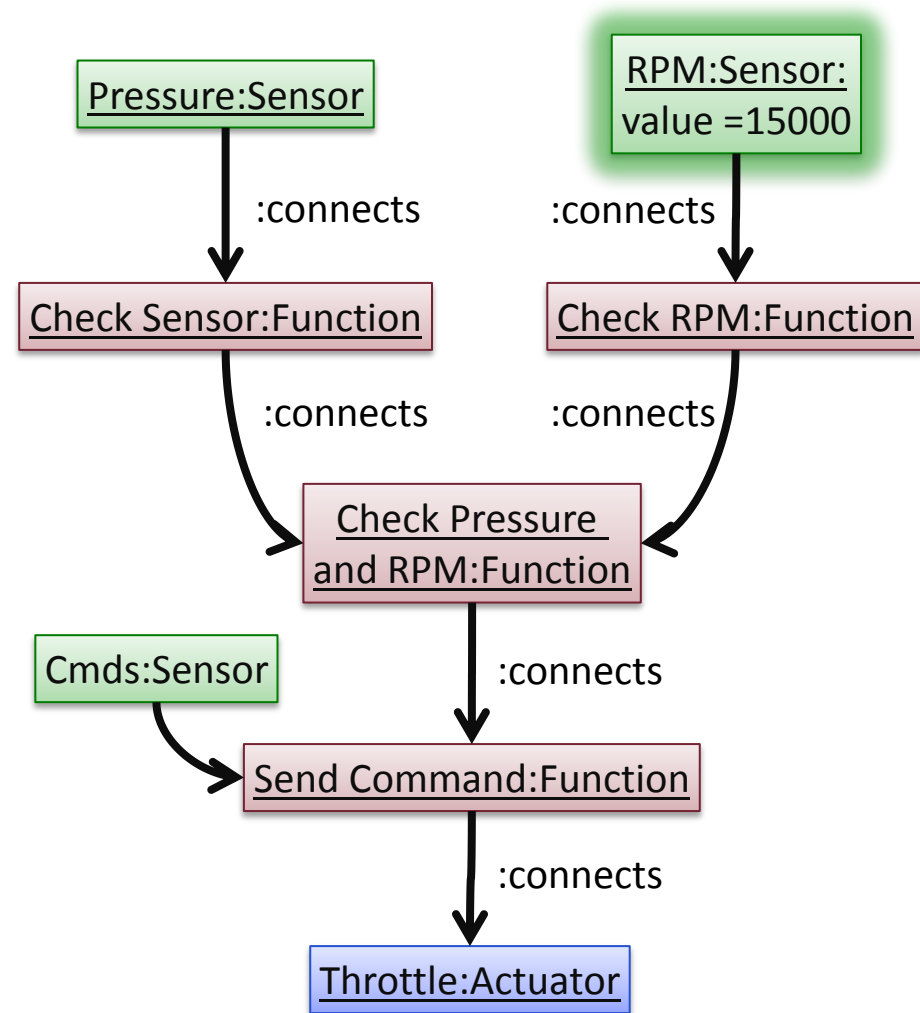
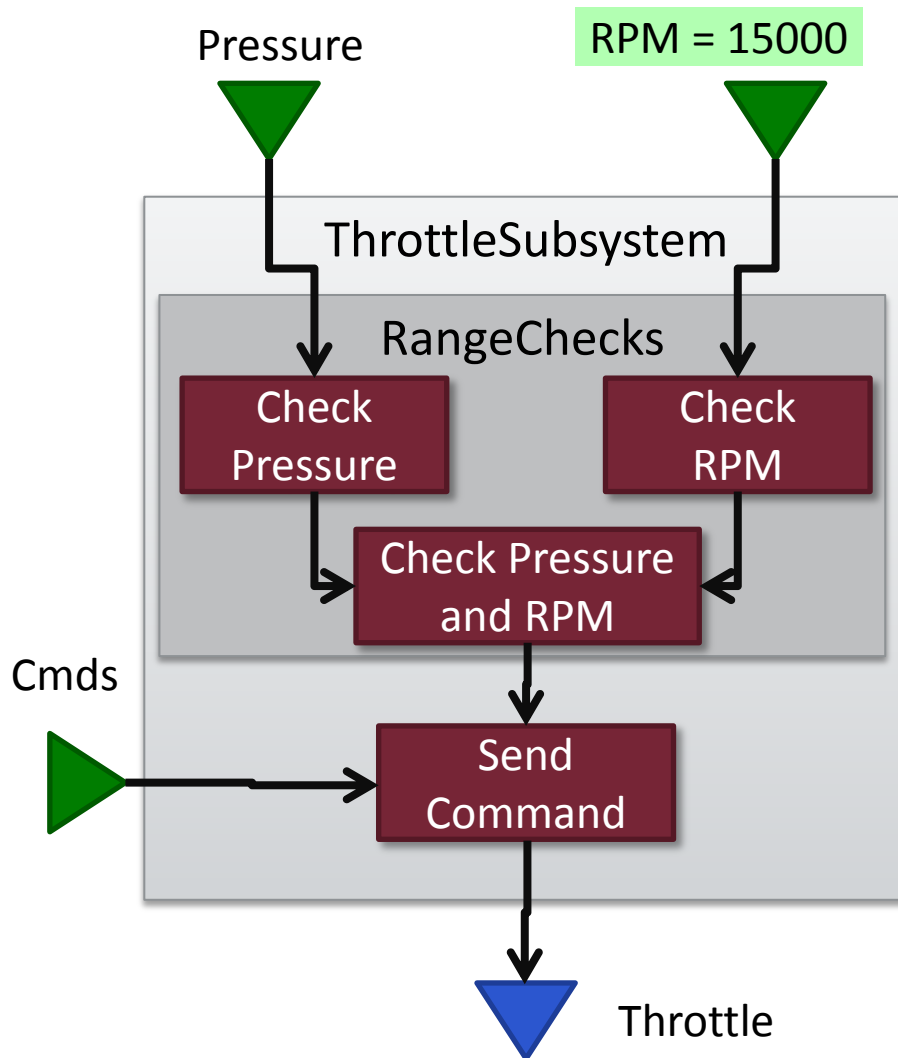
Cimkézett / Típusos gráfok



Attribútumos gráfok



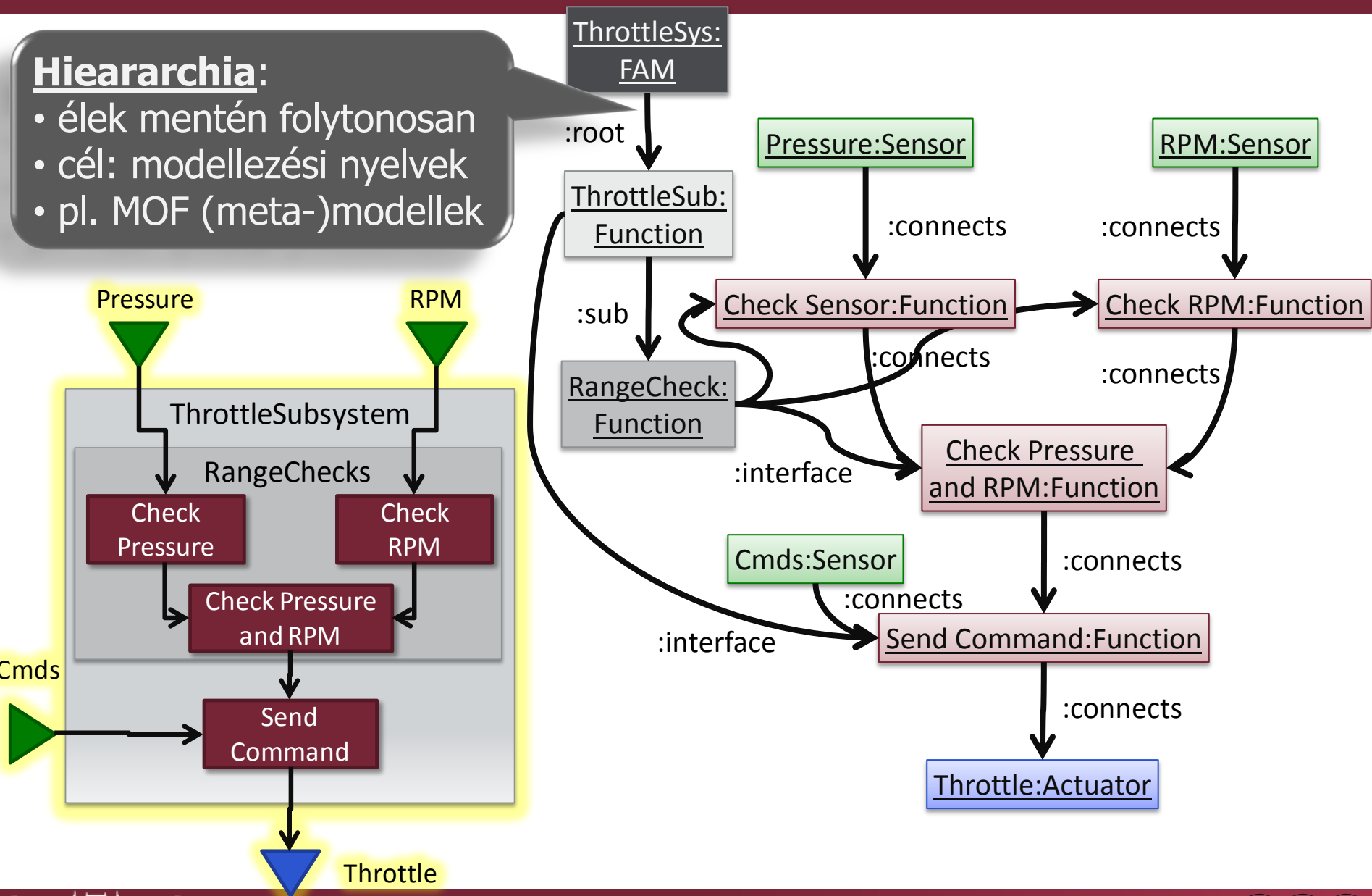
Attribútumos gráfok: UML/MOF jelölés



Hierarchikus gráfok I.

Hieararchia:

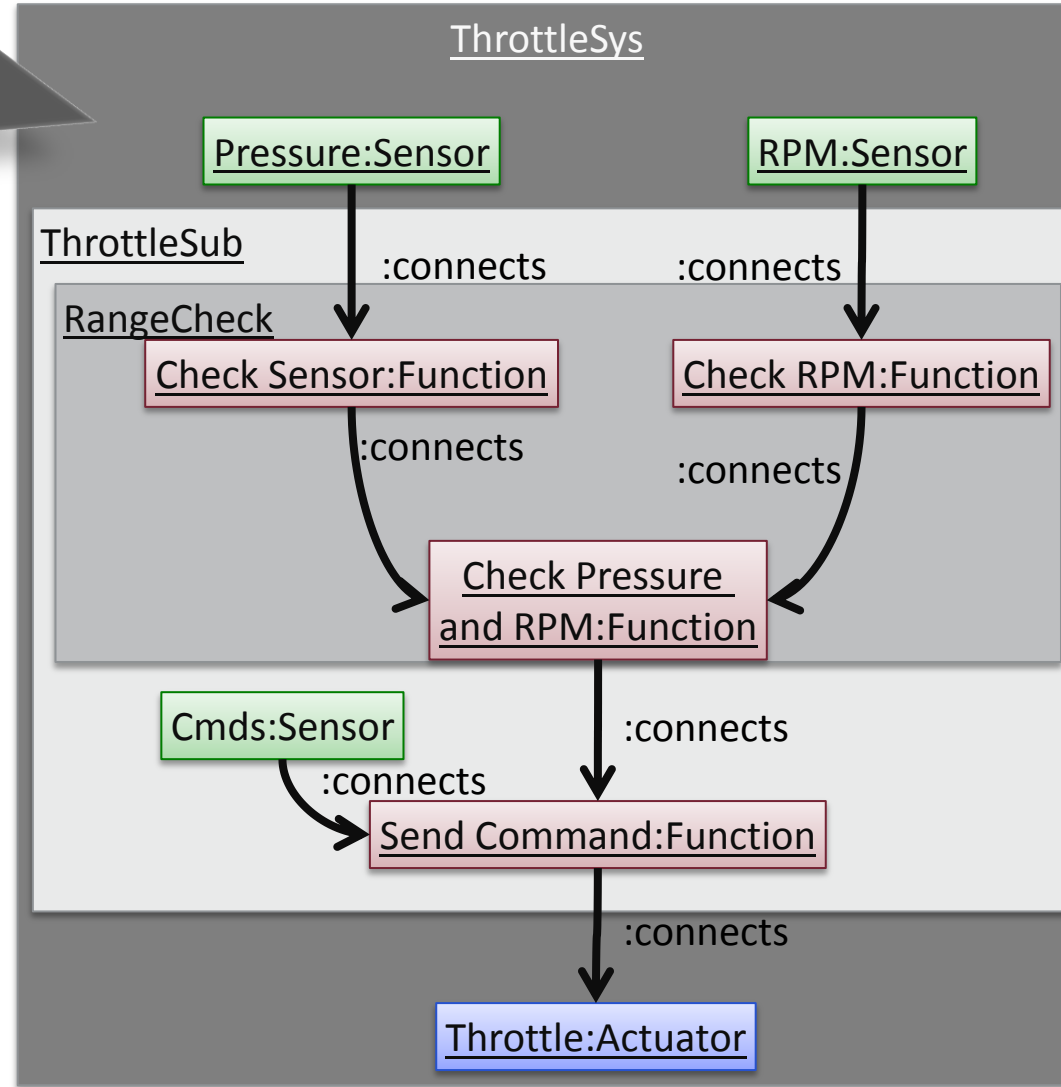
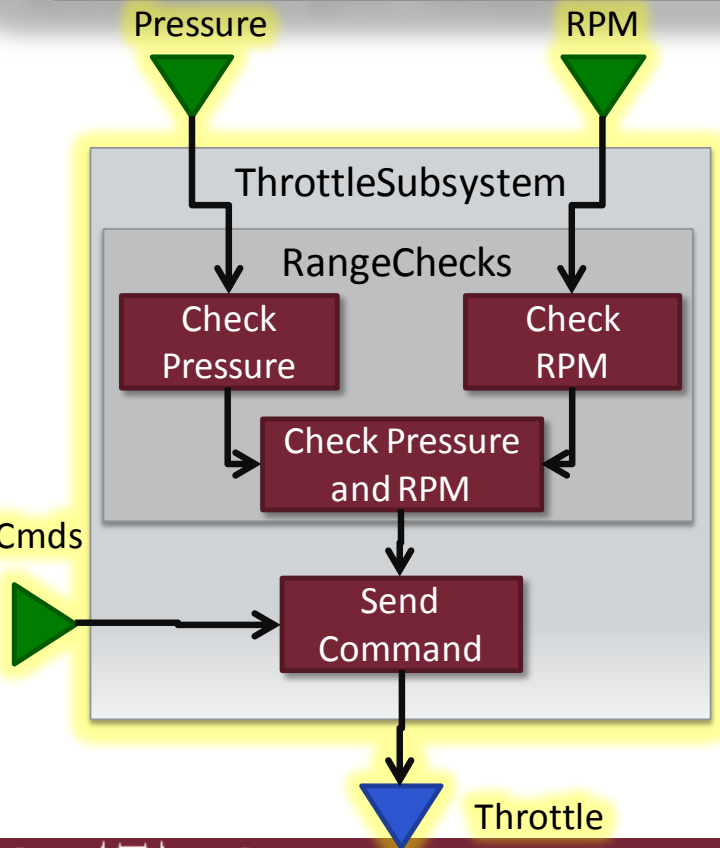
- élek mentén folytonosan
- cél: modellezési nyelvek
- pl. MOF (meta-)modellek



Hierarchikus gráfok II.

Hierarchy:

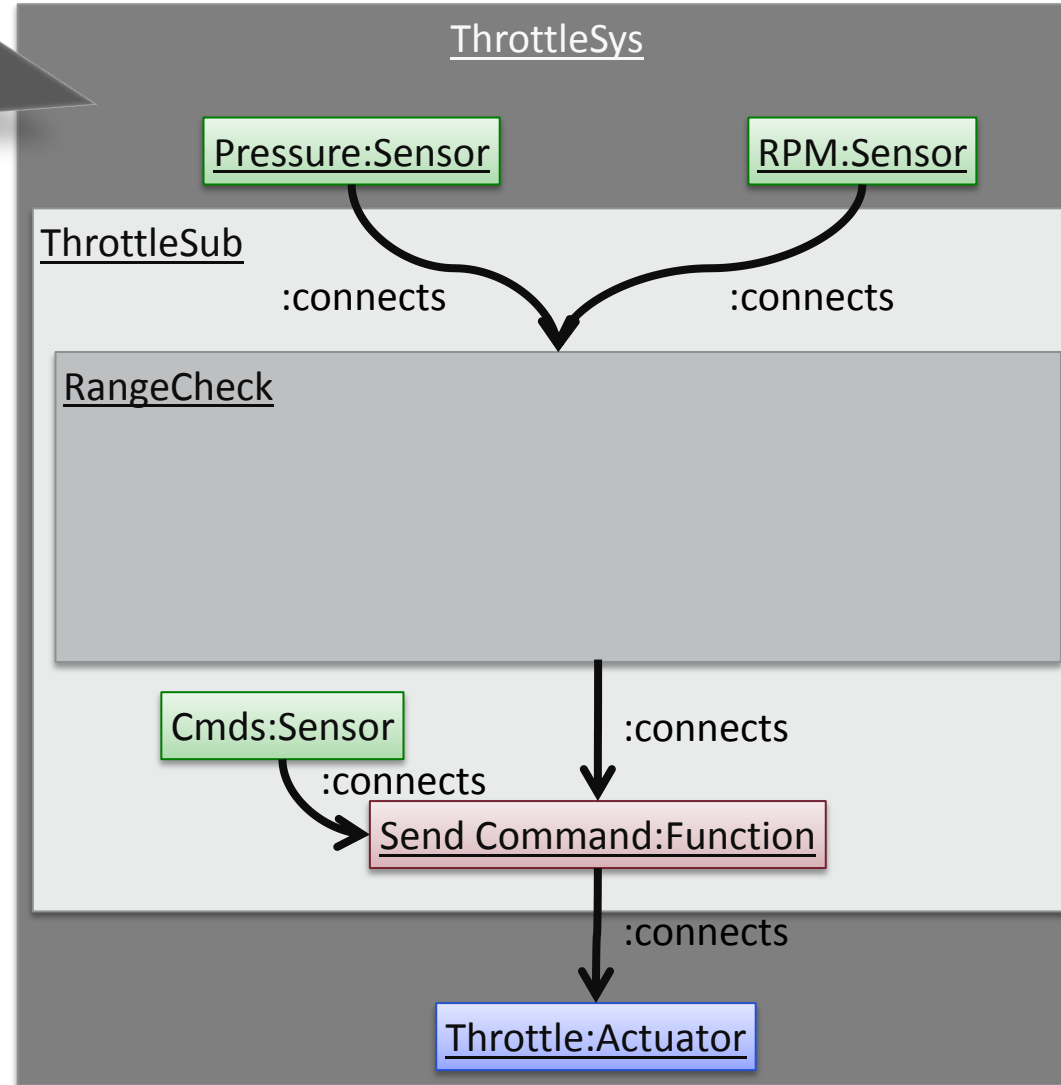
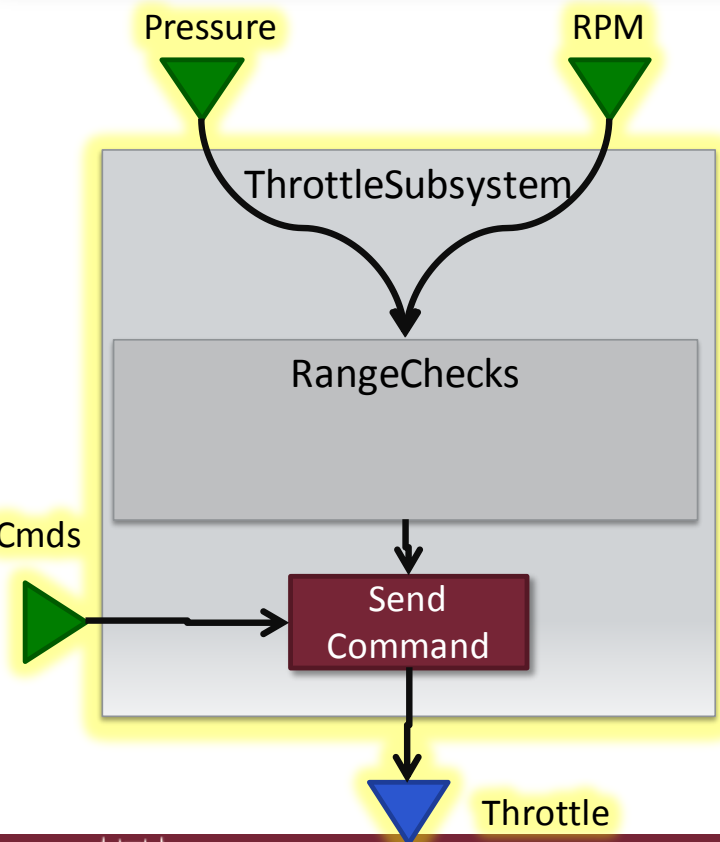
- csúcsok mentén
- cél: tárolás, szerializáció
- egyszintű: QuadStore, GraphDB
- többszintű: EMF modellek



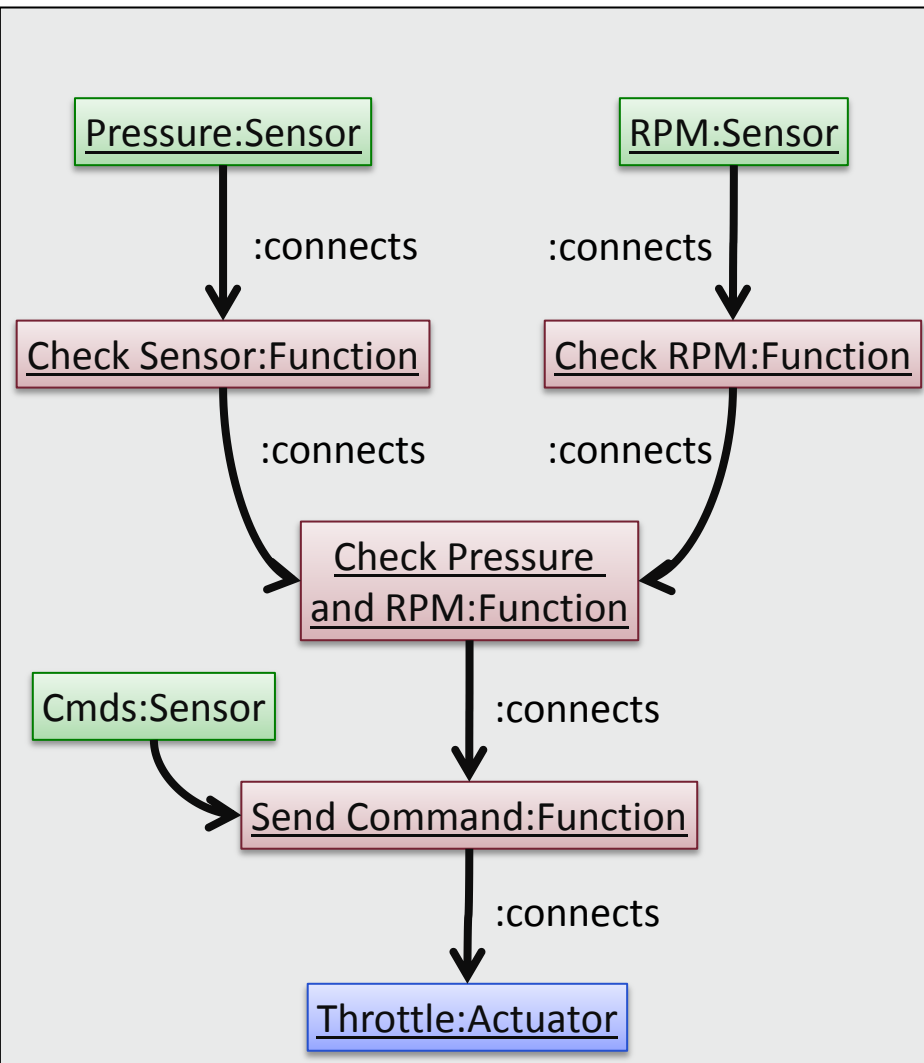
Hierarchikus gráfok III: Információrejtés

Hieararchia:

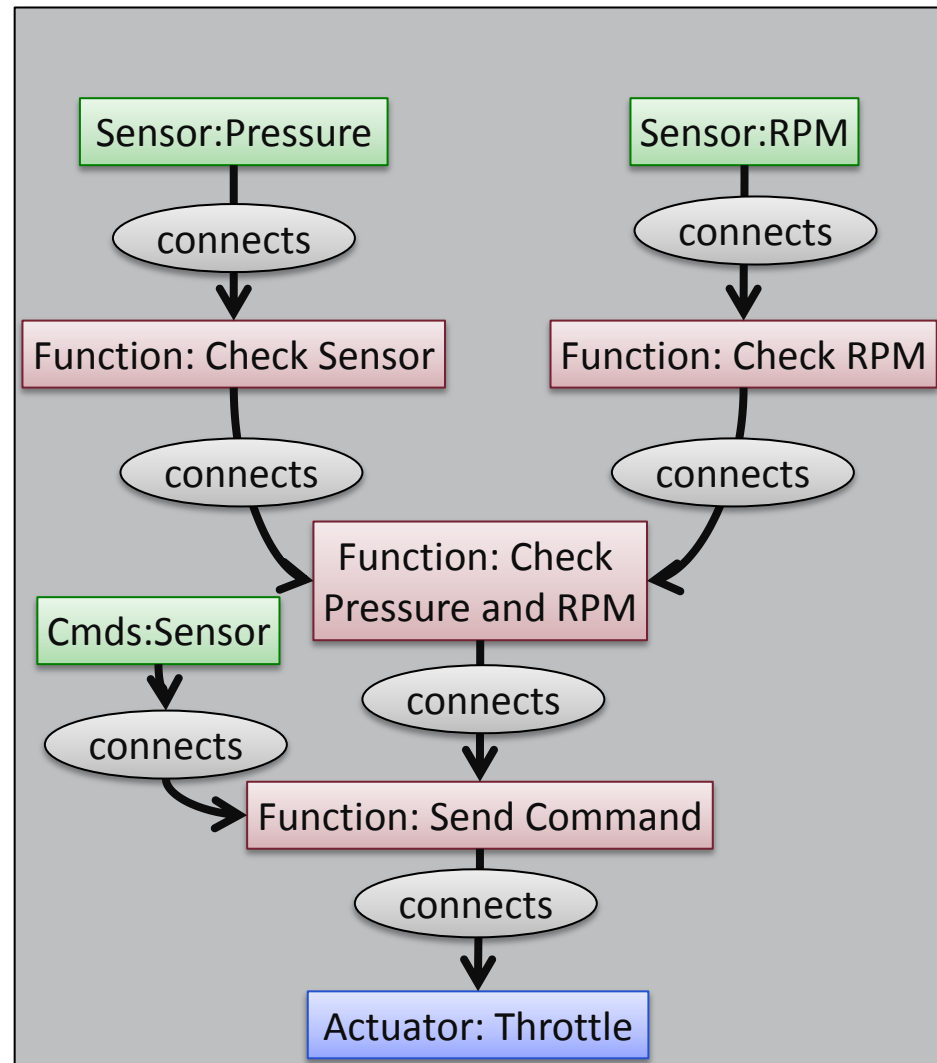
- csúcsok mentén (ki/be)
- élek átírányítása
- pl. gráfrajzoló könyvtárak



Jelölésrendszerek: MOF vs. Conceptual Graphs



MOF: Meta Object Facility
(OMG szabvány)

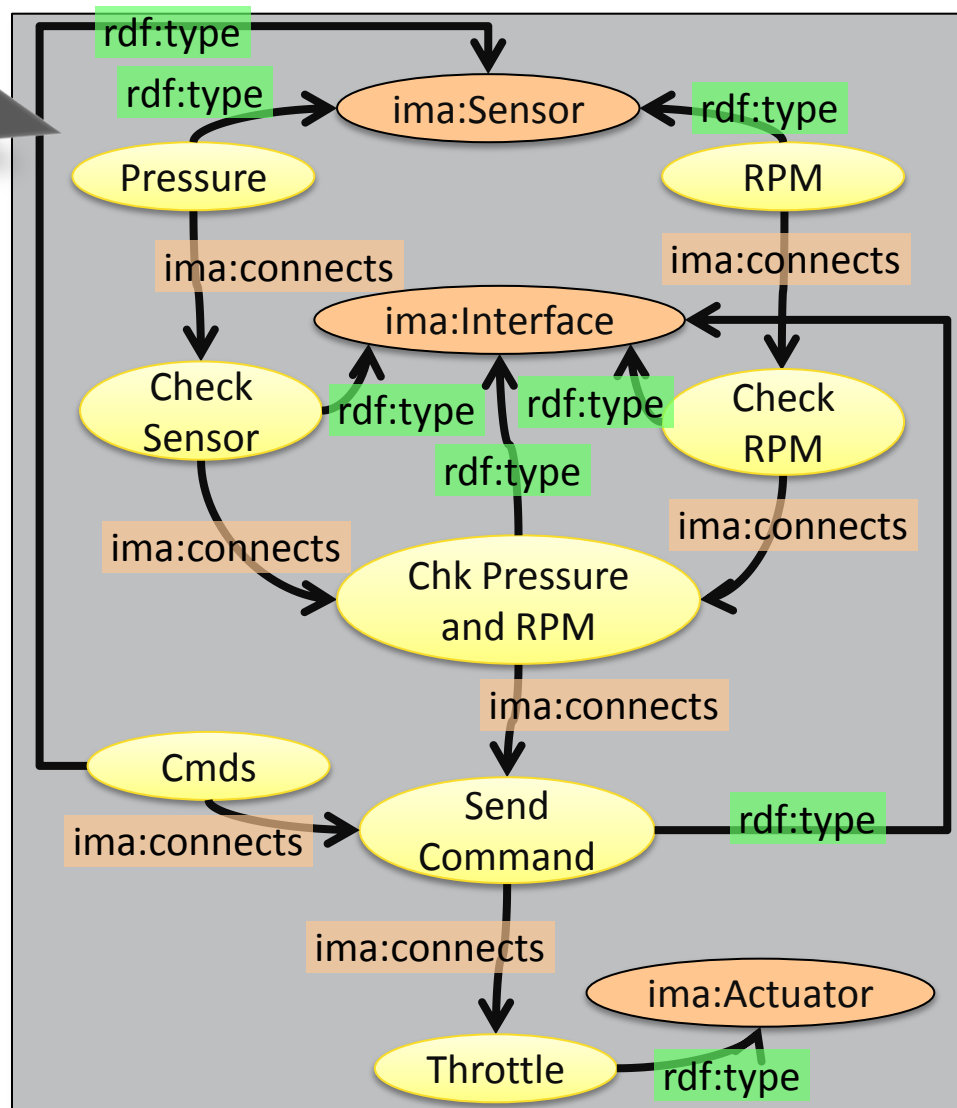
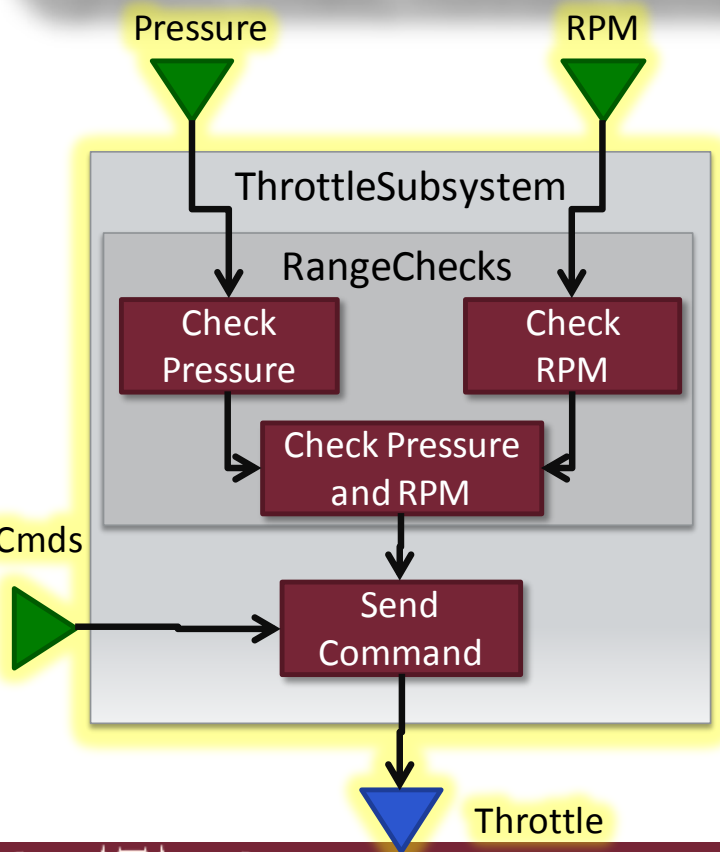


Conceptual Graph
(IEEE szabvány)

Jelölésrendszerek: RDF

TripleStore (RDF adatbázis)

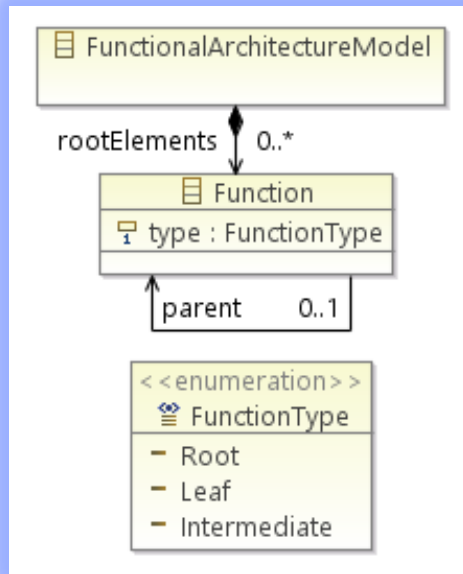
- éleket és értékeket tárol
- hármass: (címke, honnan, hová)
- QuadStore: négyes (gráfID, címke, honnan, hová)



RDF: Resource Description Framework (W3C)

Metamodellek

Metamodellek és példánymodellek

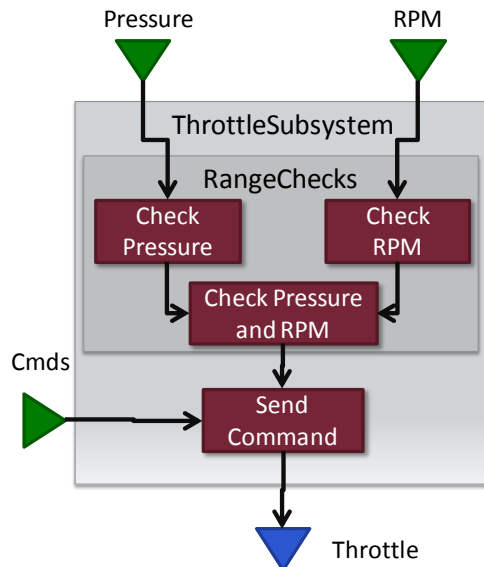


Metamodell (MOF, EMF):

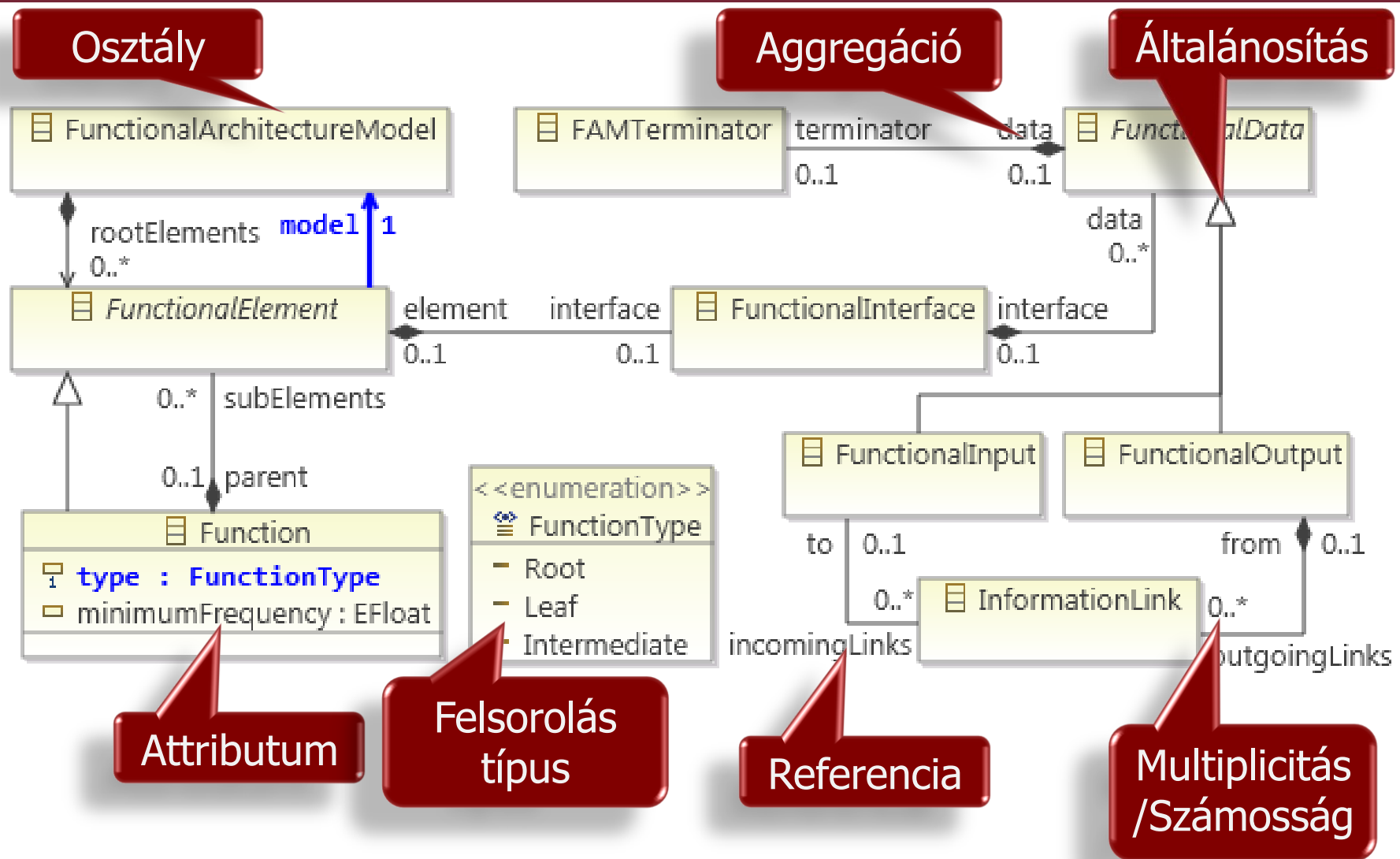
- modellezési nyelv precíz specifikációja
- cél: fejlesztőrendszerek (IDE) támogatása
 - Metamodell → interfészek, implementáció, szerkesztők
 - automatikus kódgenerálás:

Példánymodell:

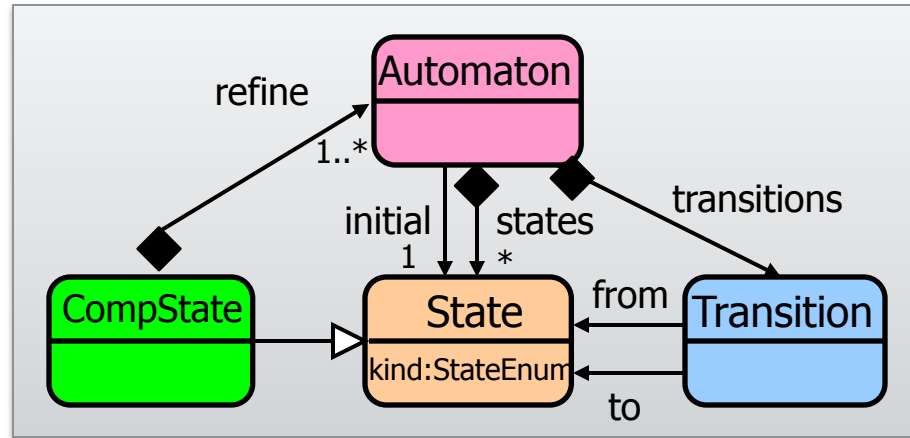
- A nyelv egy „mondata”
- A metamodell egy típushelyes példánya



Metamodellek elemkészlete



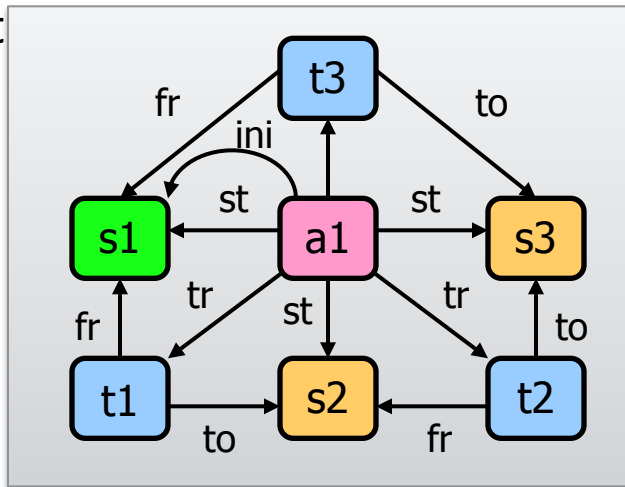
Metamodell és példánymodell: Állapotgépek



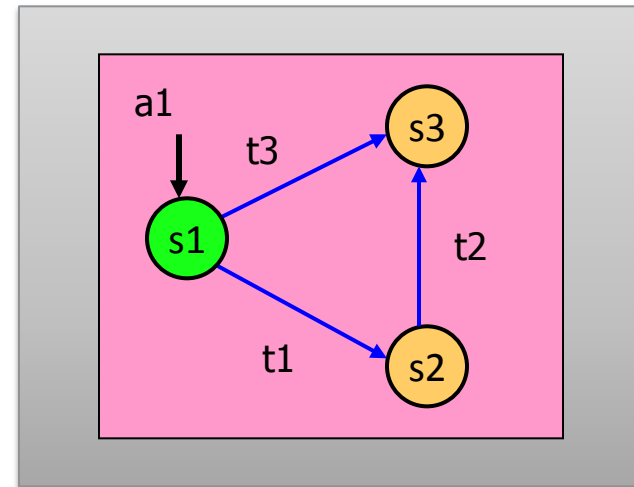
Metamodell

Metamodell szint

Modell szint

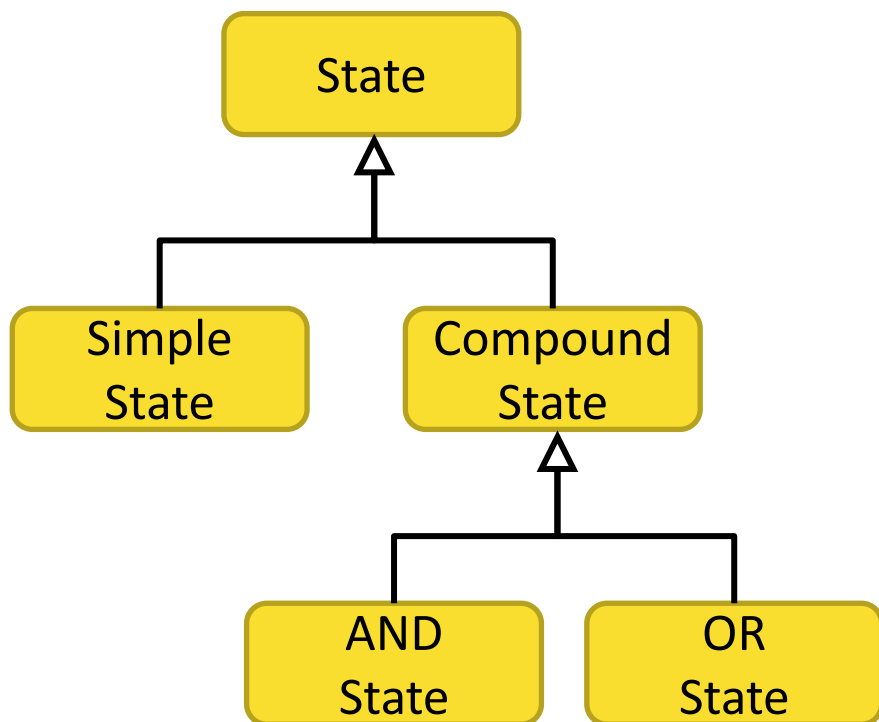


Absztrakt szintakszis



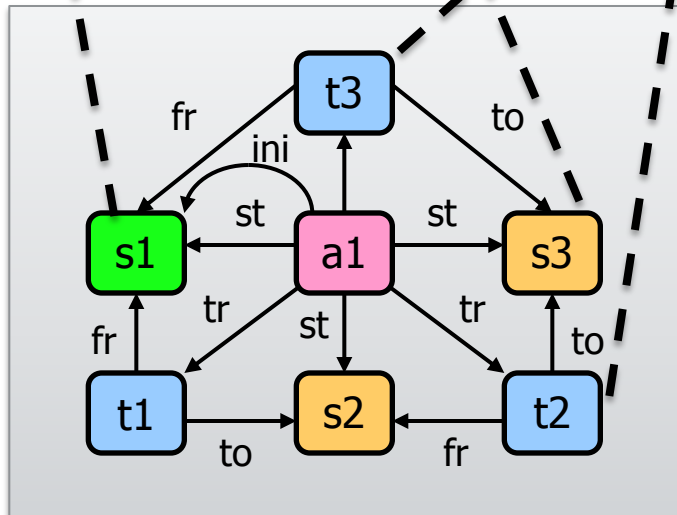
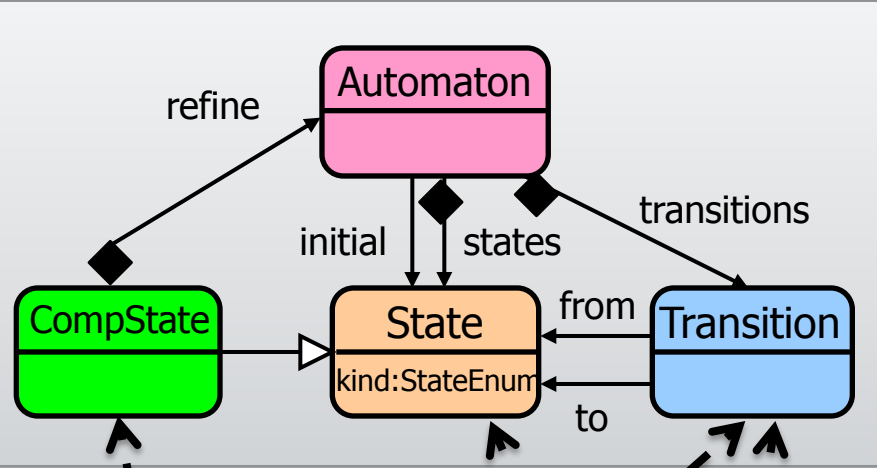
Konkrét szintakszis

Típushierarchia



- Általánosítás
 - $\cong$ Öröklés
 - Tranzitív
 - Reflexív? / Irreflexív?
- Hogyan olvassuk?
 - ***SimpleState*** alosztálya a ***State***-nek
 - ***State*** őszosztály a ***SimpleState***-nek
- Helyettesíthetőség
 - ✓ Alosztály az Őszosztály helyett
 - ✗ ~~Őszosztály az Alosztály helyett~~

Típushelyesség / Példányosítás



- Minden modelcsúcs **példánya** a metamodell egy csúcsának

- **Direkt típus:**

- Nincs nála alacsonyabb típus a típushierarchiában
- $s1 \rightarrow \text{CompState}$

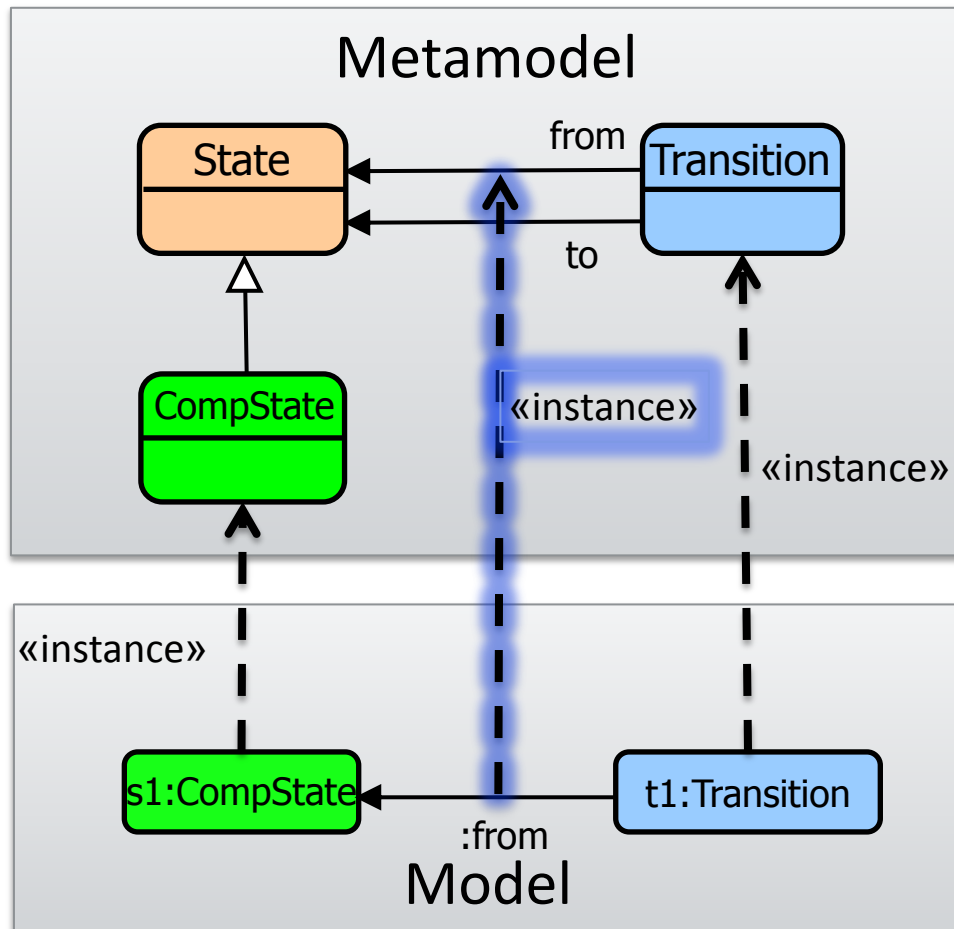
- **Indirekt típus:**

- A direkt típus őosztálya
- $s1 \rightarrow \text{State}$

Élek típushelyessége

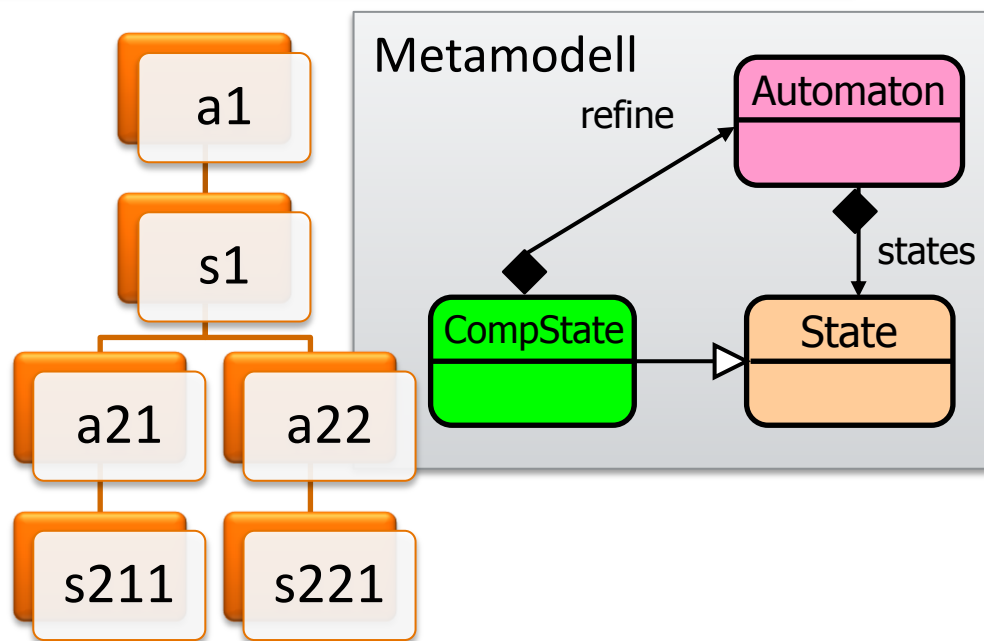
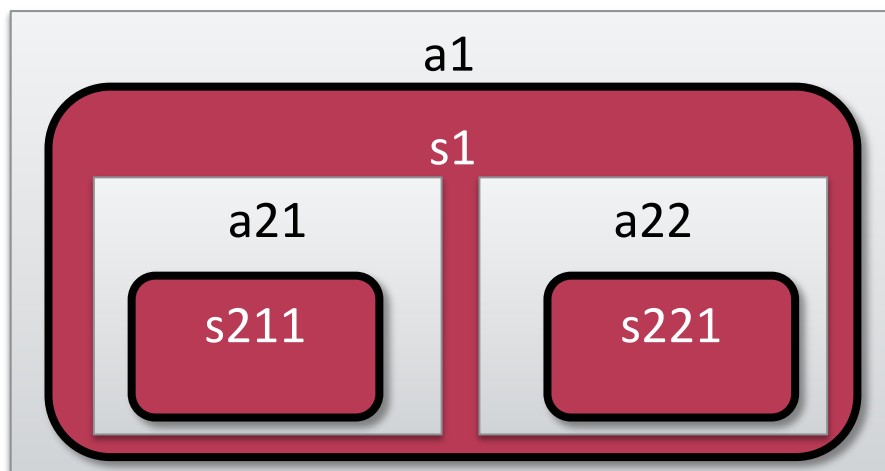
■ A modell éle **típushelyes** ha

- ***type(src(link))*** alosztálya ***src(type(link))***-nek
- ***type(trg(link))*** alosztálya ***trg(type(link))***-nek
- Informálisan:
 - Az él forráscsúcsának típusa alosztálya az él típusának forrásosztályának
 - Az él célcsúcsának típusa alosztálya az él típusának célosztályának



Can you define generalization
for references?

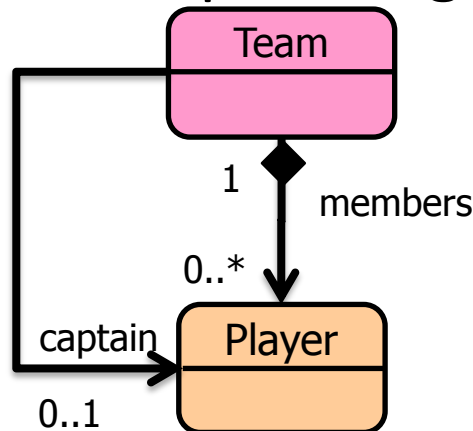
Tartalmazási hierarchia



- Minden modellelemnek szülője egyértelmű
 - N gyerek $\rightarrow$ 1 szülő
 - Egyetlen gyökérelem
- Aggregáció mint reláció:
 - A metamodelben definált (referencia élek mentén)
 - Megkötést ad a helyes modellpéldányokra
- Körök
 - Nincs körkörös tartalmazás (a példánymodellben!)
 - Aggregáció relációk lehetnek körkörösek a metamodelben

Multiplicitás megkötések

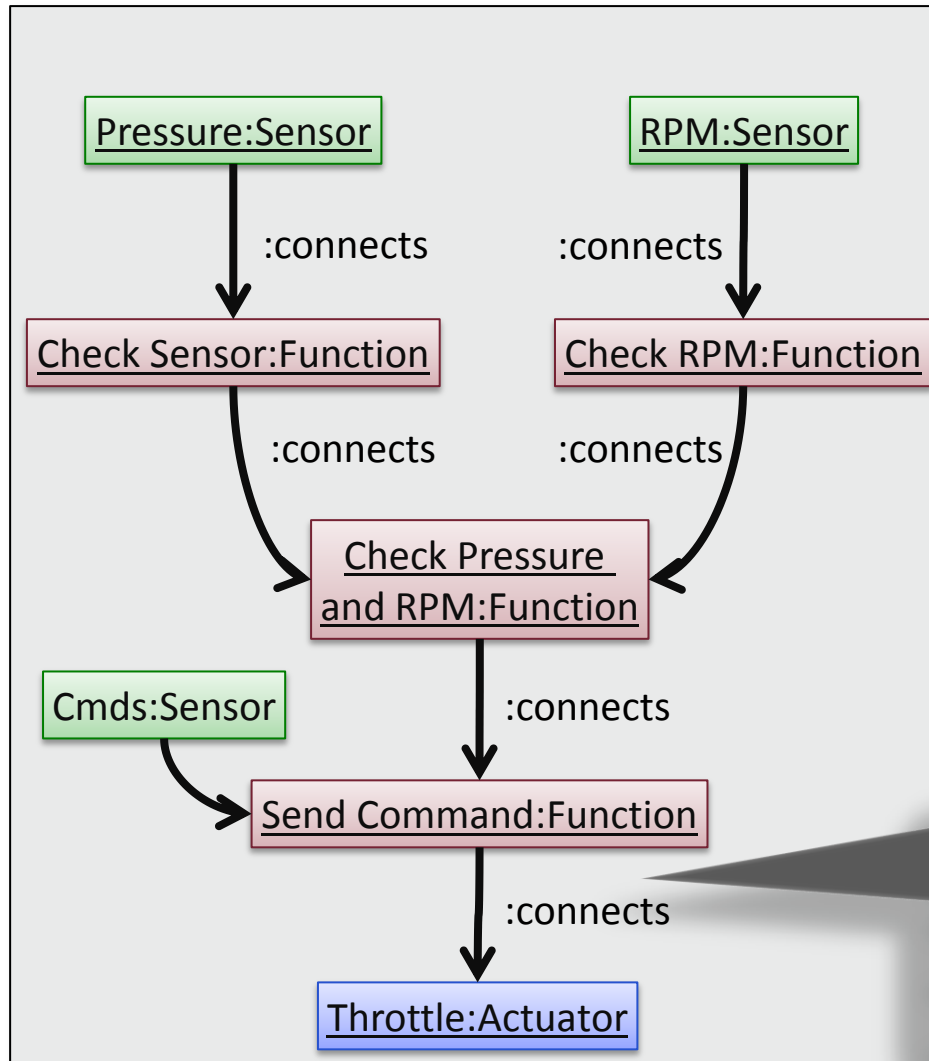
- Definíció: Alsó korlát .. Felső korlát
 - Alsó korlát: 0, 1, (nemnegatív egész)
 - Felső korlát: 1, 2, ... * (pozitív egész + any)
- Hatókör:
 - Referenciák: a megengedett számú élek adott típusú modellcsúcsok között
 - Attribútum: pl. string-tömbök (beépített értékek)



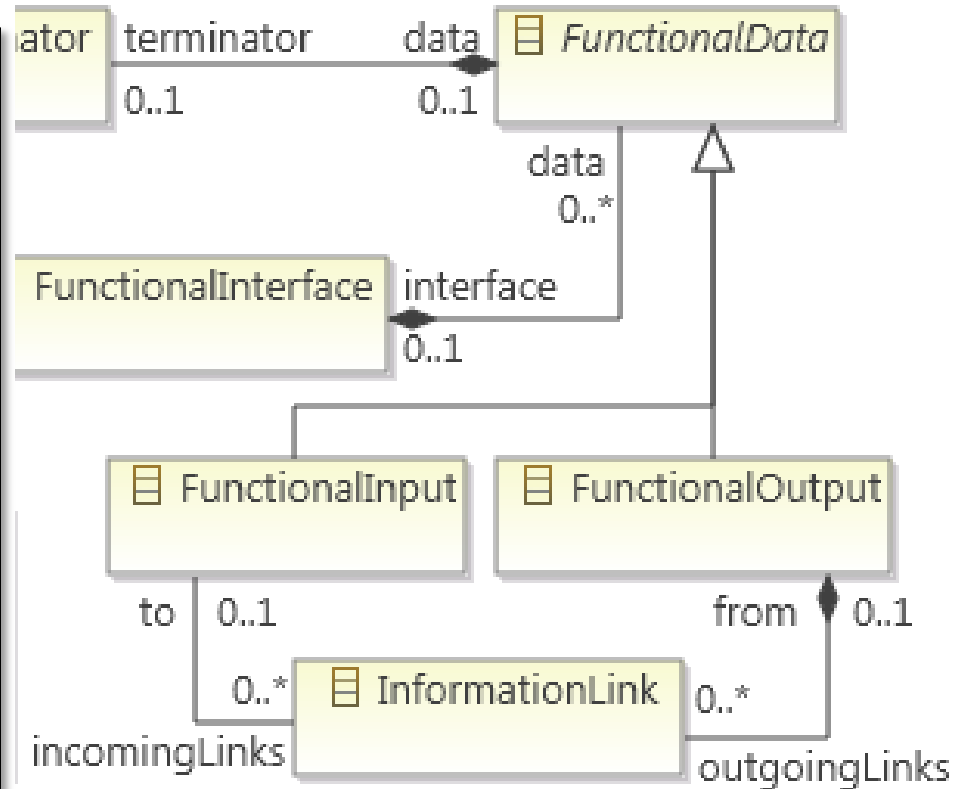
Származtatott elemek és modellnézetek

Vigyázat csalog: Honnan jön a „connects” él?

„Példánymodell” → Konkrét szintakszis



Metamodell

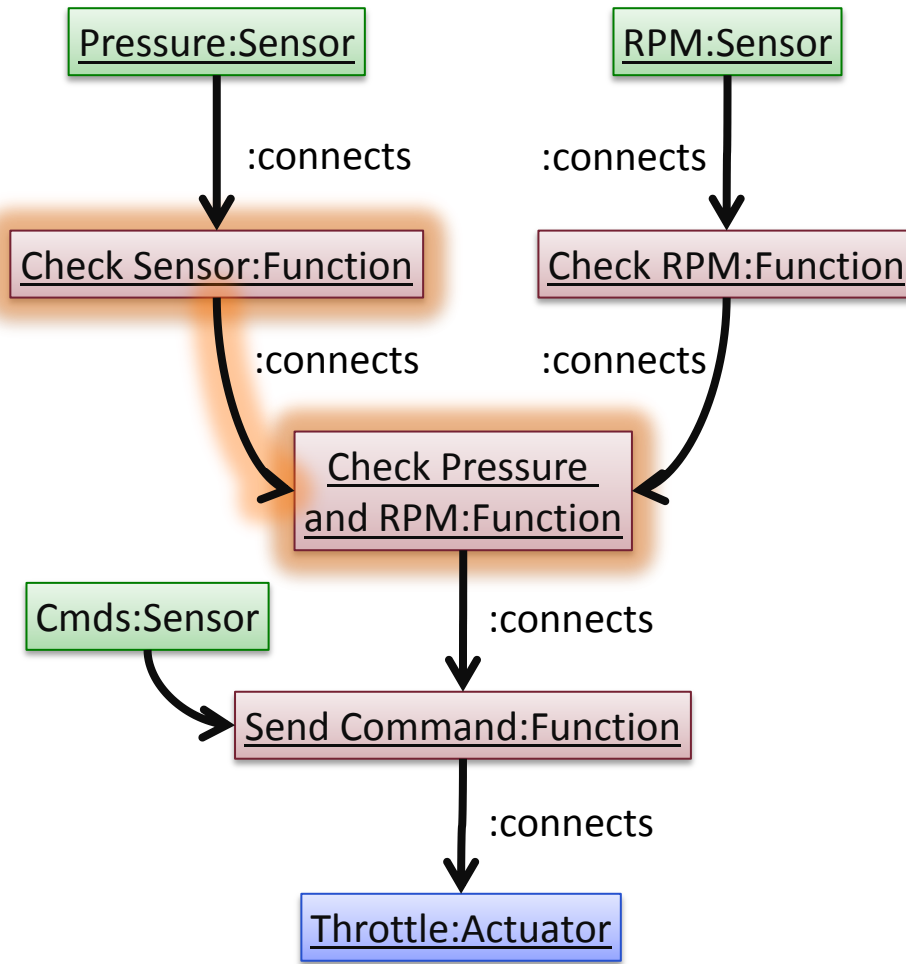


Származtatott él

- nem permanens adat
- a modell más részeiből számolt
- modell-lekérdezés definiálja

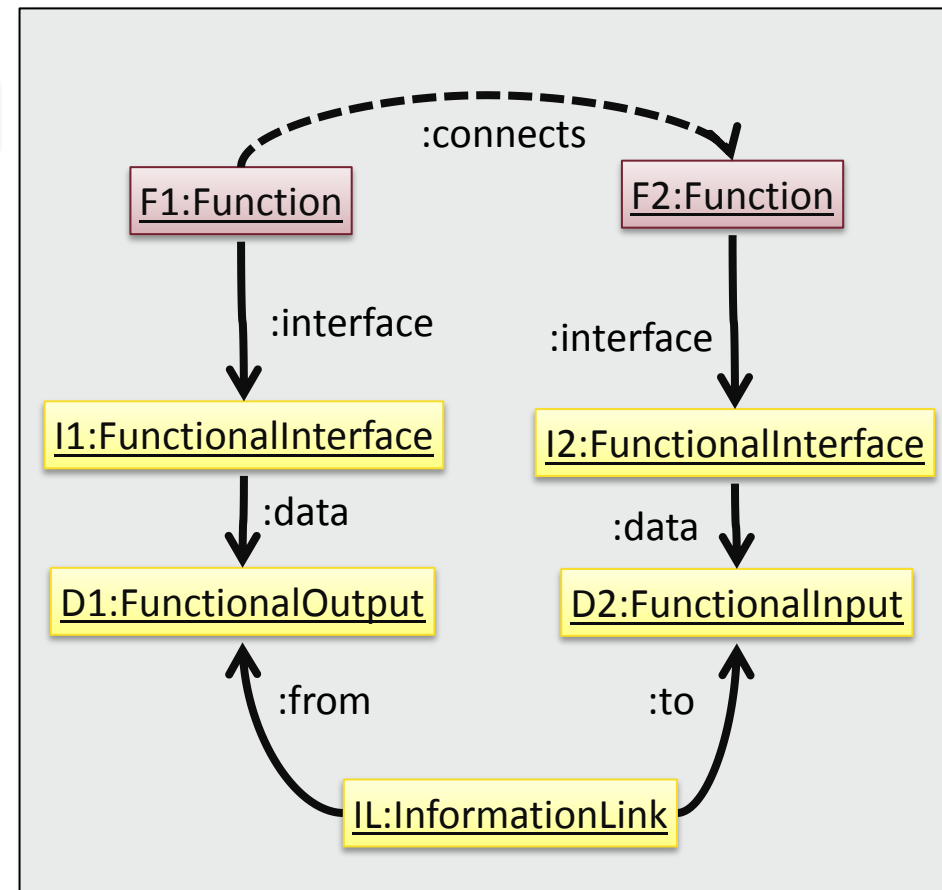
Származtatott élek definíciója

■ Nézet



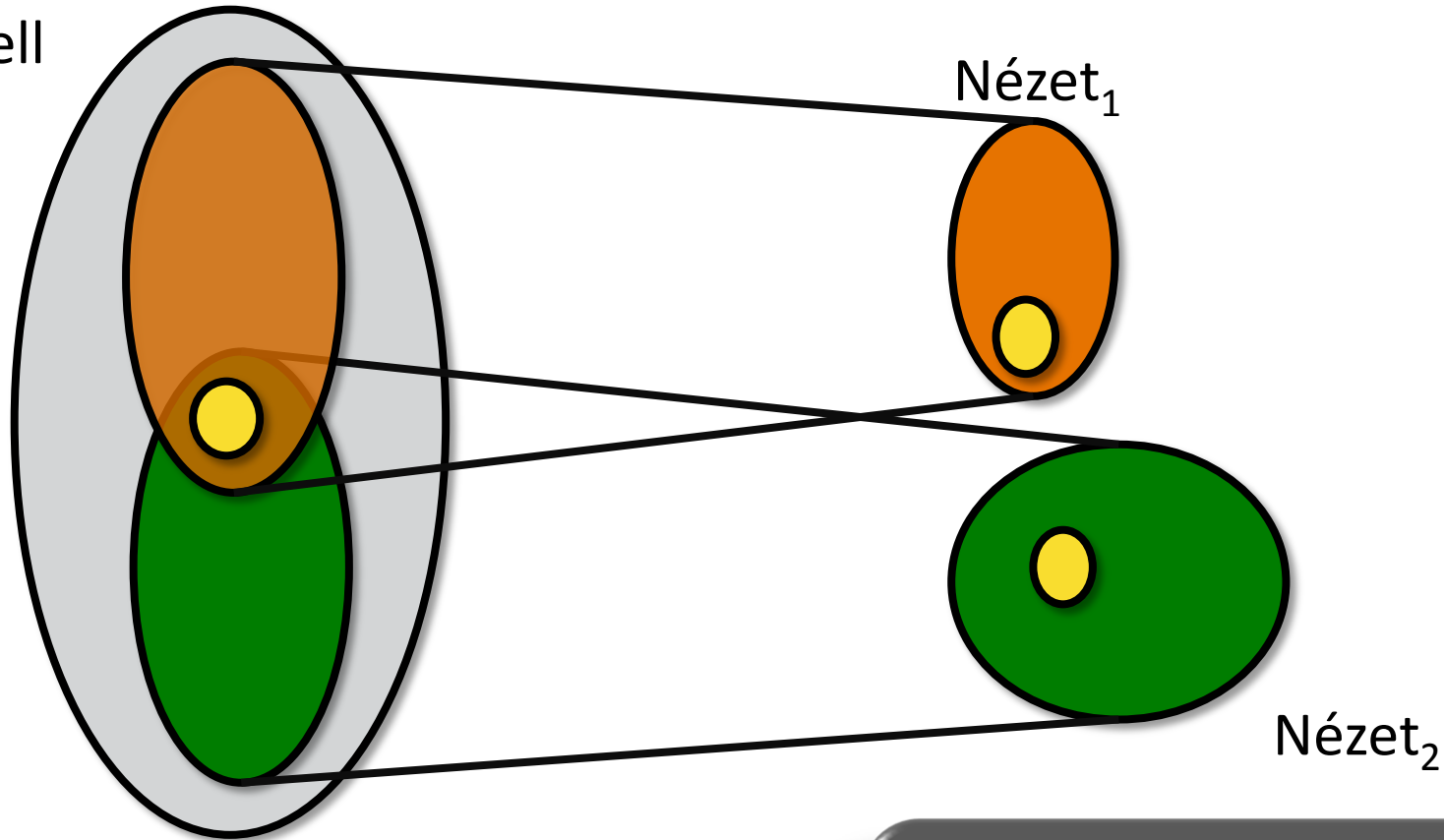
■ Lekérdezés/Mintaillesztés:

- Mintakeresés a modellben (absztrakt szintakszis!)



Modell vs. Nézetek

Modell



Lekérdezés(A,B):

- olyan A, B modellempárok
- kielégítik a lekérdezés feltételét
- 1 / összes példány felsorolása
- A, B lehet ki vagy bemenet

Nézet:

- modellből származtatott
- lekérdezés definálja
- automatikus frissítés a modell változása esetén

Konzisztenciaellenőrzés

Konzisztenciaellenőrzés kérdései

Modellszintű:

Egy modell megfelel-e a nyelv specifikációjának?

- Azonnali hibajelzés
- Nagy és változó modellek
- Komplex nyelvi kényszerek

Módszerek: Modell-lekérdezések

- Object Constraint Language (OCL)
- Gráfminták (SPARQL, IncQuery)
- Adatbázisok?

Nyelvszintű:

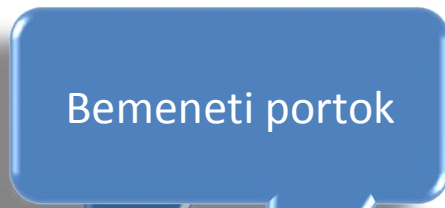
A nyelv specifikációja konzisztens-e?

- Ellentmondásmentesség
- Egyértelműség (determinizmus)
- Teljesség

Módszerek: Logikai következtetők

- Leíró logikai következtetők
- SAT megoldók
- SMT megoldók

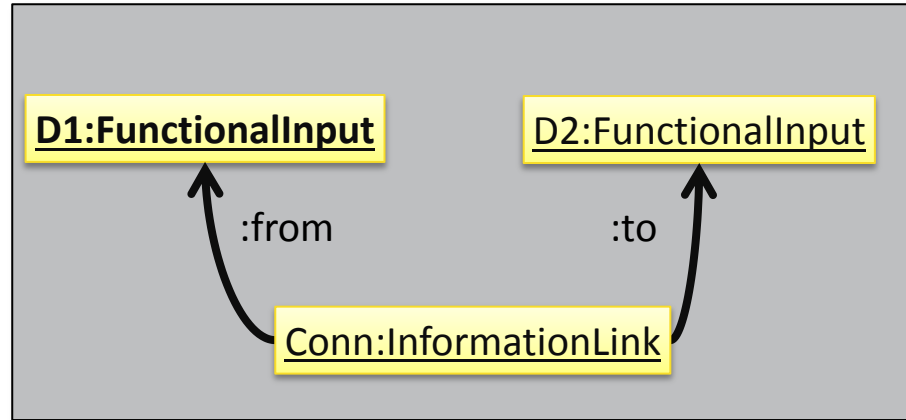
Jólformáltsági kényszerek



Function A



Function B



```
@Constraint(severity = "error", location = conn,  
message = "Both ports of $conn.name$ are inputs!",  
targetEditorId="hu.bme.mit.transima.pdm.ui.editor2")
```

```
pattern directConnection(conn:InformationLink) = {  
    InformationLink.from (conn, d1);  
    InformationLink.to(conn, d2);  
    FunctionalInput(d1);  
    FunctionalInput(d2);  
}
```

Kényszernyelvek:

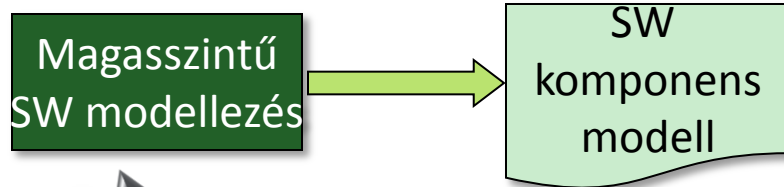
- OCL, IncQuery, (SPARQL)
- deklaratív: mit? (és nem hogyan?)

Kihívás:

- hatékony kiértékelés
- nagy modellek felett

Kritikus rendszerek modellvezérelt tervezési folyamata

Magasszintű tervezési folyamat



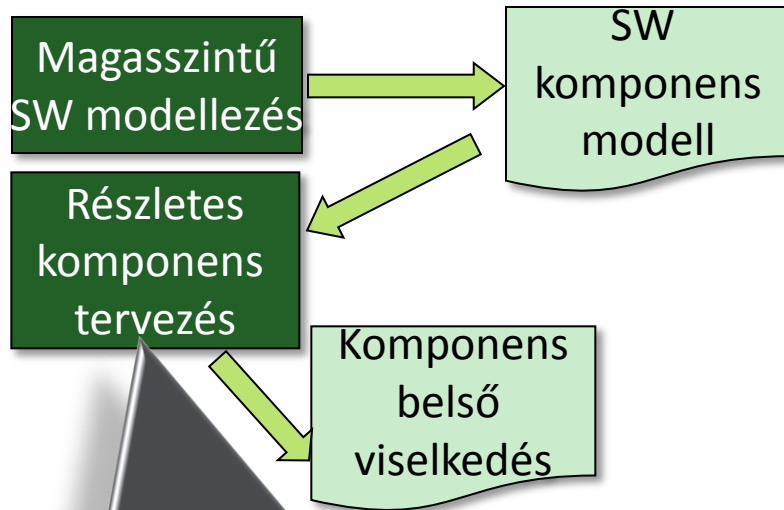
Magasszintű szoftvermodellezés

- komponensek
- interfészek
- portok
- (logikai) adattípusok

Eredmény:

- SW funkció modell

Magasszintű tervezési folyamat



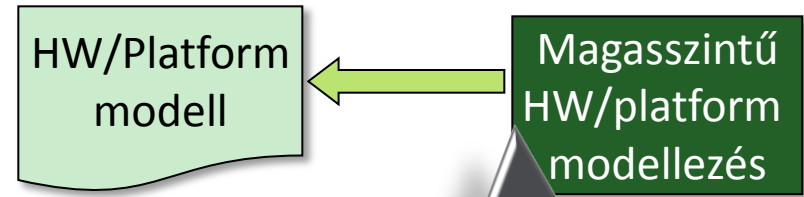
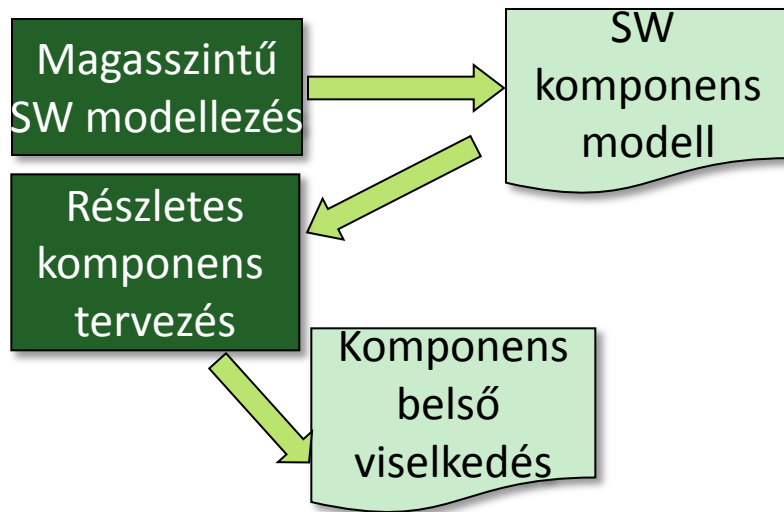
Részletes komponens tervezés

- funkcionális dekompozíció
- adatfolyam
- komponensek belső viselkedése

Eredmény:

- Állapotgépek, Adatfolyam modellek

Magasszintű tervezési folyamat



Hardver/Platform modellezés

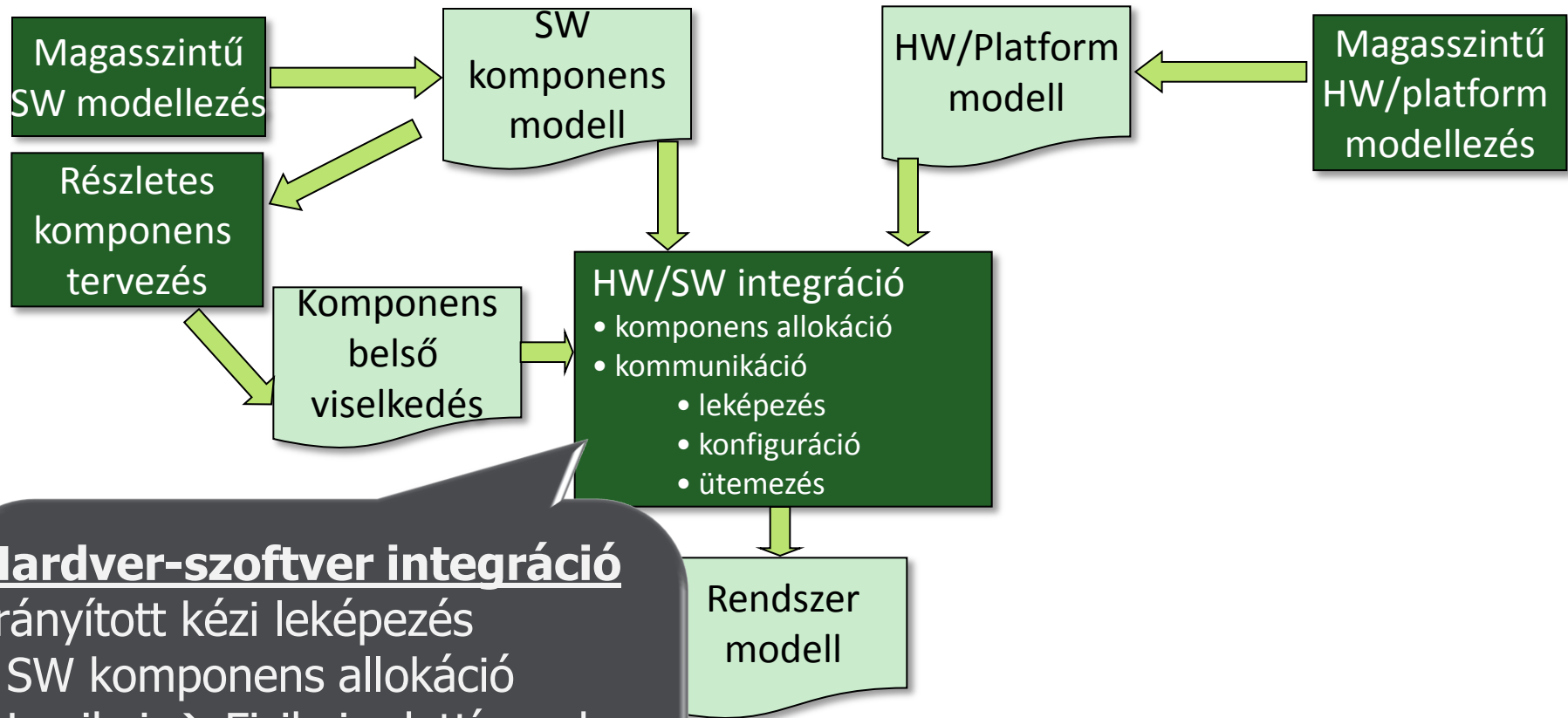
HW/Platform specifikáció

- HW erőforrások (CPU, memória, periféria, kommunikációs csat.)
- Elemek +komponens könyvtárak
- HW struktúra
- Platform szolgáltatások

Eredmény:

- Platform modell
(elem+erőforrás+topológia)

Magasszintű tervezési folyamat



Hardver-szoftver integráció

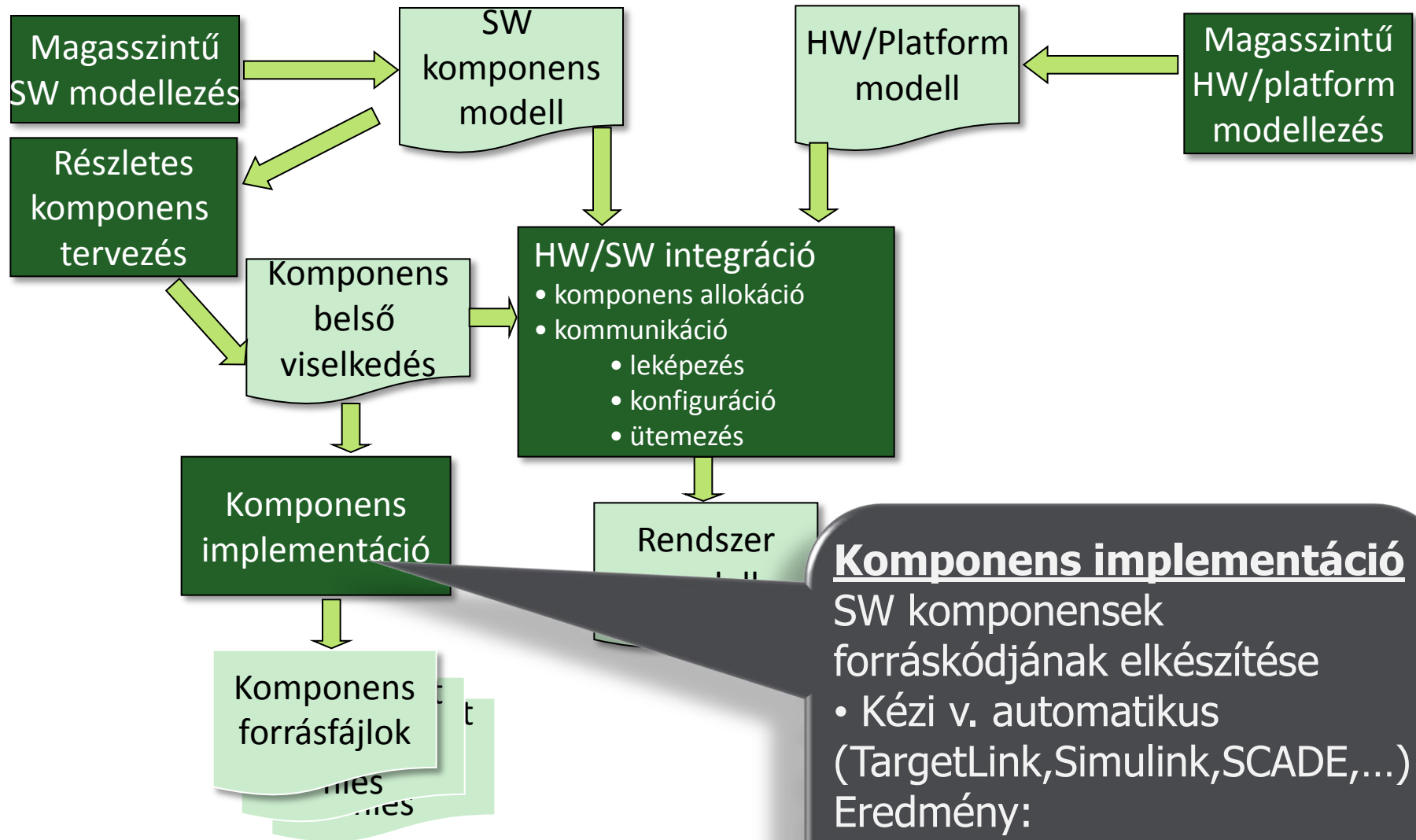
Írányított kézi leképezés

- SW komponens allokáció
- Logikai → Fizikai adattípusok
- Kommunikációs csatornák
- Ütemezés
- Megbízhatóság, WCET, memória

Eredmény:

- Integrált rendszermodell

Magasszintű tervezési folyamat

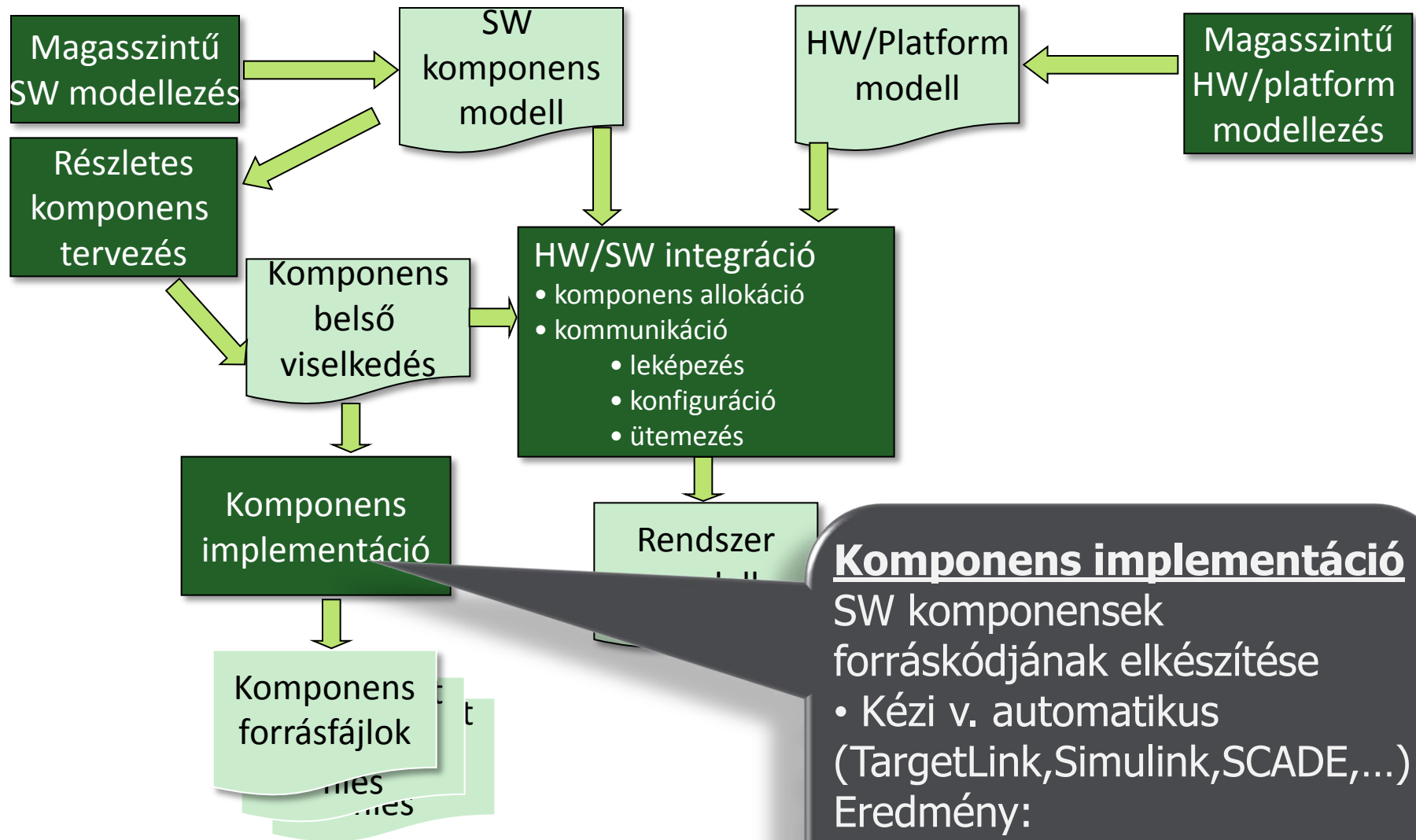


Komponens implementáció

SW komponensek forráskódjának elkészítése

- Kézi v. automatikus
(TargetLink, Simulink, SCADE,...)
Eredmény:
- Komponensek implementációi
(C, C++, stb.)

Magasszintű tervezési folyamat

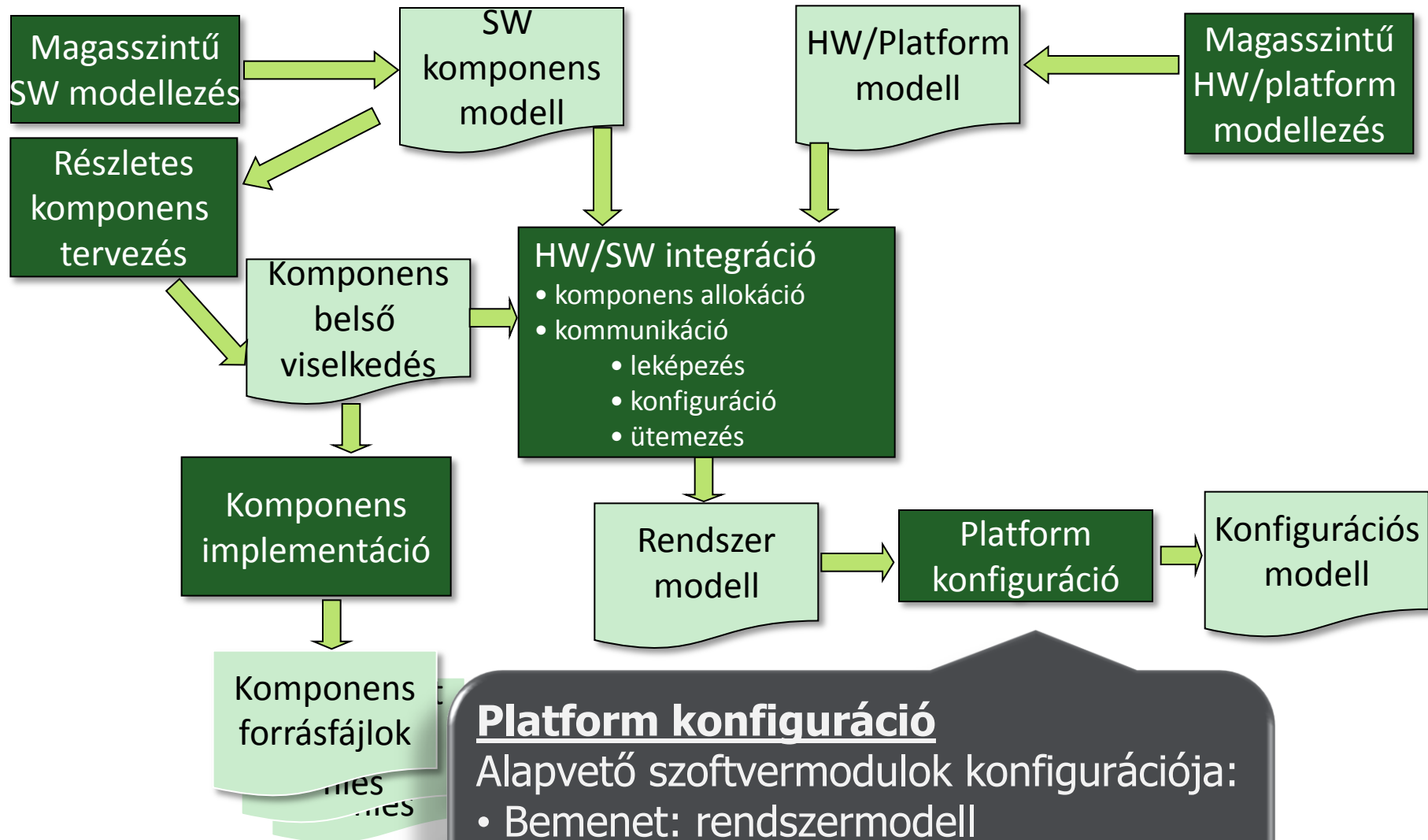


Komponens implementáció

SW komponensek forráskódjának elkészítése

- Kézi v. automatikus
(TargetLink, Simulink, SCADE,...)
Eredmény:
- Komponensek implementációi
(C, C++, stb.)

Magasszintű tervezési folyamat



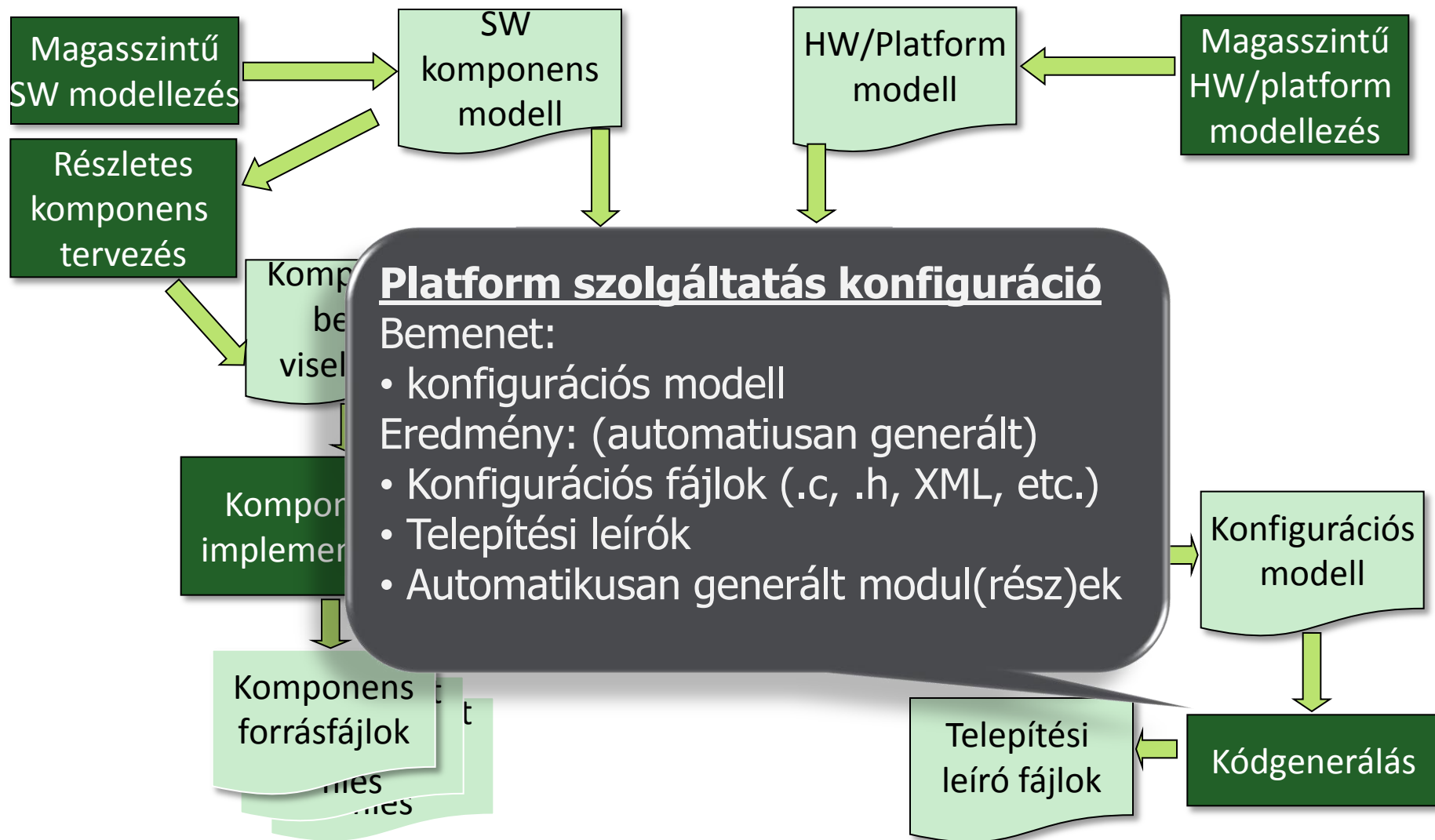
Platform konfiguráció

Alapvető szoftvermodulok konfigurációja:

- Bemenet: rendszermodell
 - Minden HW komponensre külön
- Eredmény:

- Konfigurációs modell

Magasszintű tervezési folyamat



Magasszintű tervezési folyamat

