Mintapélda:
Beágyazott valósidejű biztonságkritikus szoftverek fejlesztése formális módszerekkel és integrált verifikációval

SCADE Suite

Safety Critical Applications Development Environment

Esterel Technologies

SCADE alkalmazások

SCADE segítségével fejlesztett programkód felhasználása:

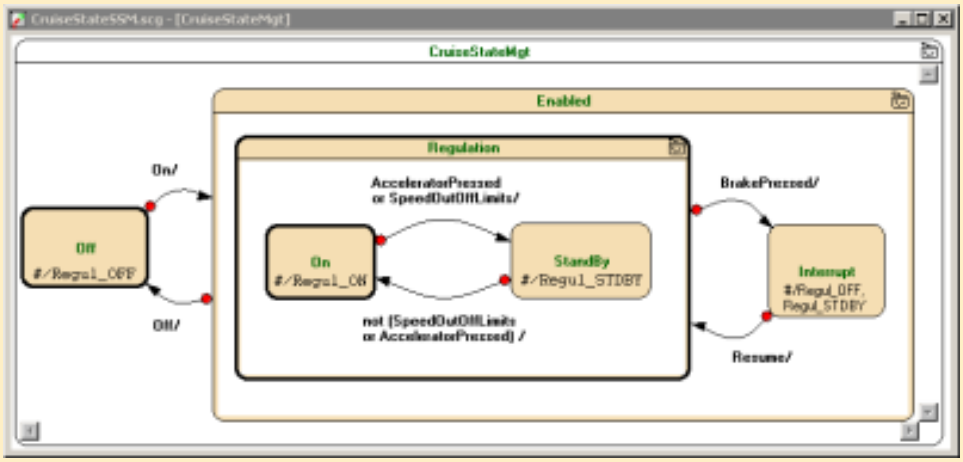
- Airbus A380, Airbus A340
- Boeing 787
- Dassault's Falcon 7X
- Ariane 5
- M51
- Eurocopter
- Z8 Helicopter (China)
- Audi A6, A8
- PSA 407, PSA 607
- BMW, Honda Motocycles
- … és sok más

Az alkalmazási terület jellemzői

- Fizikai jelenségek befolyásolása / irányítása
  - Érzékelők / beavatkozók (szabályozási kör)
  - Ember-gép kapcsolat (Man-Machine Interface)
- Vezérlők működése: Ciklikus feldolgozás
  - Érzékelők beolvasása – Feldolgozás – Beavatkozók vezérlése – Érzékelők beolvasása – …
  - Idővezérelt, eseményvezérelt, vagy lekérdezéses (polling)
- Tervezési megközelítések:
  - Vezérlés-orientált tervezés
    - Diszkrét szabályzás: Bináris jelek (pl. üzemmód váltás)
    - Véges állapotú automaták (állapotok, események, akciók)
  - Adat-orientált tervezés
    - Folytonos szabályzás: Jelfeldolgozás (diff. egyenletek)
    - Adatfolyam hálózat (feldolgozó komponensek, adatutak)

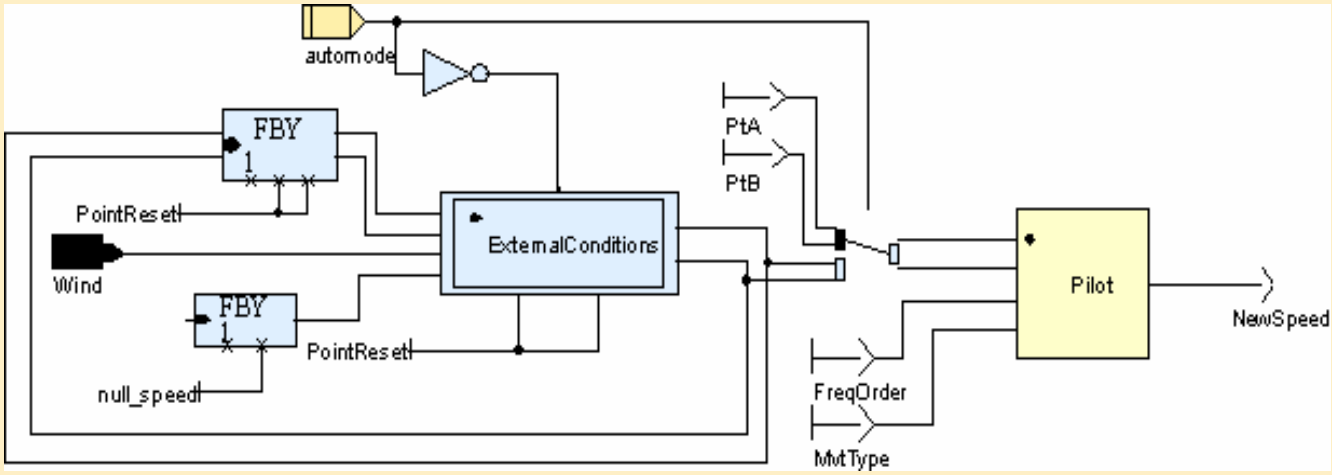
Biztonságos állapotgép

- Kötött állapothierarchia
  - Nincs állapotátmenet a hierarchiaszintek között
- Modell elemek köre korlátozott
  - Pl. nincs emlékező állapot
- Determinisztikus működés (megkötések)

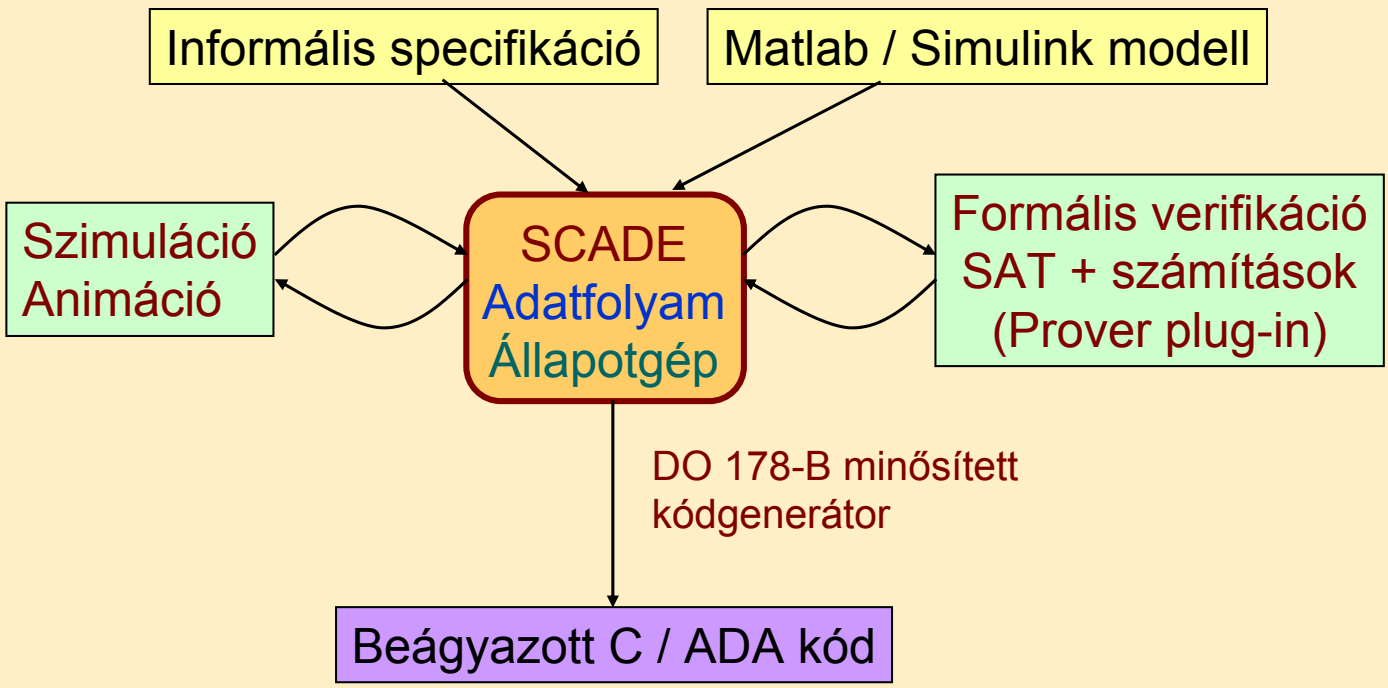


Adatfolyam diagramok

- A funkcióblokkok a számítási egységek
- Az irányított élek az adatáramlás irányát jelzik
- A bemeneteket periodikusan mintavételezzük
- A kimeneteket ciklikusan számítjuk / érvényesítjük



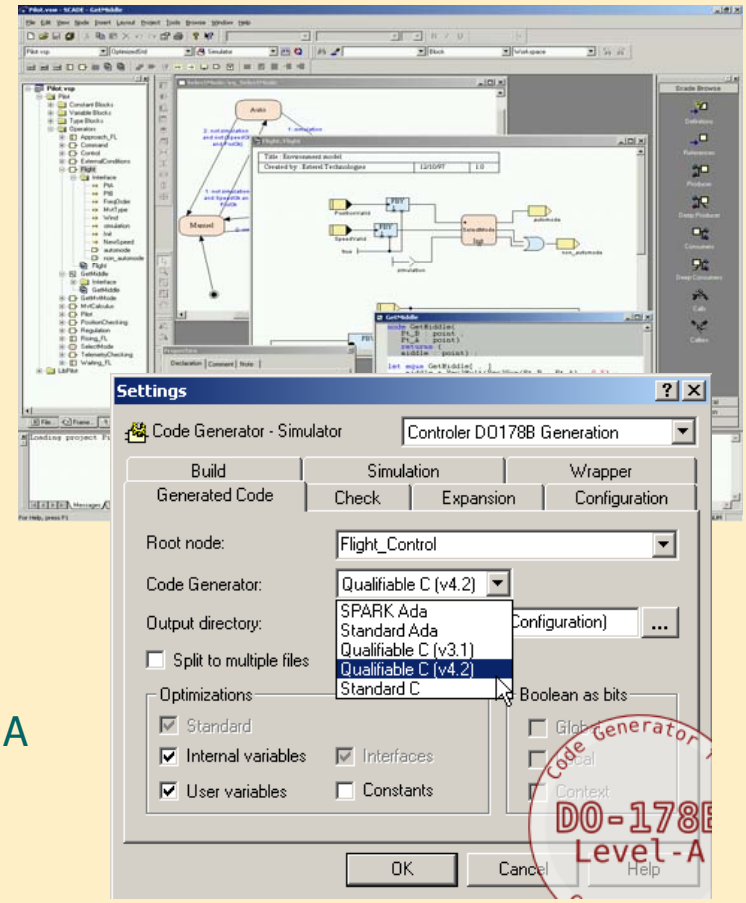
A tervezési folyamat támogatása



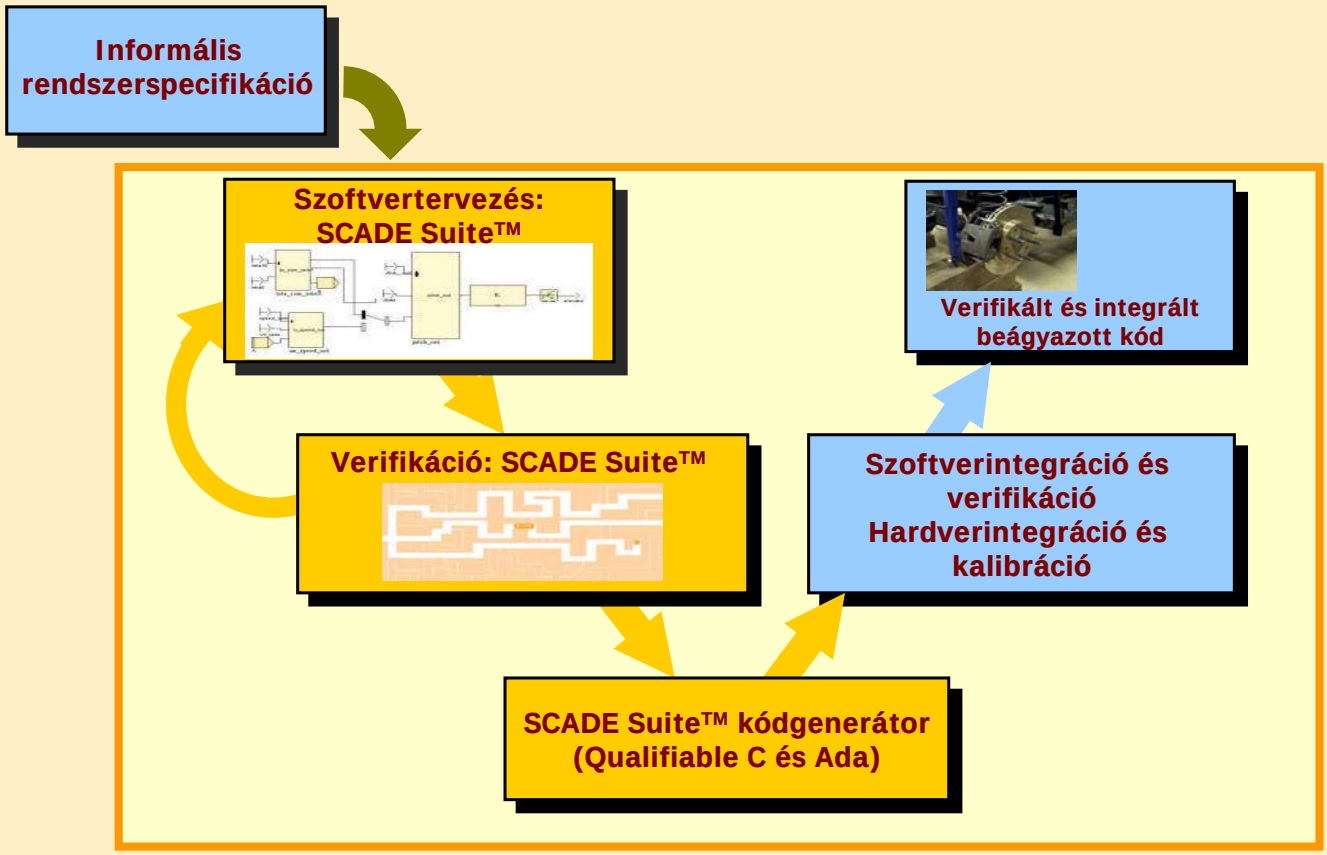
Szemantika megőrzése + minősített kódgenerátor és fordító
⇒ elhagyható a modul és / egységtesztelés (Airbus: 50%)

SCADE Suite illetve SCADE Drive

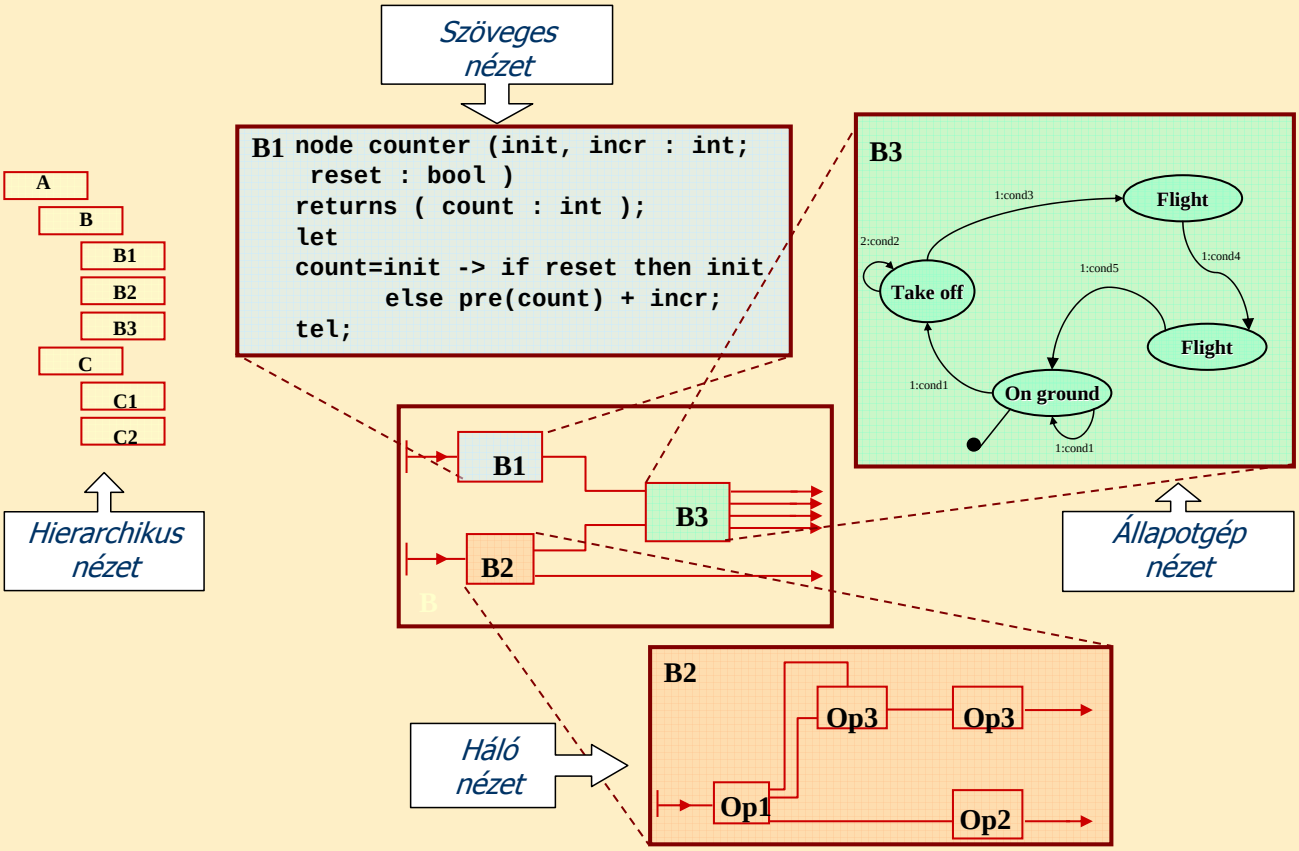
- Grafikus szerkesztőfelület
  - Adatfolyam diagramok
  - Biztonságos állapotgépek
- Statikus ellenőrzés
- Szimuláció
  - Interaktív és kötegelt mód
  - Tesztelési / debug funkció
- Formális verifikáció
  - Tulajdonságok ellenőrzése
- Kódgenerálás
  - Ada és C
  - Qualified C: DO-178B Level A vagy MISRA megfelelés



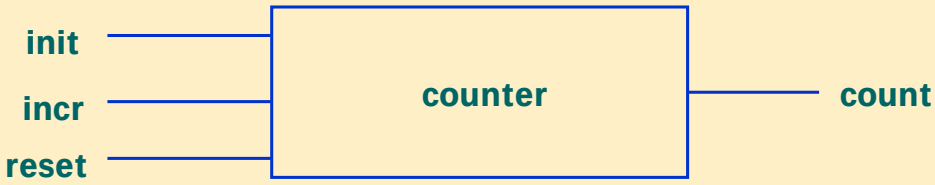
SCADE Suite™/SCADE Drive



SCADE formalizmus: nézetek igény szerint



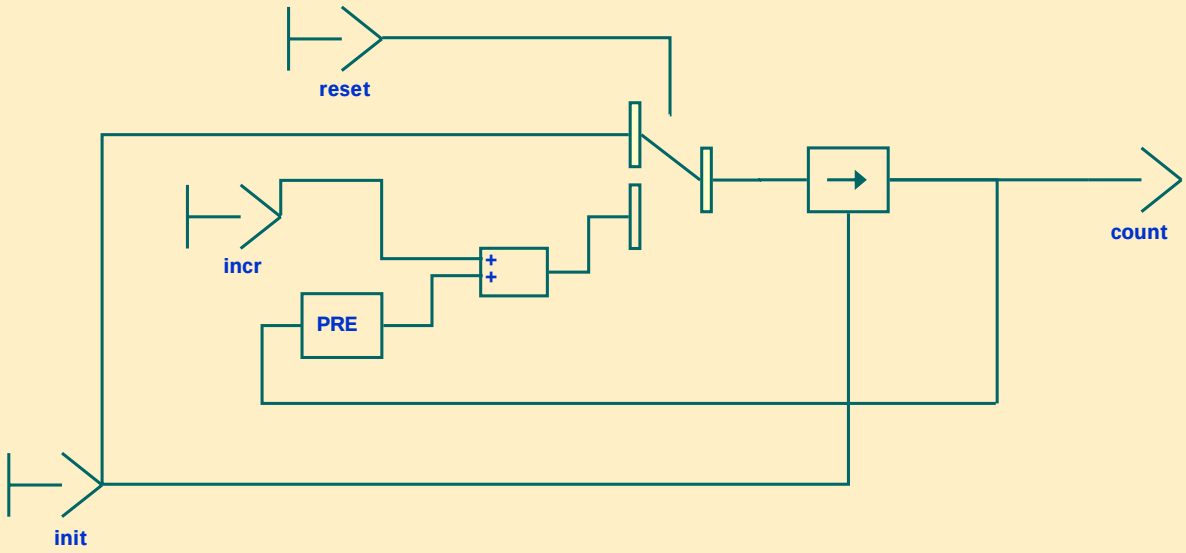
Példa: Szöveges komponens



A működés szöveges leírása:

```
node counter (init, incr : int; reset : bool)
  returns (count : int);
let equa eq_counter [,]
   count = init -> if reset then init
           else pre(count) + incr;
tel;
```

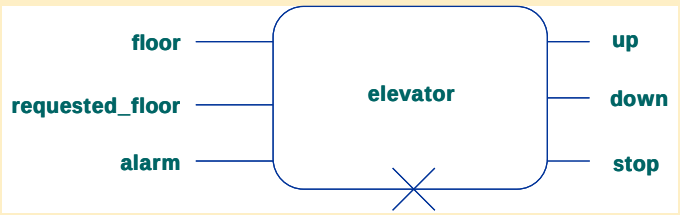
Példa: Grafikus komponens (blokkdiagram)



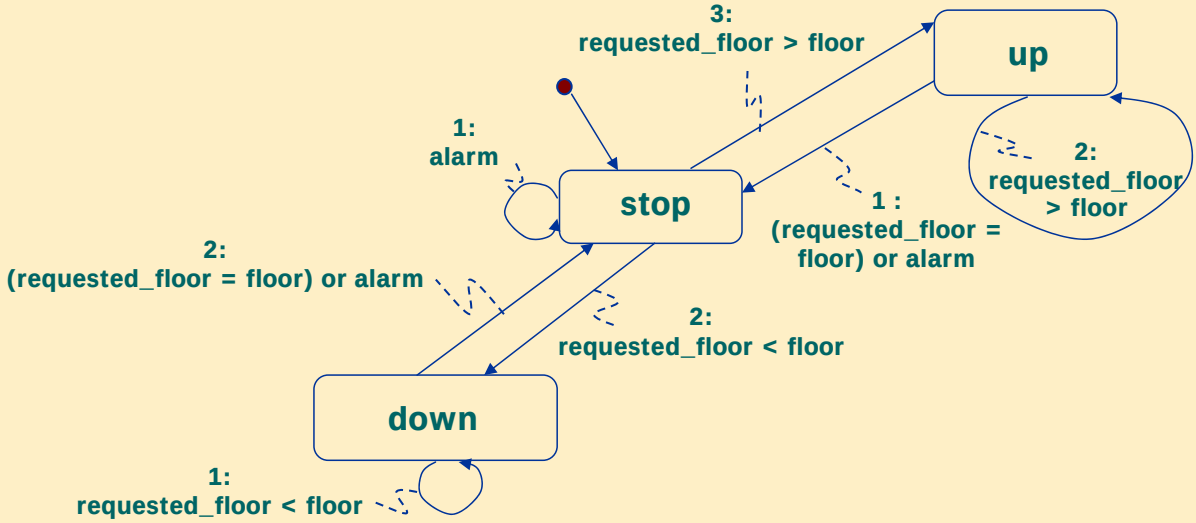
Az ekvivalens szöveges leírás:

```
count = init -> if reset then init
          else pre(count) + incr;
```

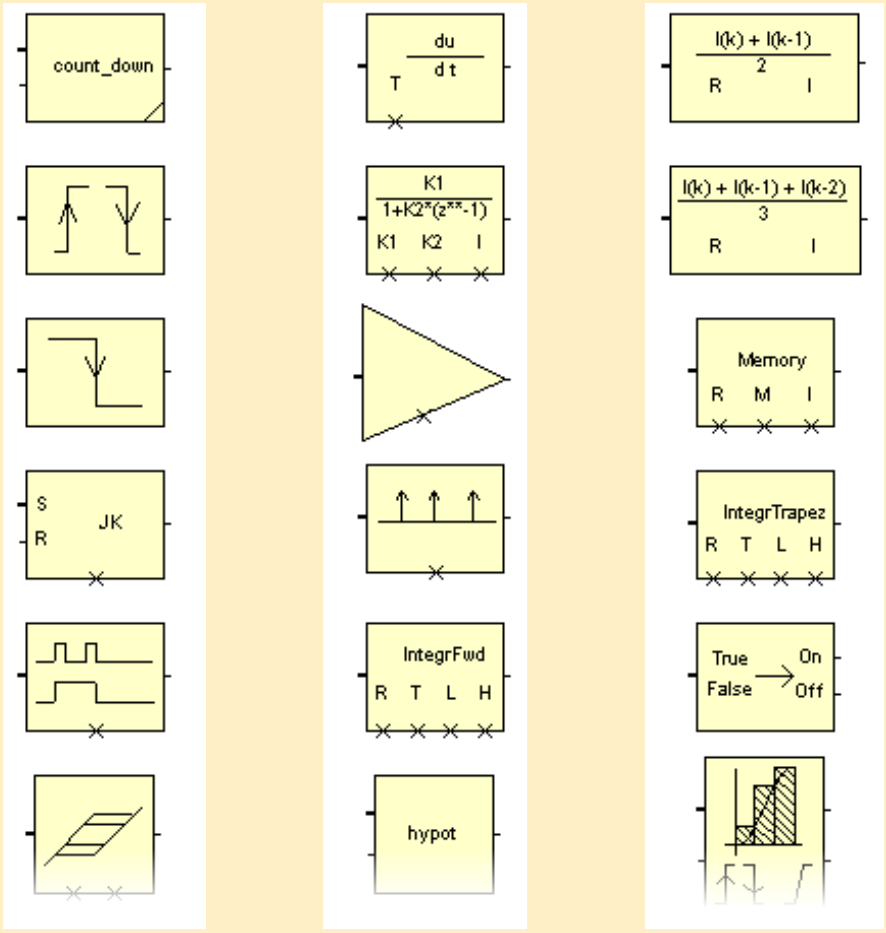
Példa: Állapotgép komponens



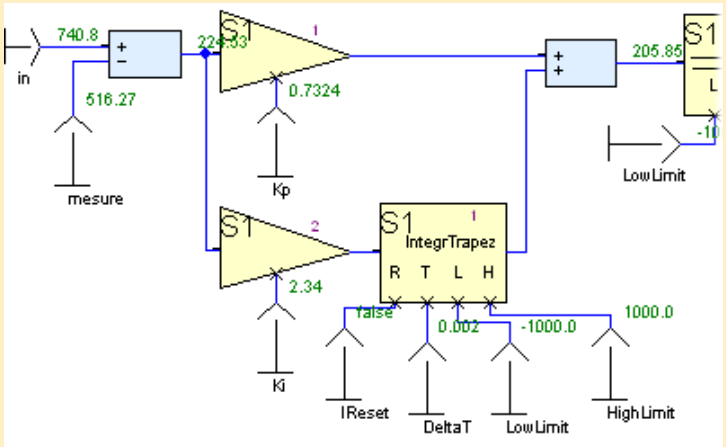
A működés állapotgépe (Moore):

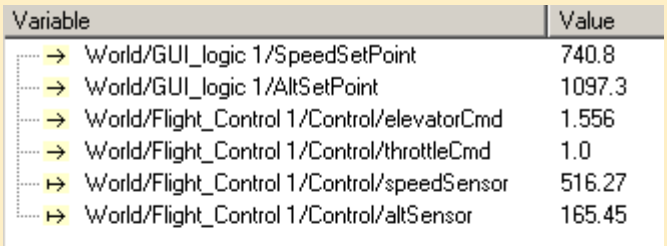


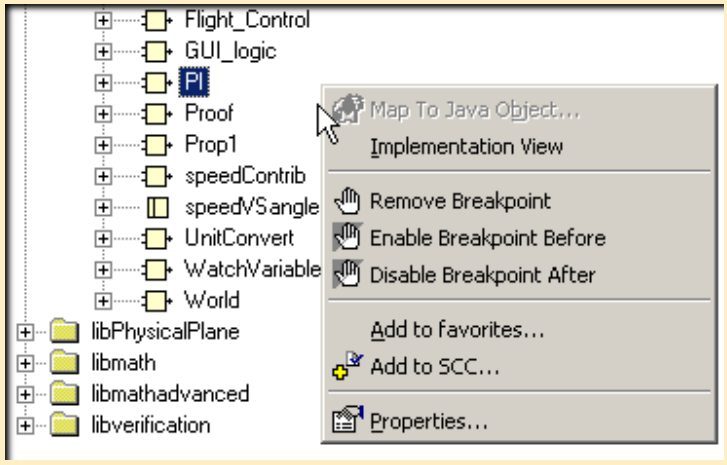
SCADE blokk-könyvtár

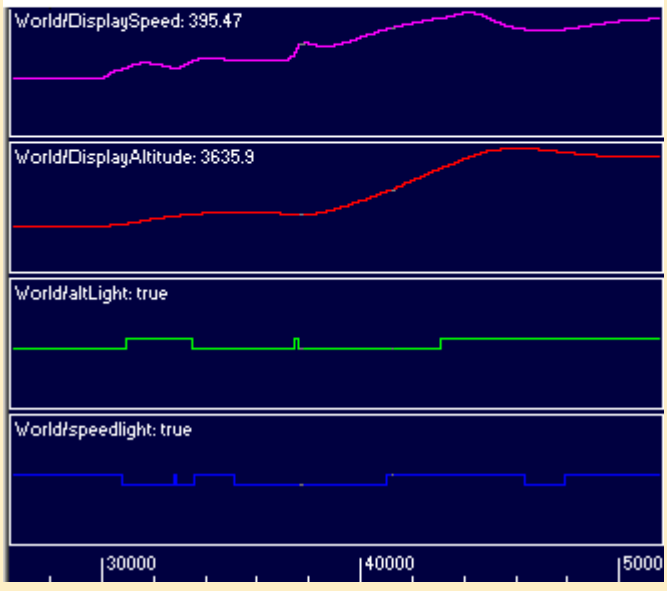


Ellenőrzési technikák: Szimuláció



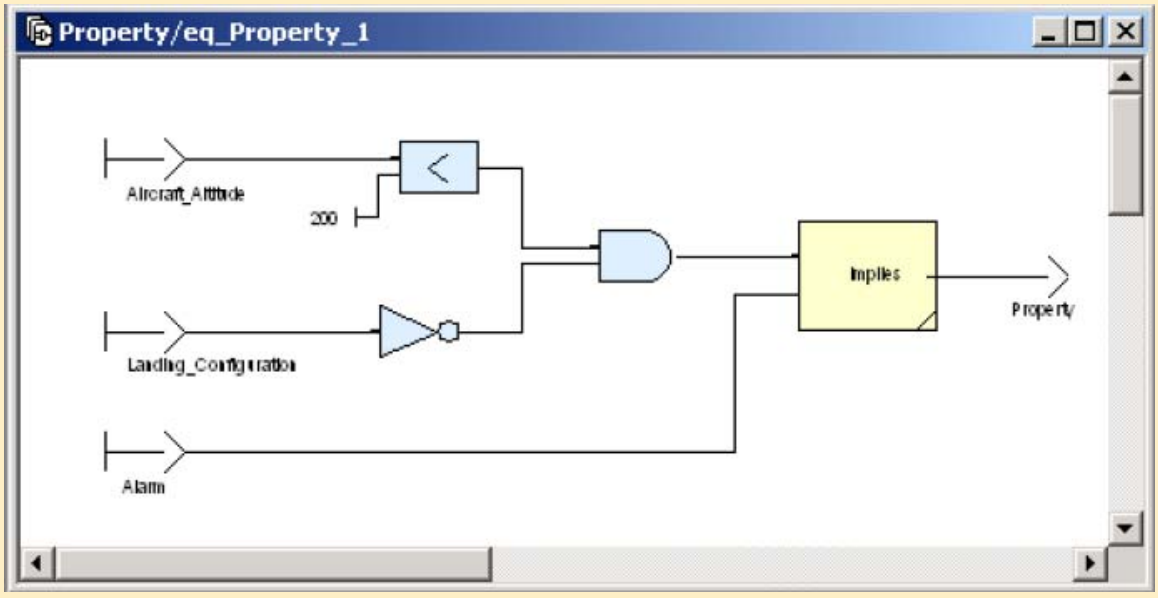






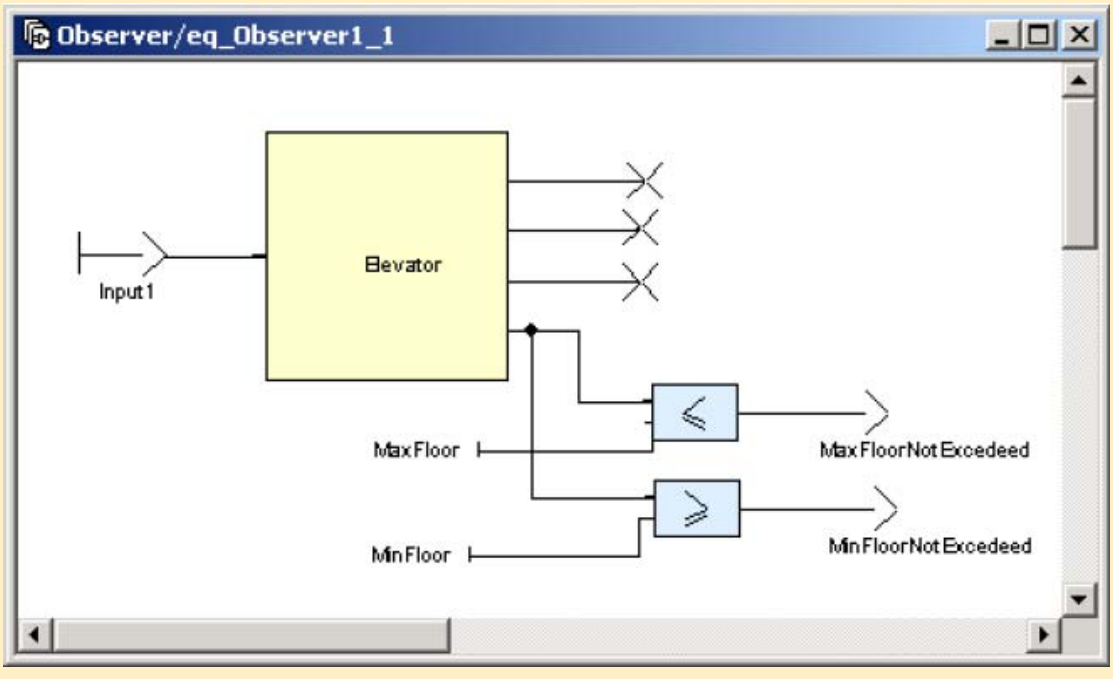
Ellenőrzési technikák: Formális bizonyító motor

- Tulajdonságok definiálása: Tulajdonság komponens (property node)
  - A helyes működést fogalmazza meg, pl.
    Aircraft_Altitude < 200 and not Landing_Configuration implies Alarm



Ellenőrzési technikák: Formális bizonyító motor

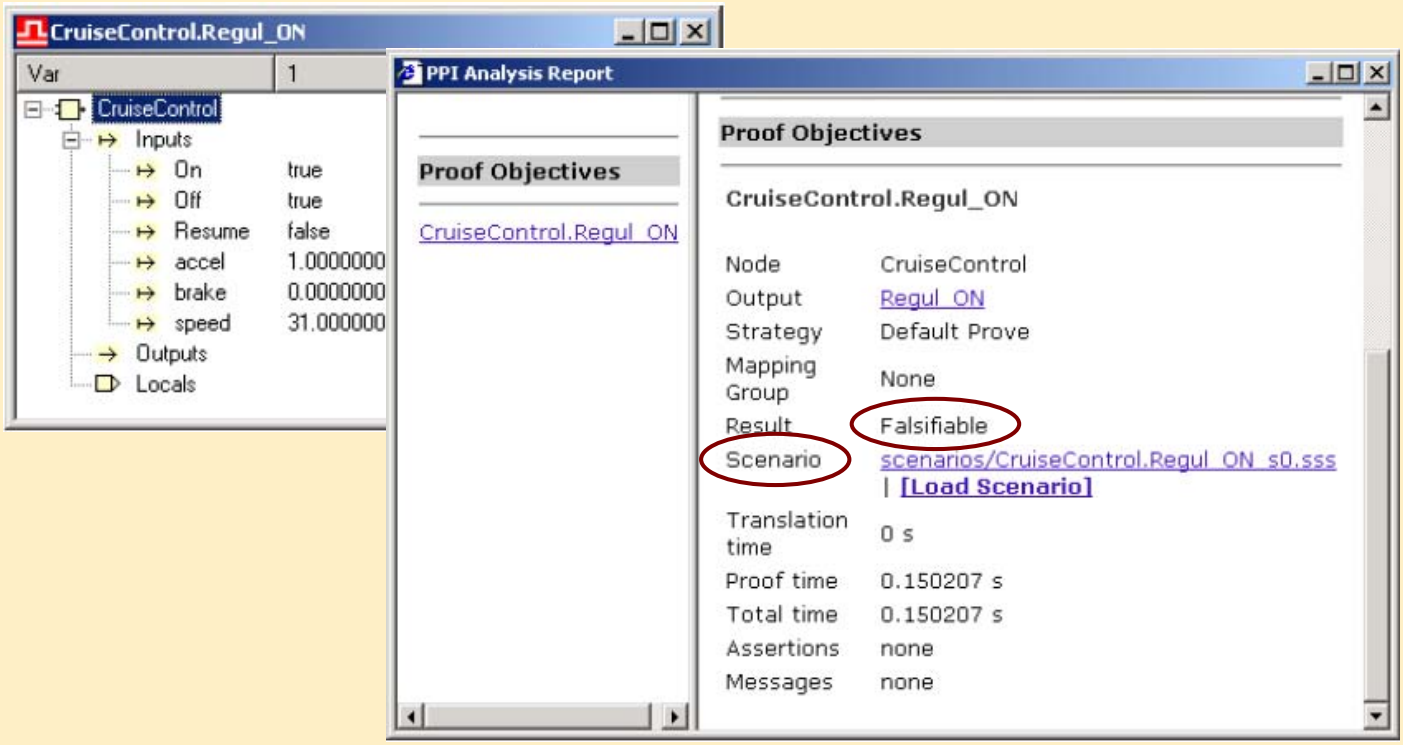
- A tulajdonság komponensek kapcsolása a tervhez: Megfigyelő komponensek (observer nodes) beillesztése



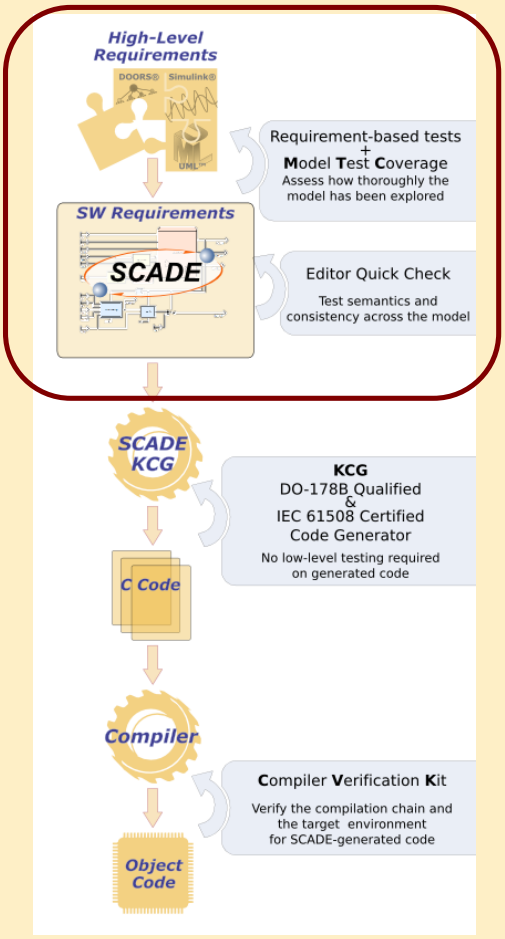
Ellenőrzési technikák: Formális bizonyító motor

Bizonyítási cél: Megfigyelő komponens kimenete igaz legyen

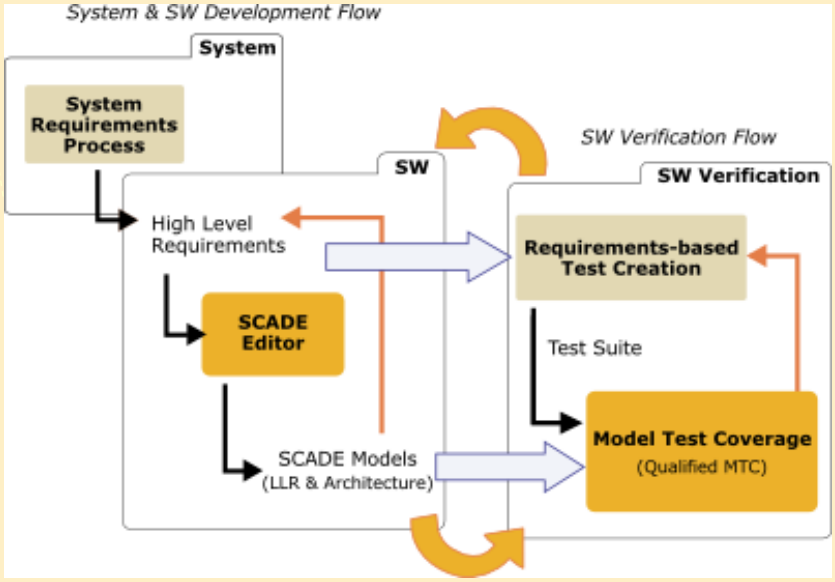
- Bizonyítás: Kimerítő keresés, ellenpélda generálás (SAT)



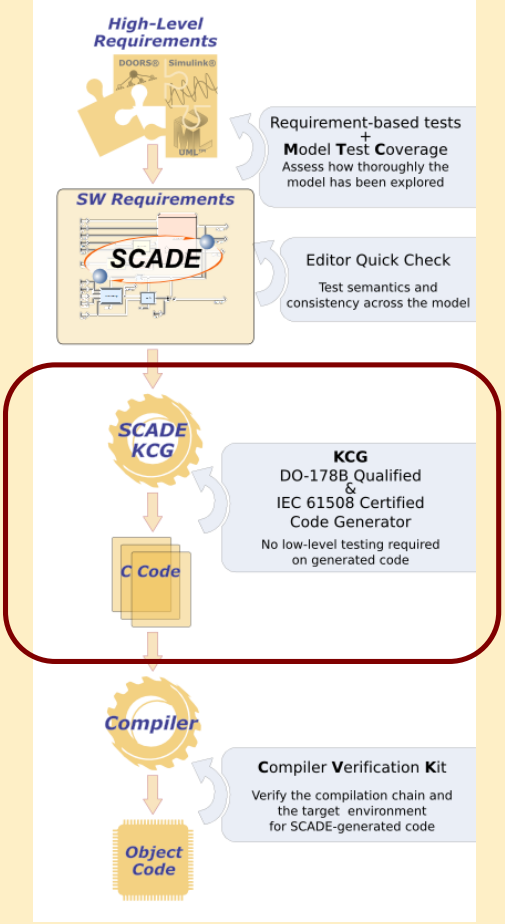
Ellenőrzési technikák: Modell alapú tesztelés



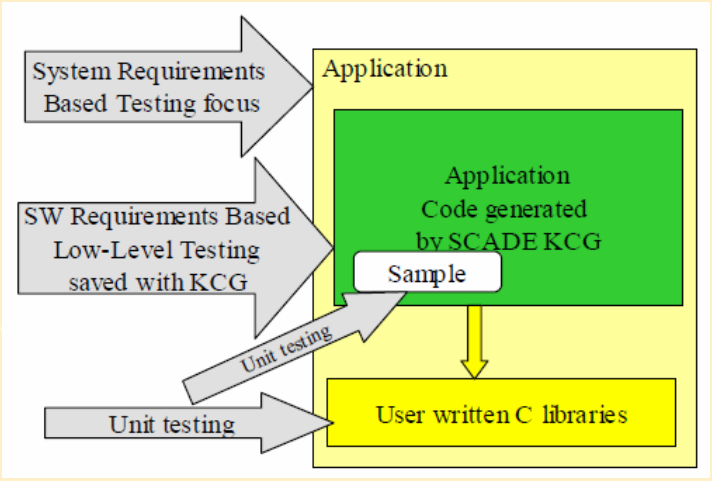
- Követelmény alapú tesztesetek
- Modell alapú tesztfedés:
  - Igazolható, hogy a modell minden eleme dinamikusan aktiválásra került
  - A teszteletlen funkciók felderíthetők



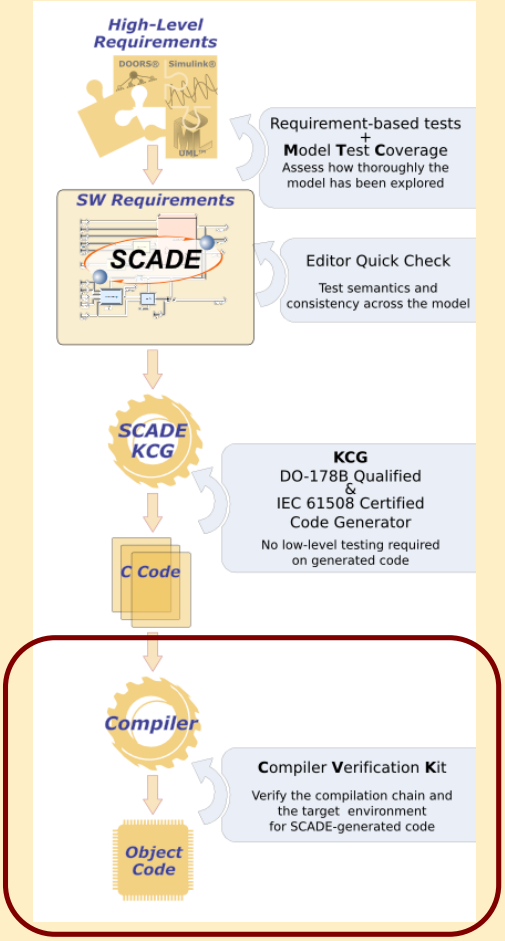
Kódgenerálás: Az ellenőrzött modell alapján



- KCG: minősített kódgenerálás
  - DO-178B, IEC 61508, MISRA szerint
  - Nincs szükség modultesztelésre a generált kód esetén
- Külső vagy kézi kód:
  - Pl. könyvtári függvények belseje
  - A tesztelés nem hagyható el!



Kódgenerálás: Az ellenőrzött modell alapján



- Compiler Verification Kit:
  - Forráskód minták
  - A lefordított kódmintához tartozó teszt esetek (sikeres futtatásuk szükséges)
- A verifikáció köre:
  - (Saját) fordító
  - Futtató platform

Manual Coding		DO-178B Processes		SCADE	
Verification	Verification of Verification			Verification	Verification of Verification
		System Requirements Allocated to Software			
Review & Analyses	?			Reviews & Simulation	Model Coverage
		Software Requirements			
Tests & Analyses	MC/DC Code Coverage			Suppressed	Not relevant
		Source Code			

A kézi és SCADE verifikáció összevetése

SCADE Suite: A biztonságigazolt „szoftvergyár”