Biztonságkritikus rendszerek architektúra tervezése

Önálló laboratórium feladat összefoglalója (1. félév)

Vass ViktorWUR93Z
Konzulens: Dr. Majzik István
BME Méréstechnika és Információs Rendszerek Tanszék
Informatikai infrastruktúra tervezése szakirány, 2005/2006. I. félév

A témakör ismertetése

A biztonságkritikus rendszerek (pl. közlekedési vezérlőrendszerek) esetén a tervezési szabványok előírják a rendszer megbízhatóságának részletes elemzését az architektúra tervezés fázisában. Addig nem adható át a rendszer, amíg nem sikerül a megfelelő megbízhatóságát kimutatni. A modell alapú tervezés korszakában ezt is modellek alapján szeretnénk elvégezni.

A feladat a tanszéken kifejlesztett megbízhatóság elemzési eszköz kiegészítése oly módon, hogy egy szabványos architektúra leíró nyelven, a leginkább az autóiparban használt AADL nyelven leírt alkalmazások megbízhatósági elemzése is automatikusan elvégezhető legyen. Ehhez el kell készíteni egy olyan modult, amely képes a megfelelő adatokkal kiterjesztett, AADL nyelven leírt alkalmazásokból előállítani az eszköz által használt belső, intermediate model-t. Ez a belső modell maga a megbízhatósági gráf. A csúcsok benne a rendszer egyes elemeit reprezentálják, az élek pedig a hibaterjedési utakat. A program meglévő része ebből állítja elő a megbízhatósági elemzésekhez végső soron használt sztochasztikus Petri-háló modellt.

A feladat e félévben végrehajtott része

Megismerkedtem azon eszköz működésével, felépítésével, illetve az általa használt adattípusokkal és formátumokkal, melyet UML modellek megbízhatósági elemzésének automatizálásához készítettek.

Tanulmányoztam az AADL leírónyelv felépítését, és meghatároztam azon elemeit, melyek a megbízhatósági elemzés szempontjából fontosak (entitások, illetve az ezek között lévő virtuális és valós kapcsolatok leírói). Átgondoltam milyen értékekkel, és hogyan szükséges kibővíteni egy AADL leírást ahhoz, hogy tartalmazza a megbízhatósági elemzéshez szükséges információkat. Meghatároztam a leképezési módszert az AADL által definiált objektumok, és a jelenleg meglévő eszköz intermediate model-jének objektumtípusai között, illetve, hogy a leírás alapján az intermediate model-ben milyen kapcsolatoknak kell létrejönniük az egységek között.

Kiválasztottam egy közepes bonyolultságú AADL rendszert (egy repülőgép irányító rendszer egyszerűsített modellje), mely az AADL leírást legtöbb elemét felhasználta. Az előzőekben meghatározottak alapján elkészítettem az ennek a leírásnak megfelelő intermediate model-t, majd a meglévő eszköz segítségével ezt átalakítottam sztochasztikus Petri-hálóvá, melyen a további elemzések közvetlenül elvégezhetőek.