

# Biztonságkritikus rendszerek architektúra tervezése

## Önálló laboratórium feladat összefoglalója (2. félév)

Vass Viktor WUR93Z

Konzulens: Dr. Majzik István

BME Méréstechnika és Információs Rendszerek Tanszék  
Informatikai infrastruktúra tervezése szakirány, 2006/2007. II. félév

### A témakör ismertetése

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

A feladat a tanszéken kifejlesztett megbízhatósági elemző eszköz kiegészítése oly módon, hogy egy szabványos architektúra leíró nyelven, a leginkább a repülőgép és autóiparban használt AADL nyelven leírt modellek 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

Az előző félév során az AADL leírónyelv és az IM között létrehozott leképezési mintát pontosítottam, illetve annak szabályait megfogalmaztam oly módon, hogy azok szisztematikusan alkalmazhatóak, leprogramozhatóak legyenek.

Létrehoztam az AADL szintakszis kibővítéseinek szabályait tartalmazó fájlt az OSATE eszközhöz, melynek segítségével a megbízhatósági elemzéshez szükséges paraméterek könnyen megadhatóak egy aadl modellben.

Leprogramoztam a transzformációt végrehajtó java programot, mely bemeneteként egy aaxl leírást vár, kimenete pedig a kész IM modell.

A programot az előző félévben is használt AADL rendszerrel (egy repülőgép irányító rendszer egyszerűsített modellje) teszteltem, mely az AADL leírást legtöbb elemét felhasználta. A szabályok és az előzőleg elkészített modellek alapján megvizsgáltam az átalakítás helyességét.