Hibamodellezés Absztrakt Állapotgépek (ASM) segítségével

Bokor Péter, V. évf. műszaki informatika

Konzulens: Dr. Pataricza András egyetemi docens
Méréstechnikai és Információs Rendszerek Tanszék

Az informatikai rendszerek, ezen belül a beágyazott rendszerek rohamos elterjedése mindinkább magával vonja az általuk biztosított szolgáltatásának biztonságának garantálását. Ez az alkalmazások széles körénél azt is jelenti, hogy a rendszerbe hibatűrési funkciókat kell beépíteni annak érdekében, hogy a szolgáltatás hibák fellépte esetén is működjék vagy legalábbis ne okozzon kárt. A bonyolultság növekedésével azonban a hibák hatásainak felmérése mindinkább problematikus, ezért szükségessé vált, hogy mind a hibák modellezését, mind pedig a hatásuk analízisét matematikai precizitású modelleken szisztematikusan végezzük. A dolgozat témája tehát elsődlegesen a beágyazott rendszerek területére fókuszálva informatikai rendszerek hibáinak modellezése és automatizált analízise.
A hibamodellezése során az alapvető ötlet az, hogy a hibák hatásmechanizmusa általánosan leírható, azaz a technológia ismeretében meg lehet mondani azt, hogy milyen jellegű szokott általában a hiba hatása lenni. Ezt matematikailag a rendszer leíró eszközének metamodelljéhez kötött hibamechanizmusokkal lehet modellezni és a jó alkalmazás modelljéből transzformációval lehet meghatározni a hibás mutációkat.

Az Absztrakt Állapotgépek (ASM, Abstract State Machines) egy univerzális modellező nyelv, melynek segítségével nemcsak formálisan modellezhetjük leírandó rendszerünket, hanem alkalmas arra is, hogy különböző modellezési paradigmák (pl. UML diagramtípusok vagy adatfolyam háló stb.) szemantikáját matematikai szabatossággal specifikáljuk. Használatának az elmúlt évekbeli rohamos terjedése arra vezethető vissza, hogy a metodika jól ötvözi a formális rendszerleírás precizitását, ill. a számítástechnikai nyelvekhez hasonló praktikus specifikáció módszereit, azaz egyszerre nyújt precizitást és megbízhatóságot, ill. érthetőséget és általánosságot.

A szokásosan nagy számú hibás mutáció birtokában elvileg elvégezhető olyan formális verifikáció és validáció, hogy akár hibás esetben is a készülék okoz-e rossz vagy veszélyes szolgáltatást, de a gyakorlati feladat méreteknél ez az analízis a számítási bonyolultság korlátai miatt kivitelezhetetlen. Ennek megkerülésére szokásos a modellekből automatikusan absztrakcióval olyan már matematikailag is kezelhető méretű leírást származtatni, amely megőrzi a vizsgálandó tulajdonságokat, azaz valósághűsége nem csökken drasztikusan, de már olyan méretű matematikai problémára vezet, amely esélyesen megoldható.

A dolgozat a fentieknek megfelelően a következő fő problémák megoldását ismerteti:

1. Hogyan lehet egy univerzális, szemantika-leíró nyelvet metamodellezéssel reprezentálni és ezen a metamodellen hogyan végezhetők el transzformációk?
2. Milyen módon lehet egy metamodell felett a hibás működés általános szabályait modellezni és matematikai transzformációk segítségével hogyan lehet inkrementálni a hibás mutációk előállítását?
3. A kapott modell alapján milyen módon lehet formális verifikációs és validációs vizsgálatokat végezni?

A dolgozat a fenti áttekintést követően röviden ismerteti a VIATRA modell-transzformációs rendszer keretében implementált kis minta tág kezelésére alkalmas prototípus fejlesztési tapasztalatait is.