Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Valósidejű biztonságkritikus rendszerek k-indukció alapú verifikációja

Tóth Tamás (RRDDD0), I. évf, (MSc) mérnök inf. szakos hallgató
Konzulens:
dr. Majzik István egyetemi docens, MIT
Vörös András tudományos segédmunkatárs, MIT
Szolgáltatásbiztos rendszertervezés szakirány
Önálló laboratórium 2 összefoglaló
2012/13. I. félév

Napjainkban egyre nagyobb szerepet játszanak a beágyazott számítógépes rendszerek, amelyeket elterjedten alkalmaznak biztonságkritikus környezetekben is, például vasúti vagy autóipari szakterületen. Ilyen rendszerek hibamentes működése kiemelten fontos, hiszen egy rendszerszintű hibajelenség komoly katasztrófához vezethet. A tervezési hibák felderítése és javítása formális módszerek alkalmazásával lehetséges, ezekkel ugyanis nemcsak a hibák jelenléte mutatható ki, hanem a rendszer hibamentessége is matematikailag megalapozott módon bizonyítható.

A biztonságkritikus rendszerek gyakran időfüggő viselkedésűek, ráadásul valósidejű követelményeknek kell megfelelniük. Ezek a rendszerek sokszor nem modellezhetők diszkrét idejű rendszerként, azaz az ellenőrzés során folytonos, idő dimenziójú változókkal is számolni kell, ami végtelen nagyságú állapottérhez vezet. Az ilyen időzített rendszerekben a végtelen állapottér vizsgálata nem megoldhatatlan feladat: rendszerek biztonsági tulajdonságainak ellenőrzésére alkalmas algoritmus a k-indukció módszere, amely az indukció általánosítása által végtelen állapotterű rendszerekre is alkalmazható.

Célom egy könnyen használható keretrendszer felépítése volt, amely modellezési és ellenőrzési támogatást nyújt időzített rendszerek verifikációjához. Munkám során az alábbi feladatokat oldottam meg:

- Definiáltam egy új modellezési formalizmust, amely segítségével időzített rendszerek működése magas szinten, a mérnöki gyakorlathoz közelálló módon leírható. A formalizmushoz olyan formális szemantikát rendeltem, amely lehetővé teszi a k-indukció alkalmazását a verifikáció során.
- Megadtam egy statikus analízis módszert, amely segítségével a magas szintű modellből a rendszer bizonyos invariánsai kinyerhetőek. A talált invariánsokkal a követelmények k-indukciós bizonyítása hatékonyan támogatható.
- A magas szintű modell megfelelő leképezésével lehetővé tettem, hogy a rendszernek ne csak biztonsági, hanem élőségi (azaz a működés során elvárt állapotok elérésére vonatkozó) tulajdonságai is vizsgálhatóak legyenek.
- A módszerhez tartozó eszközkészletet implementáltam.

A módszert sikeresen alkalmaztam egy ipari projektben, ezzel demonstrálom a módszer hatékonyságát. Az esettanulmány ismertetése során kitérek a vizsgált rendszerben a módszer segítségével talált hibára és annak kijavítására.