Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Futásidőbeli verifikáció kritikus beágyazott rendszerekben

Horányi Gergő IMJ7FZ 3. évfolyam mérnök-informatikus
Konzulens: Dr. Majzik István, MIT
Informatikai technológiák / Rendszertervezés
Önálló laboratórium összefoglaló
2010/11. II. félév

Kritikus beágyazott rendszerek fejlesztése esetén nagy fontosságú feladat a rendszer felhasználás közbeni monitorozása annak érdekében, hogy a fellépő tranziens vagy állandósult hibákat detektálni tudjuk. Munkám során egy olyan módszert dolgoztam ki, amely lehetőséget ad arra, hogy ilyen rendszereken különféle, előre specifikált tulajdonságokat futásidőben ellenőrizzünk.

Az ellenőrzött rendszerek több komponensből álló elosztott rendszerek, amelyeket modell alapon - UPPAAL időzített automaták hálózata formájában - specifikálom, majd ezekből automatikus kódgenerálás segítségével készül el az implementáció.

A futásidőbeli verifikációnak két aspektusát vizsgáltam meg. Elsőként egy úgynevezett lokális verifikációs modult terveztem meg és implementáltam. Ez esetben az elosztott rendszer komponenseit egymástól függetlenül vizsgálom. A vizsgálat tárgya, hogy az aktuális lefutás (*trace*) megfelel-e a specifikációban megadott UPPAAL időzített automata modellnek, azaz az adott komponens által felvett állapotok megengedett állapotok-e. Ezen felül további verifikációs lehetőségeket is nyújt a modul, mint például az időzítéshez kötődő invariáns feltételek ellenőrzését is. A korábban készített kódgenerátor eszközt kibővítettem, így az a komponensek generált kódját képes automatikusan a lokális monitorozáshoz felműszerezni.

Ezután megterveztem és elkészítettem egy globális verifikációs modult is. Ennek a célja az elosztott rendszer egészének ellenőrzése. A globális verifikációs modul bemenete az UPPAAL modellező eszközben már megszokott CTL kifejezések, amelyeket a globális verifikációs modul képes futásidőben kiértékelni. A kifejezések segítségével lehetővé válik, hogy a rendszer teljes állapotára és változóira temporális megkötéseket tegyünk, amelyek nem teljesülése esetén hibajelzést kapunk.

A két verifikációs modul kritikus elosztott beágyazott rendszerek tesztelése során már hatékonyan használható, hiszen tesztelés közben is tudják a specifikációtól való eltéréseket jelezni. A futásidőbeli használat során pedig egy védelmi szintet jelentenek, hiszen hiba esetén akár automatikusan egy biztonságos állapotba vihető a rendszer.

A félév során az elkészült verifikációs modulokat a tanszéken található terepasztal illetve modellvasút segítségével teszteltem. A modellvasút egy elosztott beágyazott rendszerről vezérelhető, amely mbed alapú komponensekből áll. Szintén hangsúlyos feladat volt, hogy a kódgenerátor képes legyen forráskódot készíteni a modellvasutat vezérlő komponensekhez. Ennek implementálása szintén a feladat részét képezte.