Monitorok automatikus szintézise elosztott beágyazott rendszerek futásidőbeli verifikációjához

Horányi Gergő IV. Inf., horanyi.gergo@gmail.com
Konzulens: Dr. Majzik István, Méréstechnika és Információs Rendszerek Tanszék, majzik@mit.bme.hu

Számítógépes rendszerek működése közben előforduló véletlen hibák és anomáliák detektálása futásidőbeli hibadetektálást igényel. Ennek egy megvalósítása a futásidőbeli verifikáció, azaz a működés precíz ellenőrzése a rendszer tervezése során megállapított és formalizált követelmények alapján. A futásidőbeli verifikáció egy jellegzetes megjelenése a biztonságkritikus rendszerekben alkalmazott reaktív biztonsági elvnek, ami a hibák független detektálását és a rendszer biztonságos állapotba vitelét írja elő, így fenntartva a biztonságos működést [1].

Dolgozatomban egy olyan hierarchikus monitorozó rendszert mutatok be, amely komponens- illetve rendszerszinten is képes futásidőbeli verifikációt végezni. A monitorozó rendszert elosztott beágyazott rendszerekhez (reaktív viselkedést megvalósító mikrokontroller alapú vezérlők hálózatához) dolgoztam ki. Ilyen rendszerek tervezése, a tervek ellenőrzése és a futó kód generálása időzített automata modellek alapján történhet. Így a vezérlők szintjén az automata modellek, a teljes elosztott rendszer szintjén pedig az automaták hálózatára felírt temporális logikai követelmények és futási scenariók képezik a futásidőbeli ellenőrzés alapját.

Az ellenőrzéshez szükséges monitor komponensek szoftver forráskódját a modellek és a formalizált követelmények alapján automatikusan generálom. Ennek elméleti alapját a követelményeknek megfelelő futást elfogadó automaták konstrukciója képezi. Ugyancsak automatikusan, a modellek és a követelmények alapján végzem a futó alkalmazás kódjának kibővítését (felműszerezését) annak érdekében, hogy a viselkedés megfigyelhető legyen. A kidolgozott módszerek és megvalósított technológiák előnyei és újdonságai a következőkben emelhetők ki:

- Az automatikus felműszerezés és monitorkód generálás az adott követelményekhez optimalizálja és így minimálisra csökkenti a futásidő és a kódméret növekedését.
- A rendszerszintű monitorok a klasszikus lineáris temporális logikai kifejezések helyett elágazó idejű logikán alapuló ellenőrzéseket végeznek. Így lehetőség nyílik adott lefutások halmazán (elsősorban tesztelés közben egy teszt készlet végrehajtása során) egzisztenciális jellegű követelmények (például kedvező tulajdonságú lefutások létezésének) vizsgálatára.
- A követelmény alapú monitorozás újszerű eleme a Live Sequence Chart [2] formalizmus támogatása. Ez lehetővé teszi követelmények scenáriók formájában történő specifikálását, ami szemléletes és közel áll a mérnöki gondolkozáshoz.

A dolgozatban a tervezéshez szükséges elméleti munka mellett bemutatom a monitorkód generáló alkalmazás tényleges implementációját és az első mintakísérleteket is.

Irodalom:

1. John Rushby. Runtime Certification. *Lecture Notes in Computer Science*, Volume 5289/2008, 21-35, 2008.
2. Werner Damm, David Harel. LSCs: Breathing Life into Message Sequence Charts. *Formal Methods in System Design*, 19(1):45–80, 2001.