

Házi feladat specifikáció

Mobil- és webes szoftverek

2019. 10. 08.

XCFATest

Bajcsi Levente - (XAO5ER)

levente.bajcsi@edu.bme.hu

Laborvezető: Soós Sarolta

Bemutató

A modern okostelefonok legnagyobb része az ARM valamely mikroprocesszor-architektúráját implementálja a SoC moduljában. Ezek az architektúrák sokszínűek, gyorsan változnak verzióról-verzióra, és gyakoriak bennük a programok működését akadályozó, vagy nehezebbé tevő hibák. Erre egy példa az ARM Read->Read hazard¹. Bár az ilyen hibák felderítése megoldott probléma [1], megmutattam [2], hogy a programok hibaaktivációjának felderítése messze nem triviális, formális módszer jelenleg nincs a felderítésükre. Ezzel szemben teszteléssel *kellően* meg lehet arról győződni, hogy biztonságos az alkalmazás – bár certifikálni nem lehetne ezt a tulajdonságát, jó meggyőződni arról, hogy nem fog egyből hibás állapotba kerülni az eszköz.

A fejlesztendő alkalmazás egy XCFA formalizmussal specifikált program tesztelését végezteti el.

Főbb funkciók

1. Az alkalmazással meg tudunk nyitni XCFA formalizmust tartalmazó szöveges fájlt.
2. Az alkalmazással szerkeszteni tudjuk a z XCFA formalizmusú specifikációt szöveges formában (egyszerű szöveggént, apróbb változtatások eszközölésének céljából).
3. Az alkalmazással el tudjuk menteni a változtatott XCFA specifikációt.
4. Az alkalmazással specifikálni tudunk egy tesztkörnyezetet.
5. Az alkalmazással futtatni tudjuk a tesztet.
6. Az alkalmazás kijelzi a teszt eredményét.

Irodalomjegyzék

- [1] Y. M. D. L. M. P. a. M. M. Caroline Trippel, „TriCheck: Memory Model Verification at the Trisection of Software, Hardware, and ISA,” *2nd International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2017.
- [2] A. V. V. M. Levente Bajcsi, „Will My Program Break on This Faulty Processor? - Formal Analysis of Hardware Fault Activations in Concurrent Embedded Software,” *ACM TECS*, 2019.

¹ http://infocenter.arm.com/help/topic/com.arm.doc.uan0004a/UAN0004A_a9_read_read.pdf