Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Biztonsági követelmények minta alapú formalizálása

Bártfay György, I. évf, (MSc) mérnökinformatikus szakos hallgató
Konzulens: dr. Majzik István egyetemi docens, MIT
Kritikus rendszerek főspecializáció
Önálló laboratórium 2. összefoglaló
2015/16. I. félév

A követelmények megfogalmazása igen fontos fázist jelent a szoftverfejlesztésben, különösképpen a biztonságkritikus alkalmazások esetén. Ez egy komplex feladat, továbbá a helyes és konzisztens követelmények megalkotása specifikus tudást és gyakorlatot is igényel.

A szokásos, természetes nyelven leírt követelmények gyakran nem elég precízek és könnyen félreérthetőek. Ugyanakkor a matematikai formalizmusok (például automaták, logikai nyelvek, stb.) használatakor a leírás bonyolulttá válik, ezért nehéz elkészíteni, megérteni illetve módosítani.

A dolgozatban ismertetett megoldás célja a biztonsági követelmények összeállításának egyszerűbbé és könnyebbé tétele, a helyesség és precízség megtartásával. A megoldás kihasználja, hogy a tapasztalatok szerint a biztonsági követelmények jellemzően sémákra épülnek. Erre alapozva kidolgozható egy módszer, melynek segítségével az összegyűjtött minták komponálhatóak és paraméterezhetőek, így összeállítva a komplex biztonsági követelményeket.

Ehhez elméleti kutatásként szükséges volt a minták leírásához használható formalizmus kidolgozása, a paraméterezési módszer definiálása, valamint a komponálhatóság szabályrendszerének megalkotása. A formalizmus támogatja a temporális logikai követelmények, a kontextusfüggő viselkedés és az időzítések, határidők megadását. A mintákból összeállított összetett követelményekhez leképezést definiáltunk egy precíz, formális nyelvre. Az így formalizált követelmények felhasználhatók tervek ellenőrzésére vagy futásidőbeli verifikációhoz monitorok szintézisére.

A módszer alkalmazására készített eszköz tartalmazza a leggyakoribb minták gyűjteményét valamint lehetővé teszi saját minták készítését és beillesztését. A kidolgozott formalizmusok és szabályok alapján biztosítja a minták grafikus megjelenítését, valamint ezek könnyű paraméterezhetőségét és grafikus formában történő összeállítását. Az eszköz beleillik az Eclipse környezetbe, így könnyen tanulható és használható a fejlesztés során.