Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Biztonságkritikus rendszerek tanúsítását támogató rendszer tervezése

Ágoston István (FQ2J73) II. évf, Mérnök informatikus MSc
Konzulens: Dr. Polgár Balázs, MIT
Szolgáltatásbiztos rendszertervezés szakirány
Diplomatervezés 1 összefoglaló
2010/11. II. félév

A rendszer-, és szoftverfejlesztés egyik legösszetettebb területe a biztonságkritikus beágyazott rendszerek fejlesztése. A biztonságos működés eléréséhez a szoftver (és a kapcsolódó hardver) fejlesztését igen körültekintően kell végezni. Mivel teljesen hibamentes rendszer készítése a legtöbb esetben kivitelezhetetlen, a fejlesztési folyamatot kell pontosan szabályozni a bennmaradó hibák számának minimalizálása érdekében.

A szabályozás általában valamilyen szakterület-specifikus szabvány szerint történik, mely előírásokat tartalmaz a fejlesztés menetére, kötelezővé teheti bizonyos technológia / technika használatát, illetve rögzíti az elkészült komponensek verifikálásához és validációjához szükséges lépéseket.

Éles környezetben való használat előtt a rendszert tanúsítani kell, melynek során egy tanúsító szervezet ellenőrzi, hogy a fejlesztés menete szabvány szerint zajlott-e. Az ellenőrzés alapja a biztonsági igazolás (safety case), mely tartalmazza a rendszer biztonságos működésének indoklását: kezdve az alkalmazott fejlesztési folyamat általános leírásától, egészen a konkrétan végrehajtott lépések dokumentálásáig, mely tartalmazza az elkészült részeket (modellek, kódok, modulok, stb.) és az ezekre végrehajtott ellenőrzési lépések eredményeit.

A tanúsítási folyamatot hatékonyan tudná támogatni egy olyan keretrendszer, mely lehetőséget biztosít a biztonsági követelmények és kapcsolódó szabványok előírásainak modellezésére, az előírt verifikációs és validációs folyamatok (fél)automatikus végrehajtásához és a biztonsági igazolás előállításához.

A félév során a fentebb vázolt tanúsítást támogató keretrendszer tervezésén dolgoztam, a munkát Juhász Gergellyel közösen végeztem. Ennek során áttekintettem biztonságkritikus rendszerekkel kapcsolatos fogalmakat, melyben nagy segítségemre volt a Biztonságkritikus beágyazott rendszerek című tárgy.

Kiemelt szerepet kapott a biztonsági szabványok felépítésének vizsgálata, a cél, hogy az előírásokat valamilyen formában modellezni tudjuk és a biztonsági követelmények modelljeiben felhasználhassuk. Emellett megnéztük, hogy a biztonsági igazolás modellezésére milyen megoldások léteznek, és ezt hogyan tudnánk felhasználni a keretrendszerben. Megpróbáltuk felmérni, hogy az igazolás mely részeinek előállítását lehet automatizálni, és erre a keretrendszer milyen formában tudna támogatást nyújtani: a szabványok által előírt verifikációs folyamatok modellezésével és végrehajtásával, a bemeneti és kimeneti adatok közti kapcsolatok beépíthetők a biztonsági igazolásba (biztonsági érvek, és bizonyítékok formájában). A folyamatok szerkesztéséhez és kezeléséhez a korábbi félévek munkája során elkészített folyamatmenedzsert szeretnénk felhasználni.

A témakör áttekintése után elkészítettük a keretrendszer kezdetleges architektúra terveit, és kidolgoztuk a követelmények, szabványok leírására használható modelleket.

A diplomaterv végső célja a keretrendszer terveinek finomítása és az implementáció kidolgozása, ezen belül az én feladatom első sorban verifikációs folyamatok megvalósítása és a folyamatokban felhasználandó eszközök keretrendszerhez való illesztése lesz.