Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Verifikációs folyamatok a biztonságkritikus rendszerek tanúsításában

Juhász Gergely (L2Z4UO), II. évf, (MSc) mérnök inf. szakos hallgató
Konzulens: Polgár Balázs, MIT
Szolgáltatásbiztos rendszertervezés szakirány
Diplomatervezés 1 összefoglaló
2010/11. II. félév

A szoftver- és rendszerfejlesztés egyik legösszetettebb területe a biztonságkritikus beágyazott rendszerek fejlesztése (pl. elektronikus vasúti biztosítóberendezések, autók vagy repülők vezérlőrendszere), melyet szigorú szakterület-specifikus ipari szabványok szabályoznak. Ezek előírásokat tartalmaznak mind a fejlesztés menetére, mind pedig az elkészült alkalmazás ellenőrzésére, verifikálására. Ahhoz, hogy a rendszer éles környezetben alkalmazásra kerülhessen, előbb tanúsítani kell; ehhez elő kell állítani az ún. biztonsági igazolást (safety case). Ez tartalmazza a rendszer biztonságos működésének indoklását: kezdve az alkalmazott fejlesztési folyamat általános leírásától, mely tartalmazza az elkészült részeket (pl. modelleket, kódokat, modulokat) és az ezekre végrehajtott ellenőrzési lépések eredményeit.

A költséges tanúsítási folyamatot hatékonyan tudja támogatni egy olyan keretrendszer, mely támogatja a szabványok által leírt követelmények leírását, ez ezekre épülő biztonságigazolási tervek modellezését, az ilyen tervekben meghatározott fejlesztési és verifikációs folyamatok (fél)automatikus végrehajtását, a végrehajtás során előállt részek (modellek, kódok, eredmények stb.) és a közöttük lévő kapcsolatok tárolását és végül ezek alapján a biztonsági igazolás előállítását. Az egyes részfeladatok elvégzésére többnyire elérhetőek különböző eszközök, de ezek egymástól független megoldások, a mi céljainknak nem felelnek meg, integrált felhasználásukra jelenleg nincs, vagy csak korlátozott lehetőség adódik.

A kitűzött feladatok:

- a biztonságkritikus rendszerek fejlesztésére vonatkozó szabványok, a tanúsításhoz szükséges biztonsági igazolások felépítésének, a verifikációs folyamatok szerepének a biztonsági igazolások elkészítésében és az ezek leírására használható modelleknek és eszközöknek az áttekintése,
- a fentiekben felvázolt tanúsítást támogató keretrendszer alapjául szolgáló komponensek megtervezése és elkészítése, melyek lehetőséget biztosítanak a követelmények, biztonságigazolási tervek és verifikációs folyamatok leírására, valamint támogatják egy konkrét rendszer fejlesztése esetén az egyes lépések eredményeinek tárolását és ezek alapján a biztonsági igazolás generálását,
- a rendszer működésének egy egyszerű mintapéldán keresztüli demonstrálása.

Ebben a félévben befejeztem a leendő keretrendszer (korábbi munkában elkezdett) egyik központi komponensének, a folyamat végrehajtó rendszerhez tartozó grafikus szerkesztőnek a megvalósítását. Ennek segítségével fogunk automatizáltan végrehajtható verifikációs terveket és a tanúsítási folyamatot összeállítani.

Sor került a keretrendszer magas szintű specifikálására, az alapvető modellek, architektúrális részletek meghatározására. Az irodalomkutatás kiterjedt a tanúsításhoz szükséges biztonsági igazolások felépítésének és ipari szabványok a megismerésére, így elkezdődhet a hiányzó komponensek implementációja.