MELLÉKLET

Jelentéskészítés támogatása biztonságkritikus beágyazott rendszerek integrált biztonságigazolás alapú megfelelőségminősítési folyamataiban

Azon dokumentumok együttesét, amelyek bizonyítják, hogy egy adott rendszer vagy termék elegendően biztonságos ahhoz, hogy egy megfelelő környezetben használatba vehessék, biztonságigazolásnak hívják (angolul: safety case). Több biztonsággal kapcsolatos szabvány is – különösen a közlekedéssel, nukleáris technikával vagy más, biztonságkritikus rendszereket gyakran alkalmazó iparágakkal kapcsolatos szabványok – előírja, hogy az alkalmazott ellenőrzési folyamat eredményeit ezen biztonságigazolások valamilyen formájával kell dokumentálni.

A biztonságkritikus rendszerek fejlesztéséhez speciális validációs és verifikációs (teszt támogató) eszközökre van szükség. Ezek mintegy mellesleg hatalmas mennyiségű olyan adatot is gyűjtenek, amelyek igen jól használhatóak a biztonságigazolások elkészítésénél. A jelentéstámogatás alkalmazásával a fejlesztők megszabhatják, hogy a felépített keretrendszer milyen formátumú dokumentációt készítsen a teszt eszközök által összegyűjtött adatokból.

Az EU egyik nagyméretű kutatási projektje (DECOS – Dependable Embedded Components and Systems) a beágyazott alkalmazások életciklus költségének csökkentését és megbízhatóságának növelését tűzte ki célul egy integrált beágyazott rendszer architektúra kifejlesztésével. Ezen projekt keretében a validáció és verifikáció támogatására elkészítettek egy DOORS (a svéd Telelogic AB követelmény menedzselő rendszere) alapú teszt keretrendszert (test bench), amely a teljes életciklust lefedi a platformfüggetlen modellektől a DECOS alapú alkalmazás telepítéséig, és egy moduláris, inkrementális megközelítéssel lehetőséget teremt ezen alkalmazások minősítésére is.

A diplomamunka célja az elkészült teszt keretrendszer kiegészítése jelentéstámogatással, különös tekintettel a biztonságigazolások készítésére, az alkalmazott validációs eljárás és folyamat dokumentálására a követelmények összegyűjtésétől a validációs tervek kidolgozásáig valamint a V&V tevékenységek végrehajtására, összegyűjtésére és kiértékelésére. A jelentések generálásának két egymástól függetlenül konfigurálható lépésre kell válnia: (1) a tartalom és a struktúra kinyerése az adattárból és (2) a kívánt (sablonokkal megadható) prezentációs formátumba való transzformálás. A kidolgozott rendszernek támogatnia kell az adattárból kinyert aggregált tartalom grafikus megjelenítését – pl. a tesztek teljesítésének foka a követelményekhez és a validációs tervekhez mérve – és a meglévő eszközök adatforrásként való használatát (felhasználó oldali teljesség ellenőrzés, hiányzó V&V tevékenységek azonosítása, ...).

A jelölt feladatai:

1. Biztonságigazolások alkalmazásának áttekintése biztonságkritikus rendszerek esetében, különös tekintettel a DECOS-ban alkalmazott megfelelőségminősítési folyamatokra.
2. Egy általános jelentéstámogató rendszer megtervezése, amely alkalmas biztonságigazolások készítésére.
   a. A külső konzulenssel egyeztetve gyűjtse össze és dokumentálja a rendszerrel kapcsolatos részletes követelményeket. Ehhez gyűjtsön információt a rendszer leendő felhasználóitól is.
   b. Vizsgálja meg a területen alkalmazható létező eszközöket és lehetséges architektúrákat.
   c. Válassza ki a megfelelő architektúrát és technológiát, a felhasználandó eszközöket, és dokumentálja döntéseit.
3. A teljes rendszer használhatóságának demonstrálása gyakorlati példákon.

Huszerl Gábor

adjunktus