Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék

Formális protokoll elemzés ProSigma biztonságkritikus rendszerhez

Pogonyi Ádám(FWRE53), I. évf, (MSc) villamosmérnök hallgató
Konzulens: Majzik István, MIT
Beágyazott információs rendszerek szakirány
Önálló laboratórium 2 összefoglaló

Biztonságkritikus szoftverek fejlesztése során használatos szabványokban ajánlott, vagy különösen ajánlott formális módszerek alkalmazása. A modellezésen alapuló formális elemzés különösen jól használható protokollok esetében. A modellek segítségével elméletben verifikálható a protokoll helyes működése, illetve hibái felderíthetők.

A Prolan Irányítástechnikai Zrt. által fejlesztett biztonsági jelátviteli rendszer (fantázia nevén ProSigma) belső IO egységek bővítő, kommunikációs buszának (IOCAN) helyessége alapvető fontosságú. Önálló laboratórium 2 tárgyban a ProSigma rendszeren belüli IOCAN protokoll formális modellezésével és alapvető verifikációjával foglalkoztam. Az IOCAN protokoll viszonylag egyszerű protokoll, mégis 100-200 követelmény vonatkozik rá. Ezen követelmények ellenőrzéséhez manuálisan teszteket készíteni nyilvánvaló nehézséget jelent. Törekvés, tehát hogy ezen tesztelés a lehető legnagyobb mértékben automatikus legyen. A munka motivációja, hogy ezt az automatikus teszteset generálást és tesztelést támogassuk.

A modellezéshez időzített automatákat használtam, mivel ezek jól illeszkednek a valós idejű protokollhoz, használatukkal kényelmesen kezelhetők a protokoll időzítésekkel kapcsolatos részei. Konkrét modellezési eszköznek az UPPAAL programot használtam. Elkészítettem az IOCAN protokoll alapvető funkcióinak modelljét és az elkészült modelleken verifikációs lekérdezésket hajtottam végre. A verifikációs lekérdezések lényegében a protokollra vonatkozó követelmények formalizált változatai, amiknek kielégülését az UPPAAL verifier segítségével vizsgáltam. A modellek nem térnek ki minden speciális esetre és követelményre, de ezen alap modellkészletből kiindulva kevés módosítással illetve bővítéssel ezek is lefedhetők.

A félév során elkészült formális modellek az IOCAN protokoll verifikációjára használhatók, azonban az elkészült modellek és verifikációs esetek segítségével lehetőség nyílik konkrét tesztesetek teszt-szekvenciák automatizált generálására. Így az egységek, illetve a rendszer tesztelési, verifikációs folyamatával járó nehézségek valamelyest csökkenthetők.