Misszókritikus beágyazott rendszerek hibatűrő felépítése

MSC Önálló laboratórium 2 feladat összefoglalója

Varga Tibor (WOBMWJ)
Konzulens: Bartha Tamás
BME Méréstechnika és Információs Rendszerek Tanszék
Szolgáltatásbiztos rendszertervezés ágazat, 2009/2010. II. félév

Az önálló labort a **misszókritikus beágyazott rendszerek** témájában végeztem. Az általam vizsgált konkrét rendszer egy a SZTAKI tulajdonában lévő **autonóm modellrepülőgép**, mely rendelkezik fedélzeti számítógéppel, emellett **olcsó és alacsony megbízhatóságú modellező elemekből** épül fel. Ezzel kapcsolatban vizsgáltam, hogy milyen meghibásodások léphetnek fel, milyen következményekkel jár egy hiba. A cél annak feltárása, hogyan tehető megbízhatóvá ez a rendszer, és ez által milyen szintű megbízhatóságot érhetünk el. A kutatás **motivációját** egy konkrét katonai-célpontrepülőgép project adta, ahol a repülő megbízhatósági szintjéről nem volt garantálható semmiféle konkrét értékelés. Tehát a modellrepülőgépen elvégzett elemzés tapasztalatai, módszerei, esetleg eredményei **kiterjeszthetőek** lennének egy ilyen, komolyabb projectre is.

Az előző féléves munka eredménye egy FMEA jellegű elemzés lett a SZTAKI-nál fejlesztett modellrepülőgép lehetséges hibamódjai alapján, mely kiindulási alapként szolgált a további megbízhatósági elemzésekhez.

Az aktuális féléves munkában először a kapott és a teljes összefoglalóban hivatkozott dokumentumok alapján megvizsgáltam a **repülőgép iparban használatos hibatűrési megoldásokat**. Alapvető a Fly-by-wire technika használata, melynek lényege, hogy a repülőgép vezérlése tisztán elektronikus úton, mechanikai segédberendezések nélkül történik. Ipari megoldásokra példaként foglalkoztam a Boeing 777 és az Airbus A3x0 széria több tagjánál használt hibatűrő repülésirányítási rendszerrel.

Ezek után a SZTAKI-nál tervben lévő újabb, két motoros modellrepülőgéphez alkalmazható különböző architektúrákat vizsgáltam **hibafa alapú analízissel**. A hibafa analízis egy felülről-lefelé irányú megközelítés, a rendszer szintű hiba valószínűségének kiszámolására a komponens hibák OR(vagy) és AND(és) alapú kombinálásával. A hibafa modellezéséhez több szoftvert is kipróbáltam, főként demó verziósakat, melyek végül nem bizonyultak megfelelőnek: Risk spectrum, Cara, ISOGraph FaultTree++, Relex, RAM commander, Sharpe. Végül az **OpenFTA** nevű ingyenes szoftvert használtam a feladatra.

Az OpenFTA használatával hibafákat készítettem a Bauer Péter által tervezett **szimpla** és **duplázott** CAN hálózatot használó architektúrát, ebből szimulációt futtatva nyertem valószínűségi értékeket az egyes - rendszer szintű hibához vezető - komponens hiba kombinációkhoz. A kapott értékeket figyelembe véve elkészítettem egy **javított architektúrát**, ahol az akkumulátorok elemzéshez használt megbízhatósági értékét is növeltem, megelőző karbantartás javasolása folytán. Az így összeállított rendszerben a hibavalószínűséget leginkább befolyásoló tényező az egyes motorokhoz tartozó vezérlőegység lett, melyeknek redundáns felépítése nem célszerű, így ezzel nem fokozható annak megbízhatósága.

A **munka folytatásaként** a CAN hálózat vizsgálata és kiépítése lett célul kitűzve, melyhez szükséges lesz a megfelelő protokollok implementálása, a hibadetektálás és megelőző hibadetektálás megoldása. A végcél a megtervezett rendszer kivitelezése a projecten dolgozó további fejlesztőkkel együttműködve.