Kivonat

Az elmúlt évek során az informatikai és a biztonságkritikus rendszerek komplexitása rohamosan növekedett: például egy Airbus A380-as repülőgépen is több millió sornyi kód felelős az utasok biztonságáért. Az összetett rendszerek elvárt funkcionalitásának teljesítéséhez, a bonyolultságukból adódóan, elosztott működés szükséges, melynek megtervezése a hagyományos mérnöki módszerekkel csak nehezen lehetséges.

A problémának egy lehetséges megoldásaként az elmúlt években meghatározó paradigmává vált a modell alapú megközelítés. A metodika célja, hogy a rendszer elkészítése során már a korai fázisoktól, magasszintű modellekből kiindulva származtassuk a konfigurációt, dokumentációt és forráskódot is. Az előálló megoldások analízise és helyes működésének tesztelése a konvencionális módszerekkel jellemzően csak nagy erőforrás-ráfordítással lehetséges. Azonban a modellvezérelt megközelítés közvetlenül lehetőséget nyújt formális módszerek alkalmazására is, melyekkel a hibák a fejlesztés korai fázisában felfedezhetőek.

Dolgozatomban áttekintem a modellvezérelt rendszerfejlesztés módszertanát, ezen belül kiemelve az állapotgép alapú megközelítést támogató xtUML nyelvet. A nyelv alkalmazhatóságát egy elosztott vasút-irányítási biztonságkritikus demonstrátor esettanulmányon keresztül igazolom, melyben a biztonsági logikát modell alapon terveztem meg. Az elkészített modell helyességének matematikai precizitású bizonyításához formális modelleket származtattam, melyeken temporális logikai nyelven fogalmaztam meg követelményeket. A követelmények teljesülését egy iparilag releváns formális modellellenőrző keretrendszerben (UPPAAL) vizsgáltam.