HORVÁTH BENEDEK
mérnök informatikus
BSc, 7. félév

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar

KONNERTH RAIMUND ANDREAS
Mérnök informatikus
MSc, 1. félév

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar

MÁZLÓ ZSOLT
Mérnök-informatikus
BSc, 7. félév

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar

Témavezetők:
Vörös András
tudományos segédmunkatárs, BME VIK
Dr. Horváth Ákos
tudományos munkatárs, BME VIK
Jász Zoltán
külső munkatárs (rendszermérnök), Ericsson Magyarország Kft.

Elosztott biztonságkritikus rendszerek modellvezérelt fejlesztése

Felgyorsult világunkban akár észrevétlenül is körbevesznek minket biztonságkritikus rendszerek, melyekben lévő technológiai megoldások különböző veszélyeket jelentenek az emberéletekre vonatkozóan.

Ezen rendszerek komplexitása az elmúlt évek során rohamosan növekedett, pl. 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.

Ennek a problémának egy lehetséges megoldásaként az elmúlt években meghatározó paradigmává vált a modell alapú megközelítés az informatikai és közlekedés-irányítási területeken. A metodika célja, hogy a rendszer elkészítése során már a korai fázisoktól, magasszintű modellekből kiindulva, finomítási lépéseken keresztül származtassuk a konfigurációt, a dokumentációt és a 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.

Jelen dolgozat célja egy modellvezérelt fejlesztési alapokon nyugvó, elosztott biztonságkritikus rendszer tervezési és analízis-módszerének kidolgozása, majd ezt a metodikát állapotgép-alapú működés-leíró modellekből kiindulva egy iparilag releváns keretrendszerbe integrálni. A használt keretrendszer támogatja a különböző platformokra történő automatikus forráskód szintézist,

amellyel a céleszközre történő telepítés egyszerűsíthető. A modellek formális analízisét időzített automatákkal és temporális logikákkal valósítottuk meg.

Esettanulmányként egy elosztott vasútirányítási biztonságkritikus demonstrátor alkalmazáson keresztül mutatjuk be a módszert, amelynek keretében több csomópontból álló, összetett sínhálózatban történő közlekedés hibamentes működésének biztosítását végeztük. A demonstrátor komplexitását jól jelzi, hogy a szoftverarchitektúrán túl a különböző hardverelemek integrációját is meg kellett valósítanunk, így mind a vezérléshez szükséges elektronikát, mind a biztonságkritikus rendszer teljes hálózatát magunk valósítottuk meg.