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 nőtt, és az elvárt funkcionalitások kiszolgálása elosztott rendszereket igényel. A feladatok implementálásához nagyságrendekkel több forráskód szükséges: egy Airbus A380-as repülőgépen is több százmillió sornyi kód felelős az utasok biztonságáért.

Az előálló megoldások analízise és helyes működésének tesztelése a konvencionális módszerekkel jellemzően csak nagy erőforrás-ráfordítással lehetséges, így az elmúlt években meghatározó paradigmává vált a modell alapú megközelítés ezen a területen. Ennek 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. 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-módszerét kidolgozni, 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 demonstrátor alkalmazáson keresztül mutatjuk be a módszert, amelynek keretében egy elosztott vasútirányítási biztonságkritikus demonstrátort valósítottunk meg több csomópont részvételével, összetett sínhálózatban történő közlekedés hibamentes működésének felügyeletére. 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 implementáltuk.

Model-based development of distributed safety-critical software systems

As technology is rapidly evolving, more and more safety-critical systems surround us. These, mostly unnoticeable systems can even use technological solutions, which may pose different threats upon people's lives.

The complexity of such software systems has increased rapidly, which led to the appearance of distributed systems in order to fulfill the required functionalities with high efficiency. In the software development world, this resulted in an increase of several orders of magnitude in lines of source code. For example, on an Airbus A380 airplane several million lines of code are responsible for the safety of the passengers.

Testing and analyzing the correct behavior of such systems with the conventional approaches usually requires high amount of resources, therefore in the latest years the model-based approach became the dominant paradigm in this area. This approach aims to facilitate the derivation of the system's configuration settings, documentation and even code generation through automatic transformations from the early stages of the development, when only high-level design models are constructed. The model-driven approach also provides a direct opportunity to apply formal methods that allow the discovery of both design and behavioral errors in an early stage of development.

This study aims to develop a design- and analysis approach of a distributed safety-critical software system by using state machine-based behavioral models and to integrate this approach to an industrially relevant framework. The used framework supports automatic code synthesis to various platforms, thus simplifying the deployment on the target device. In the formal analysis of the models timed-automatons and temporal logics are used.

As a case study we present the approach through a demonstrator application, in which we developed a distributed safety-critical railway control system with multiple nodes and a complex network of tracks. The aim of the control system is to ensure a fault-free operation of the trains. The demonstrator clearly shows the complexity of even such small scale systems, because in addition to the software architecture, the integration of the different hardware components, the control electronics and the system's entire network also had to be implemented.