Kiterjesztett szimbolikus tranzíciós rendszerek: köztes nyelv mérnöki modellek formális verifikációjához

A modellvezérelt fejlesztési folyamatban a formális verifikáció korai visszacsatolást tud adni a fejlesztés alatt álló rendszerről. A formális módszerek gyakorlati alkalmazását azonban számos akadály hátráltatja. Egyrészt a mérnöki modellek általában magasabb szintű modellezési nyelveken vannak megfogalmazva, míg a formális módszerek alacsony szintű matematikai formalizmusokon képesek működni. Másrészt a verifikációs algoritmusok komoly erőforrásigénnyel rendelkeznek, főleg a komplexebb mérnöki modellek esetében. A Theta egy általános, konfigurálható verifikációs keretrendszer, ami ezeket a kihívásokat különböző alacsony szintű formalizmusok és hatékony, absztrakcióalapú algoritmusok segítségével igyekszik leküzdeni. A létező formalizmusok azonban általánosságban vagy túlságosan alacsony szintűek vagy túlságosan domén specifikusak a modellvezérelt fejlesztéshez.

Ebben a dolgozatban bemutatok egy új köztes formalizmust, a kiterjesztett szimbolikus tranzíciós rendszereket (eXtended Symbolic Transition System, XSTS). Az XSTS formalizmus magasabb szintű nyelvi elemeket, illetve egy szöveges reprezentációt kínál a mérnöki modellek könnyebb transzformációja érdekében. Ezek mellett tiszta és jól definiált szemantikával rendelkezik különböző absztrakt domének felett és alkalmazkodik a létező verifikációs algoritmusok interfészéhez. Továbbá XSTS specifikus algoritmikus kiegészítéseket és stratégiákat is megalkottam a teljesítmény javítása érdekében.

A munkám integrálásra került a Gamma modellező keretrendszerbe, lehetővé téve, hogy megközelítésemet ipari partnerek által biztosított valós példákon szisztematikusan kiértékeljem. Az eredmények rávilágítottak a különböző algoritmuskonfigurációk erősségeire és gyengeségeire, és igazolják az XSTS formalizmus alkalmazhatóságát és hatékonyságát.