発表概要

組込みシステムを対象とした線形ハイブリッドオートマトンのモデル検査器の開発と検証

冨坂 征平[1,a)]　柳瀬 龍[1,b)]　小野 祐貴[1,c)]　山根 智[1,d)]

2013年8月2日発表

組込みシステムには，その用途に合わせて満たすべき特性が存在し，組込みシステムが特性を満たしているかどうか検証を行う必要がある．この検証手法の 1 つとして，形式手法に基づいて自動検証するモデル検査法が用いられている．本論文では，新たに 1 階述語論理の限定記号消去処理を含むモデル検査器を開発し，CPU と DRP から構成される動的再構成可能システムの安全性に関する検証実験を行った結果について示す．このモデル検査器では，検証対象となる組込みシステムを線形ハイブリッドオートマトンによって仕様記述を行い，到達可能性解析を用いて検証する．到達可能性解析は，システムの安全性検証において有効な手法である．

Development of Model Checker of Linear Hybrid Automaton for Embedded Systems

Shohei Tomisaka[1,a)]　Ryo Yanase[1,b)]　Yuki Ono[1,c)]　Satoshi yamane[1,d)]

Presented: August 2, 2013

As embedded systems have properties, which must hold true, it is important to verify such properties. One of verification methods is model checking, which is automated verification method based formal methods. In this paper, we developed a new model checker including quantifier elimination of first order logic, and verified Dynamically Reconfigurable System which is composed of CPU and DRP by using our model checker. We specify the system by linear hybrid system, and verify whether safety properties are satisfiable in the system or not by reachability analysis. Reachability analysis is an effective verification method related to the safety properties of embedded systems.

[1] 金沢大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Kanazawa University, Kanazawa, Ishikawa 920–1192, Japan
[a)] stomisaka@csl.ec.t.kanazawa-u.ac.jp
[b)] ryanase@csl.ec.t.kanazawa-u.ac.jp
[c)] ono@csl.ec.t.kanazawa-u.ac.jp
[d)] syamane@is.t.kanazawa-u.ac.jp