Safety Verification Utilizing Model-based Development for Safety Critical Cyber-Physical Systems

石郷岡 祐[1]　Habib Saissi[2]　Thorsten Piper[2]　Stefan Winter[2]　Neeraj Suri[2]

概要：The application of cyber-physical systems (CPSs) in safety-critical application domain requires rigorous verification of their functional correctness and safety-relevant properties. We propose a practical verification process which enables to conduct safety verification of safety critical CPSs. The verification process consists of (a) a system model construction method, which generates a system model by combining software described in C and plant model code reused from model-based development, (b) a model transformation method, which transforms the plant models including differential algebraic equations (DAE) to approximate models without DAE to reduce verification complexity induced by DAE solver execution, (c) a model simplification framework, which enables the simplification of bond-graph plant models using domain-knowledge-based replacement of complex model components for further verification overhead reductions, and (d) a formal verification based on symbolic execution. We implemented the proposed methods and framework, and successfully applied the proposed verification process for safety verification of automotive brake control systems. The results of the study demonstrate that the verification detects a complex failure condition in a real-world brake control system from the generated system model and that the automated model transformations of the CPS models yield significant verification complexity reductions without impairing the ability to detect unsafe behavior.

本招待論文は，Journal of Information Processing に掲載されました「Safety Verification Utilizing Model-based Development for Safety Critical Cyber-Physical Systems」[1] についてご紹介いただくものです．

参考文献

[1] Ishigooka, T., Saissi, H., Piper, T., Winter, S. and Suri, N.: Safety Verification Utilizing Model-based Development for Safety Critical Cyber-Physical Systems, *Journal of Information Processing*, Vol. 25, pp. 797–810 (2017).

[1] 日立製作所
[2] Technical University of Darmstadt