発表概要

MWF/MNWFに基づくFTAとSpec Patternsによるモデル検査式の導出

加藤 淳[1,a)]　松本 充広[2]　春山 真一郎[1]

2012年3月15日発表

モデル検査を実施するにあたり，検査対象システムとして満たすべき性質（プロパティ）を検証する検査式を導出する必要がある．先行研究として，検査対象システムの望ましい事象や望ましくない事象を分解・詳細化することで，モデル検査の検査式を導出する手法が提案されている．しかし先行研究では事象を分解・詳細化するルールが明確化されていない．検査式の導出が実施者の経験やスキルに依存して行われる．その結果，検査式が検証すべき性質を十分に網羅しておらず，モデル検査において検証漏れが生じる可能性がある．本発表では Must Work Function（MWF）/Must Not Work Fnction（MNWF）に基づく Fault Tree Analysis（FTA）および非形式的なプロパティを時相論理式に変換する Spec Patterns を用いて，安全性プロパティを検証する検査式を導出する手法を提案する．提案手法では Computer-Based Control System（CBCS）安全要求で定義されているハザード要因「MWF の喪失」および「MNWF の起動」の 2 分岐で FT を作成する．CBCS 安全要求とは高い安全性が求められる国際宇宙ステーションのコンピュータシステムに適用される安全要求である．作成した FT の基本事象に対して Spec Patterns を適用する．それらによって安全性プロパティの検査式を導出する際に高い網羅性を確保する．また，本発表では産業事例に対する提案手法の適用結果を報告する．適用の結果から，従来の方法では見逃された検査式を提案手法により導出することが可能であることを確認する．

Derivation of Formulae for Model Checking by MWF/MNWF-based FTA and Spec Patterns

Atsushi Katoh[1,a)]　Michihiro Matsumoto[2]　Shinichiro Haruyama[1]

Presented: March 15, 2012

When we conduct model checking to verify properties of a system, it is necessary to derive formulae of the properties. Some related works have proposed how to derive formulae, and with those method formulae can be developed by decomposing and refining the desired / undesired events for the target system. However, those related works don't define rules under which the events can be decomposed and refined. Therefore, conductors of model checking have to derive formulae dependent on their experiences and skills. As a result, there are some possibilities that the verification by model checking is not adequate because the formulae don't sufficiently cover the properties which should be verified. In this report, a method using Must Work Function (MWF) / Must Not Work Function (MNWF)-based Fault Tree Analysis (FTA) and Spec Patterns is proposed. The proposed method derives formulae for verifying safety properties by using MWF / MNWF-based FTA and Spec Patterns, a tool which can translate informal properties into formulae in temporal logic. In the proposed method, fault trees are constructed according to the dichotomy of "Loss of MWF" and "Activation of MNWF", both of which are defined as hazard causes in the Computer-Based Control System (CBCS) Safety Requirements. The CBCS Safety Requirements are applied to the computer systems in International Space Station to secure the high safety. Spec Patterns are used to the preliminary events in the constructed fault trees. With MWF / MNWF-based FTA and Spec Patterns, high comprehensiveness is secured in deriving formulae for safety properties. In this report, application results of the proposed method to an industrial case are also presented. As a result, it is confirmed that the proposed method can derive formulae which have been overlooked by the former methods.

[1] 慶應義塾大学大学院システムデザイン・マネジメント研究科
Graduate School of System Design and Management, Keio University, Yokohama, Kanagawa 223–8526, Japan
[2] 有人宇宙システム株式会社
Japan Manned Space Systems Corporation, Chiyoda, Tokyo 100–0004 Japan
[a)] katoh.atsushi@z7.keio.jp