Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 12, December 2013, pg.26 – 39

RESEARCH ARTICLE

Model Checking of Safety Properties for Complex Systems Using MWF Inactivation and MNWF Activation

Atsushi Katoh[1], Shinichiro Haruyama[2], Naohiko Kohtake[3], Yoshiaki Ohkami[4]

Graduate School of System Design and Management, Keio University
[1] katoh.atsushi@z7.keio.jp; [2] haruyama@sdm.keio.ac.jp; [3] kohtake@sdm.keio.ac.jp; [4] ohkami@sdm.keio.ac.jp

Abstract— One of the aims of model checking is to confirm a system's safety properties. Safety properties state that undesirable events never occur. This paper describes a method that derives comprehensive and rigorous safety properties for model checking. In general, an undesirable event in a system is abstract, and so safety properties corresponding to undesirable events cannot be directly applied to model checking. To be applicable to model checking, safety properties must be derived by interpreting undesirable events in a system using the system specifications. In the model checking of complex systems, some safety properties may be neglected or insufficiently specified because the functions and/or conditions in the systems are complex. The proposed method adopts the concepts of "Must Work Function (MWF) Inactivation" and "Must Not Work Function (MNWF) Activation" to solve these issues. Comprehensive and rigorous safety properties for model checking are derived according to these concepts. Undesirable events are embodied by rewriting knowledge according to the term rewriting system. The effectiveness of the proposed method is evaluated by applying it to a wireless rail crossing system. The results show that the derived safety properties offer a significantly improved degree of comprehensiveness and rigor.

Keywords— Model Checking; Safety Property; Must Work Function (MWF); Must Not Work Function (MNWF); Term Rewriting System

Full Text: http://www.ijcsmc.com/docs/papers/December2013/V2I12201307.pdf