Developing Reliable and Safe Software

Keishi OKAMOTO

Professor	okamoto@sendai-nct.ac.jp
Affiliated Societies	Japan Society for Software Science and Technology, The Mathematical Society of Japan

Keywords	Mathematical informatics-related (60020), Software-related (60050)

Research Topics

- Mathematical logic
- Formal methods
- STAMP/STPA

Research Seeds

1) Mathematical Logic

Mathematical logic is a background of formal methods. We develop logics for formal methods. Recently, we are developing a frame of well-formed requirement documents based on argumentation theory, which is an extension of mathematical logic.

Papers:

1. A Bayesian Approach to Argument-Based Reasoning for Attack Estimation, Hiroyuki Kido and Keishi Okamoto, August, 2017, Proc. Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17, pp.249–255

2. Balancing Between Cognitive and Semantic Acceptability of Arguments, Hiroyuki Kido and Keishi Okamoto, July, 2017, Knowledge Science, Engineering and Management: 10th International Conference, KSEM 2017, Melbourne, VIC, Australia, August 19-20, 2017, Proc. (Lecture Notes in Computer Science), pp.160-173

2) Formal Methods

Formal Methods are methods to develop software that is highly reliable, safe etc. We develop a translation tool from a specification language VDM++ to a programing language C#. We also give models that are first-order descriptions to verify refinement relations.

3) STAMP/STPA

STAMP is a novel accident model developed by Nancy G. Leveson. STPA is a hazard analysis method based on STAMP. We explore case studies to promote STAMP/STPA in Japan, and propose extensions of STAMP/STPA.

Papers:

3. はじめてのSTAMP/STPA(実践編), IPA/SEC, May, 2017, ISBN 978-4-905318-51-4, Information-technology Promotion Agency, Japan(IPA)

4. はじめての STAMP/STPA, IPA/SEC, April, 2016, Information-technology Promotion Agency, Japan(IPA)

Related Technology