The 3rd STAMP Workshop in Japan

Title

Collaboration between STAMP/STPA and model checking

- Based on STAMP analysis example “Fallen Barrier Trap at Railroad Crossing”-

Speaker, Authors

Shinshu University Kozo Okano, Shinpei Ogata, Pan Yang, Rin Karashima

Abstract

Recent information systems become large and complex. Thus, the demand for research on accident cause analysis and countermeasure construction of the information systems is increasing. Systems Theoretic Accident Model and Processes (STAMP) has features that can analyze errors of interaction between constituent elements, constituent elements and human beings, as well as troubles of system components and human error. STAMP based Process Analysis (STPA) analyzes in advance the possibility of system accident against the interaction between the controller and the controller. Although STAMP / SPTA does not consider cooperation with formal method, more effective accident analysis can be expected by cooperation of model checking based on the formal method. In this paper, we consider the method of cooperation with the model checker UPPAAL for time automata with the STAMP analysis example “Fallen Barrier Trap at Railroad Crossing.” In particular, we consider the possibility of application of mathematical programming for the derivation of the range of time variables. In addition, the results of actual analysis using UPPAAL will also be described. Based on the above results, we also consider how to link a STAMP / STPA tool, STAMPWorkbench, and the model checker.

Keywords

(1) STAMP/STPA

(2) Timed Automata

(3) Model Checking

(4) Mathematical programming

(5) Fallen Barrier Trap at Railroad Crossing