

The 3rd STAMP Workshop in Japan

Title

Introducing a Tree Structure to a Scenario Derived in STPA Analysis

Speaker, Authors

Hitachi, Ltd. Hiroshi Mine, Wakana Takeshita

Abstract

We propose the introduction of a tree structure to a scenario derived in STPA analysis. Usually, in STPA analysis, a scenario is written by using only a natural language or a table in which a horizontal axis is hint-words and a vertical axis is UCAs. However, in such a way, one scenario is written as one sentence. Therefore, it is difficult to re-use a part of a scenario in another analysis. Also, since existing ways to write a scenario depend on an analyzer, it is difficult to check the completeness of a scenario and to review the scenario from others. In this presentation, we propose the introduction of a tree structure to a scenario. This proposed tree structure is very similar to FTA. This proposed tree structure is composed of some nodes, some gates and some edges. Since one scenario can be written by deriving some nodes, a part of a scenario can be re-used in another analysis. Also, by one node corresponding to one hint-word or one control action, a reviewer can check an analysis status easily. We tried this proposal on an autonomous driving system and checked that we can write a scenario by a tree-structure, re-use a part of tree in an analysis of different UCA in same system and check the analyzed hint-word easily.

Keywords

- (1) STPA
- (2) Loss Scenario
- (3) Tree-structure