(10) Title

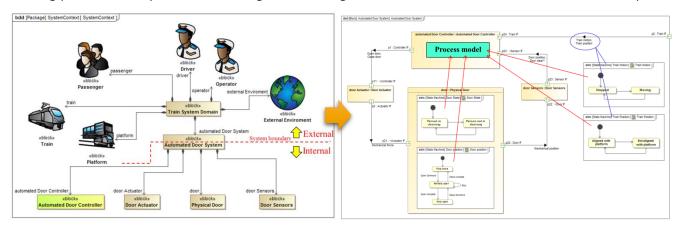
STAMP/STPA with using system model

Speaker, Authors

Hitachi Industry & Control Solutions, Ltd. Takeo Hashimoto

Abstract

STAMP/STPA is said that it can be used for analyzing not only the system malfunction but also the cause of accidents which were caused from the interaction between the components such as multiple systems, humans, and environments. One of the differences between STAMP/STPA approach and conventional safety analysis approaches is that STAMP/STPA approach can be used for safety analyzing even at a concept design phase (before defining system elements). STAMP/STPA also has an aspect of as a method to generate ideas easily, we could get the variety of analysis results depend on analysts. But without the analysis process, it is difficult to judge the coverage and validity of the analysis result. Therefore we think visualizing and recording the thinking process of analysis are a key solution for this issue, and we introduce the STAMP/STPA trial result with specific examples by using system models which were made by system engineering approach. We used international standard SysML (Systems Modeling Language, ISO/IEC 19514:2017) to visualize "Control structure "and "analysis process". For example, we made "Control structure(right figure)" depend on the analysis result of "System context(left figure)", "Sequence diagram", and so on. (Not shown all process) Visualizing the thinking process of analysis enables us to get new findings such as the lack of actors or new consideration points.



Keywords

- (1) Systems Engineering
- (2) Unexpcted event
- (3) Visualizing the analysing process
- (4) SysML
- (5) Traceability