The 3rd STAMP Workshop in Japan

Title

A Proposal to Use a Hazard Log Tool in Conjunction with STAMP/STPA

Speaker, Authors

Kyosan Electric Manufacturing Co.,Ltd.　MASATO　SAKAI / TETSUYA　TAKATA

Abstract

STAMP and STPA can analyze causes of accidents that may stem from the overall system design or a discrepancy in interfaces between components based on how relevant interfaces behave when a software module fails. In this regard, comparing with conventional accident models such as FTA and FMEA that have a difficulty in finding accident causes, STAMP and STPA can perform more credible analyses.

The analysis procedure using STAMP and STPA is unambiguous, which thus facilitates the analysis process. Moreover, even beginners can start a safety analysis according to the STAMP theory if they use a modeling tool and follow the guidance provided by the tool.

Nevertheless, STAMP and STPA have a shortcoming in that, although they can completely identify unsafe control actions that may cause hazards, they cannot distinguish between impossible actions and possible actions to be watched carefully. For that reason, the complete identification of those actions by STAMP and STPA, if combined with a risk-based design method, is considered effective in demonstrating that a target system has been established safely.

This presentation shows how to identify the risk of hazards within a system according to defined accidents systematically based on the risk analysis specified in IEC 62278 as the third phase of a RAMS lifecycle as well as completely by means of STAMP and STPA, take countermeasures against the risk and reduce the risk to an acceptable level.

Furthermore, this presentation proposes the use of a hazard log tool that has different characteristics from other modeling tools by focusing on and recording identified hazards. The hazard log can be updated as the risk of each hazard is reduced synchronously with the progress of the design, ensure the traceability of hazards and transparency of the risk reduction process and serve as primary evidence to validate and justify the techniques used.

The hazard log proposed in this presentation is created based on the concept of hazard management method, on the assumption that it will be used for an actual risk analysis for the purpose of a safety audit.

Keywords

(1)　STAMP／STPA

(2)　electronic interlocking systems

(3)　RAMS（IEC62278）

(4)　modeling tools

(5)　Hazard Log Tool