(5) Title

Using STAMP/STPA focusing on "freedom from interference"

Speaker, Authors

University of Nagasaki, Shigeru Kusakabe

Abstract

In the software architecture field, there exists a claim that proper usage of "views and perspectives" is useful in describing and analyzing architecture. Likewise, the author proposes usage of some useful phases to facilitate better application of STAMP/STPA. The author considers FFI, "Freedom From Interference" is one of such a useful phase. FFI is mentioned in ISO 26262, Part 1, Definition 1.49, as "Absence of cascading failures between two or more elements that could lead to the violation of a safety requirement". While FFI is strongly related to partitioning in an ISO 26262 context, the phase can be useful in more general context. For example, we can correlate the description and analysis of EMV2 (Error Model annex version 2) for AADL(Architecture Analysis & Design Language) with the modeling and analysis of STAMP/STPA. Moreover, the we facilitate modeling and analysis of more general cases such as a case of project management with the phrase in STAMP/STPA.

Keywords

- (1) Freedom from interference
- (2) Architecute description and analysis
- (3) Perspective
- (4) ISO26262