

Presentation Abstract

Presentation Title	Modeling and Hazard Analysis using STPA
Author(s)	Takuto Ishimatsu
Point of Contact (POC)	Phil Loftis
POC E-mail	Philip.D.Loftis@nasa.gov
POC Fax	304.367.2035
Presentation Abstract	<p>A joint research project between MIT and JAXA/JAMSS is investigating the application of a new hazard analysis to the system and software in the JAXA H-II Transfer Vehicle (HTV). Traditional hazard analysis focuses on component failures but software does not fail in this way. Software most often contributes to accidents by commanding the spacecraft into an unsafe state (e.g., turning off the descent engines prematurely) or by not issuing required commands. That makes the standard hazard analysis techniques of limited usefulness on software-intensive systems, which describes most spacecraft built today.</p> <p>STPA is a new STAMP-based hazard analysis technique based on systems theory. The goal of STPA, which is to create a set of scenarios that can lead to a hazard, is the same as FTA but STPA includes a broader set of potential scenarios including those in which no failures occur but the problems arise due to unsafe and unintended interactions among the system components.</p> <p>This presentation explains the experimental application of STPA to the JAXA HTV in order to determine the feasibility and usefulness of the new hazard analysis technique. Because the HTV was originally developed using fault tree analysis and following the NASA standards for safety-critical systems, the results of our experimental application of STPA can be compared with these more traditional safety engineering approaches in terms of the problems identified and the resources required to use it.</p>