The 3rd STAMP Workshop in Japan

Title

Application of STAMP/STPA to Automatic Control System in Safety Analysis

Speaker, Authors

Japan Manned Space Systems Corporation　Yasutaka Michiura

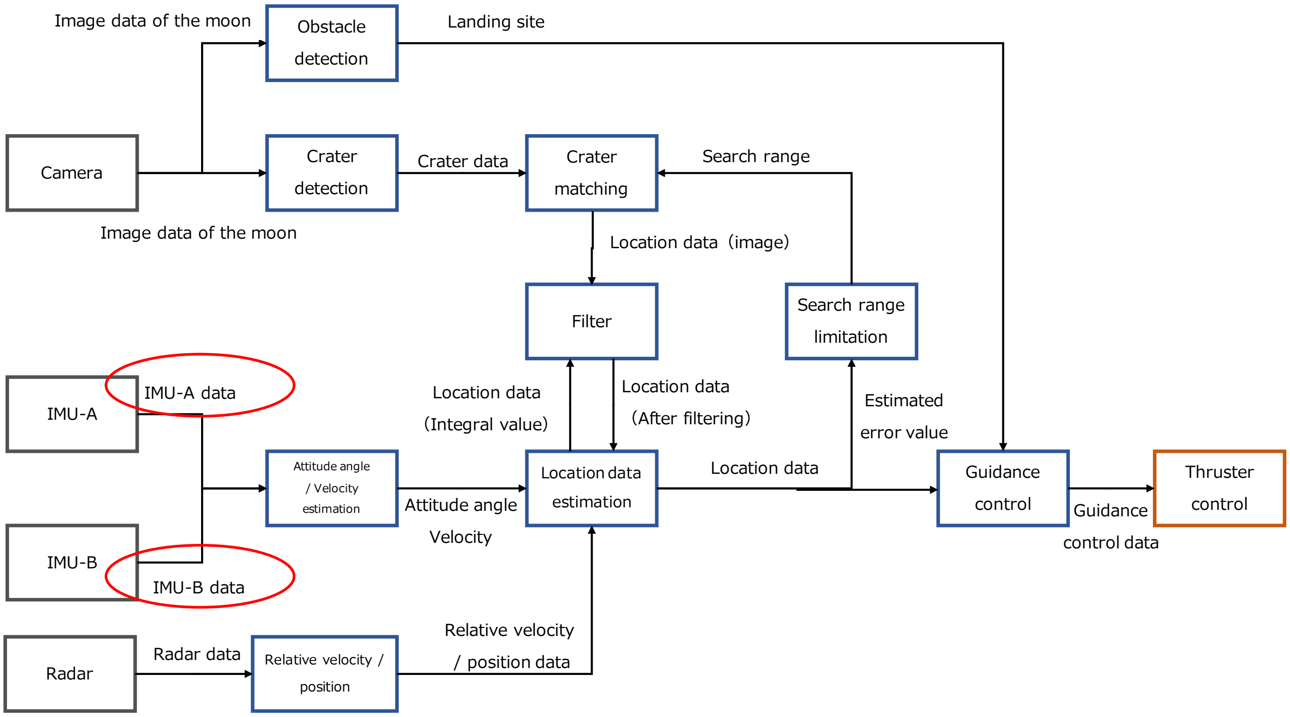
Abstract

In recent years, Systems such as spacecraft / aircraft / automobile are characterized by large scale, complexity, and automatic control. There are several problems when analyzing such a system using STAMP/STPA. In this presentation, we introduce the problem of STAMP/STPA analysis and its solution.

■Issue 1: Blind spot of four guide word analysis

In Step 1, four guide words are applied for each Control Action (CA) to identify Unsafe Control Action (UCA). However, when analyzing a complicated system such as an automatic control system, there is a hazard scenario that can not be identified if it is only analyzed using a guide word for each CA.

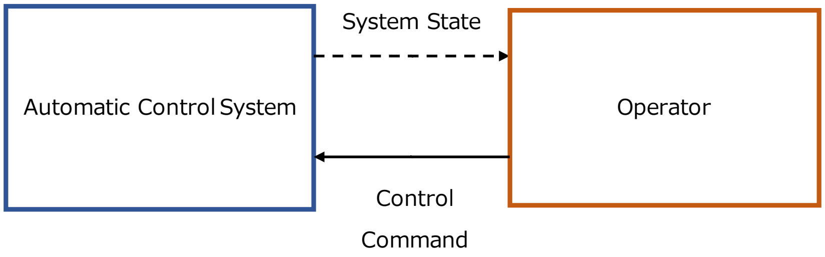
For example, in the case of Control Structure as shown below, even if one of the IMU-A data / IMU-B data is not provided, the hazard is not reached. Because the functions are redundant, it is designed to be compatible as a system even if one CA is not provided. However, if both CAs are not provided, the function is not established and leads to a hazard. Therefore, it is necessary to analyze the behavior of multiple CAs.



■Issue 2: Identify Control Action that does not exist

In the case of the automatic control system, the intervention of the operator is unnecessary at the time of normal operation, but there is a case that the intervention of the operator is required when a fail occurs. In such a case, in order to operate the system, it is necessary to know the state of the automatic control system.

For example, in Step 1, it is possible to analyze the situation where CA is not provided. However, as shown in the figure below, it is impossible to analyze by guide word when there is no CA (system state).



In order to solve issue 1 and 2, it is necessary to not only analyze individual CAs but also to grasp the feature of the system from the Control Structure and to identify hazard scenarios.

Keywords

(1) STAMP/STPA

(2) Automatic control system

(3) Human-machine system

(4) Hazard analysis

(5) Spacecraft