Paper ID: 47232
student

IAF SPACE SYSTEMS SYMPOSIUM (D1)
Space Systems Engineering - Methods, Processes and Tools (2) (4B)

Author: Mr. Konstantinos Konstantinidis
Universität der Bundeswehr München, Germany

Mr. Philipp Malessa
Bundeswehr University Munich, Germany
Prof.Dr. Roger Förstner
Universität der Bundeswehr München, Germany

SAFETY GUIDED DESIGN OF A GN&C SYSTEM FOR SAFE AND PRECISE LANDING NEAR A PLUME SOURCE ON ENCELADUS, BASED ON SYSTEMS-THEORETIC PROCESS ANALYSIS (STPA)

Abstract

A persistent problem with planetary landers has been ensuring adequate landing reliability. Future landing missions in particular will target scientifically interesting areas that are however surrounded by very challenging terrains.

One example of such a challenging landing is on Enceladus, a promising hot spot for astrobiology in the solar system. A spacecraft landing near one of the plume sources in the bottom of one of the "tiger stripe" canyons on the south pole of Enceladus and deploying an ice melting probe to sample relatively shallow liquid water, would be able to look for signatures of life before they are degraded by exposure to the vacuum of space. The lander would have to meet very challenging landing accuracy and safety requirements on an exceptionally challenging terrain. The unprecedented planetary protection requirements in the vicinity of the plumes, mean that landing reliability will be a driving requirement for this mission. To perform this challenging landing, a GN&C system is necessary, implementing three main complex and software-intensive functions: terrain relative navigation (TRN), hazard detection and avoidance (HDA) and landing guidance.

A method to assist in the reliable and safe design of such a complex system would be highly desirable. Several fault management methods have been applied in aerospace in the past few decades (FTA, FMEA, etc) but they have difficulty dealing with complex, software-heavy systems such as the landing GNC discussed above.

In this paper, we describe the application of the novel Systems-Theoretic Process Analysis (STPA), a hazard analysis methodology based on a new model of accident causation called Systems-Theoretic Accident Model and Processes (STAMP), for the safety guided design of the landing GN&C system for landing on Enceladus. Analysing the GN&C system using the STPA process from the earliest conceptual phase, we first identify and try to eliminate hazards. For hazards that cannot be eliminated, we identify the potential for their control at a system level. We then create a control structure to enforce the corresponding safety constraints. We iterate this process until all hazardous scenarios are eliminated, mitigated, or controlled. The final result is a GNC system design that takes into consideration safety and reliabilty from it's earliest phases.