Paper ID: 15202
oral
student

SPACE SYSTEMS SYMPOSIUM (D1)
System Engineering Tools, Processes and Training (1) (3)

Author: Mr. Kohei TANAKA
Keio University, Japan, k.tanaka@z3.keio.jp

Dr. Yutaka Matsuno
University of Tokyo, Japan, yutaka.matsuno@me.com
Dr. Yoshihiro Nakabo
National Institute of Advanced Industrial Science of Technology (AIST), Japan,
nakabo-yoshihiro@aist.go.jp
Prof. Seiko Shirasaka
Keio University, Japan, shirasaka@sdm.keio.ac.jp
Prof. Shinichi Nakasuka
University of Tokyo, Japan, nakasuka@space.t.u-tokyo.ac.jp

TOWARD STRATEGIC DEVELOPMENT OF HODOYOSHI MICROSATELLITE USING ASSURANCE CASES

Abstract

This paper introduces initial results of adopting assurance cases to the development of Hodoyoshi satellite.

As the technology of satellite has been highly advanced, it has become difficult to assure dependability of a satellite system. Currently, dependability of satellite system is mainly supported by various risk analysis and verification results. However, due to time and cost constraints, management of risk analysis and verification has been done in an ad-hoc manner. Therefore, it is difficult to assure why such analysis and verification result are required for the dependability in some cases.

An assurance case is a documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment. Assurance cases are written in a top-down manner to argue the top goal about dependability of the system. In Europe, assurance cases are widely used as regulation in safety-critical areas. Assurance cases are often written in a graphical notation to ease the difficulty of writing and certifying them. GSN (Goal Structuring Notation) is one of such notations. A characteristic of GSN is that when decomposing a goal, it is required to explicitly write the rationale for the decomposition.

We use GSN for a satellite project called “Hodoyoshi” project in Japan. Hodoyoshi means “reasonably reliable”. Reasonably reliable is a development approach which does NOT omit the necessary tests and verifications to be done on the ground before launch when dealing with mission failure risks, but reduces the workload needed to ensure successful system operation. To realize this concept, it is important to share and understand the reason why the analysis and/or verification is required to assure the system.

The purpose of adopting the assurance case is to design the satellite which doesn’t lose its function for two years. The arguments about the reliability of satellite have done by dividing into its lifecycle so that designers can recognize its aim and what they should validate in the phase.

There are three benefits. First, an assurance case helps to ensure a minimum number of criteria to develop a reliable satellite by using strategies of the assurance case from the other reliable satellites. Secondly, all project members can argue logically about the system reliability. From this, designers can fix the architecture of satellite early. At last, the project member can understand the critical points of design and the impact of design changes.