Abstract

Spacecraft system development faces new operational challenges, such as adapting to new mission concepts and supporting multi-spacecraft constellation operations that require greater autonomy and reduced workload. At the same time, high operational reliability is essential because repairs in space are extremely difficult. Therefore, engineers must share a common understanding of operations from the early development phase by defining and reviewing operational scenarios. However, scenarios represented by activity diagrams often become large and complex, especially when off-nominal states with many variations are included, making them difficult to review and increasing the risk of design inconsistencies and missing requirements.

This study aims to improve the reviewability of operational scenarios by (i) enabling compact representation of large scenarios in activity diagrams and (ii) enhancing review coverage through exhaustive enumeration of state transitions and execution paths for off-nominal scenarios derived from a single nominal scenario. These capabilities are realized within a model-based development framework using three proposed metamodels: the operational layer definition metamodel, the operational stereotype metamodel, and the operational abnormal event metamodel integrated with STAMP/STPA safety analysis.

In the compact representation method, behaviors that have low review value and are already commonly understood are defined as common behaviors using stereotypes. By applying these stereotypes to action elements in activity diagrams in an annotation-like manner, known behavioral portions can be omitted. Removing such action elements reduces the number of elements and achieves a more compact representation. As a result, diagrams can be generated without requiring scrolling, improving visibility, enabling an overall view of the scenario, and facilitating intuitive understanding and effective review of essential aspects. However, among the omitted information, elements necessary for review are preserved as tagged values. Furthermore, a method is included to verify stereotypes and tagged values from a review perspective, ensuring that all information required for review is retained.

For the generation of off-nominal scenarios, the nominal scenario is analyzed using STAMP/STPA, and the results are represented in a SysML model and integrated into the MBSE framework. To derive off-nominal scenarios from the nominal scenario, we propose the concept of a join point, inspired by aspect-oriented approaches. Join points are defined within the nominal scenario, and unexpected abnormal scenarios (e.g., unsafe control actions and unsafe scenarios) derived from STAMP/STPA analysis are inserted at these points. This enables branching from the nominal scenario to abnormal states, thereby generating off-nominal scenarios.

In addition, to comprehensively review transitions to unexpected abnormal states, execution paths are explored from a single scenario, and all possible state transitions are enumerated and represented as a graph. Execution paths are exhaustively enumerated using a SAT-solver-based approach. Inspired by the path exploration mechanism of bounded model checking, we implement a SAT-solver-based approach to enumerate feasible execution routes and state transitions, which we refer to as Bounded Search.

Experiments using representative JAXA spacecraft scenarios show that the compact representations reduce both the number of elements and the required screen area by approximately 50%, enabling activity diagrams to fit within approximately a single A4 page, thereby improving review visibility. Furthermore, off-nominal scenario analysis revealed previously unanticipated transitions, demonstrating that the proposed approach provides effective design feedback and contributes to improved spacecraft system reliability.

Keyword: Spacecraft operation; Model-based systems engineering; review; activity diagram; compaction; Bounded model checking; SAT solver