5B-07

宇宙機自動ドッキングシステムを対象としたMBSE手法と物理シミュレーションとを連携させた安全性分析・評価手法の提案

染谷　一徳†‡　和田　恵一†　河津　要†　青木 利晃‡

宇宙航空研究開発機構†　　北陸先端科学技術大学院大学‡

1. はじめに

有人宇宙活動・宇宙探査ミッションを担う宇宙機に必要とされる重要な機能の一つである自動ドッキングシステムは,国際宇宙ステーション（ISS）と宇宙機もしくは 2 機の宇宙機同士との間で、相対位置/速度/姿勢を精密に制御するランデブー,そして機械的な接触・反力を伴う状態でのドッキング機構の制御によって実現される.特に高い安全性[1]が求められるドッキングシステムにおいては,正常ケース（ノミナルシナリオ）に加えて,異常時のケース（オフノミナルシナリオ）の網羅的な検討が求められるとともに,定量的な評価として,物理的な接触・反力を伴う制御及び機体の挙動について物理シミュレーションによる解析評価が必要となる.

課題は,オフノミナルシナリオの識別と検証方法である.STAMP (Systems Theoretic Accident Model and Processes) などの安全解析ツールを用いて,オフノミナルシナリオの分析を行った.しかし,オフノミナルシナリオはバリエーションが多く,どれが重要かを識別し,開発チームメンバ間での合意形成が困難であった.また,そのオフノミナルシナリオがどの程度,安全なのかを定量的に評価するのも困難であった.

本論文では,開発チームメンバの間で重要なオフノミナルシナリオの合意形成を得るために,シナリオのモデル化による共通認識の形成,及びオフノミナルシナリオの定量的な評価・検証として物理シミュレーションとの連携方法の検討結果について説明する.

2. 提案手法

オフノミナルシナリオのモデル化,及びシミュレーションとの連携について,Model Based Systems Engineering（以下,MBSE）手法[2]を用いる. MBSE 適用効果として,システムの可視化による関係者間での共通認識の強化,及び Single Source of Truth の概念によるシステム設計とシミュレーションの連携における整合性の担保を狙う.オフノミナルシナリオのモデル化とシミュレーションとの連携のプロセスを図 1 に示す.

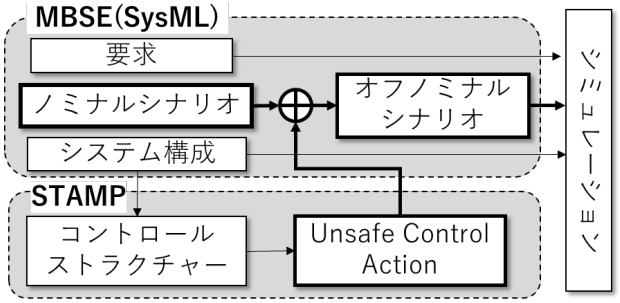

図 1　全体プロセス

オフノミナルシナリオのモデル化には,システムモデリング言語である SysML を用いて,アクティビティ図で作成する.モデル化手順は,まず正常であるノミナルシナリオをアクティビティ図で設計する.次に STAMP の解析結果の UCA(Unsafe Control Action)が,ノミナルシナリオ上のどこのインタフェースに該当するか対応付けを行う.最後に,UCA の内容に基づき,ノミナルからオフノミナルへ分岐を追加し,オフノミナルシナリオをノミナルシナリオの派生シナリオとして生成する.オフノミナルシナリオはノミナルシナリオを幹として,枝葉のように派生させ,議論の発散を防ぐ.物理シミュレーションとの連携においては,SysML で分類される要求,シナリオ,構造を対象にシミュレーション側のモデルと整合性を取る.要求はシミュレーション結果の要否判定に用い,構造はシステム構成とシミュレーションモデルの構造の整合,シナリオは検証ケースになる.

3. 試行と結果

3.1. オフノミナルシナリオのモデル化

アクティビティ図には縦割りの列（スイムレーン）を設け,シナリオ上の登場人物（アクター）を割り当てる.スイムレーンを跨ぐフローの線はアクター間のインタフェースと定義できる.STAMP のコントロールストラクチャーでも同様のアクターをコンポーネントとして配置することで,コンポーネント間のコントロールアクシ

Anomaly scenario modeling for safety analysis in the automatic docking system to the International Space Station

† Kazunori Someya, Keiichi Wada, Kaname Kawatsu, Japan Aerospace Exploration Agency

‡ Toshiaki Aoki, Japan Advanced Institute of Science and Technology

ョンが,アクティビティ図のアクター間のインタフェースと対応付けすることが出来る.これにより,STAMP の UCA が,ノミナルシナリオのアクティビティ図のどこのフローに対応するかが決定できる.オフノミナルシナリオは UCA に基づき,ノミナルシナリオからの分岐として表現することで、アクティビティ図でモデル化する.例えば,自動ドッキングシステムでは,UCA として,ISS に接触したことを検知する情報が遅延した場合に,ISS に衝突する非安全がある.まず,UCA とアクターを手掛かりに,対応する検知情報がインタフェースされる箇所をノミナルシナリオ上で特定する.そして,その箇所に分岐を追加し,遅延が発生した場合のシナリオを追記することで,オフノミナルシナリオを作成する（図 2）.

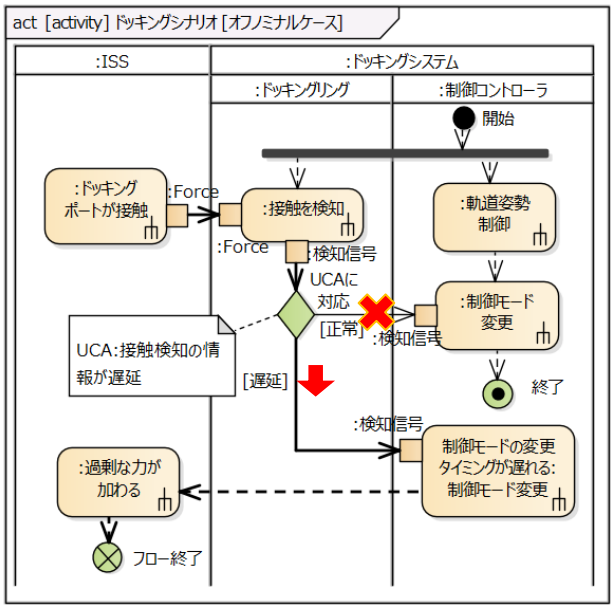

図 2　オフノミナルシナリオ

オフノミナルシナリオのモデル化により，開発プロジェクトからは,UCA の発生の前後など状況が理解しやすいとの評価が得られた.

しかし,UAC を発生させる原因は 1 つではなく,UCA に対応するオフノミナルシナリオも 1 つではない．今後の課題として UCA に対して FTA や FMEA を用いて原因特定し,シナリオの網羅性向上を図る.

3.2. 物理シミュレーションとの連携

オフノミナルシナリオに対する安全対策が十分かどうかの評価は,網羅的でかつ定量的な評価が求められる．3.1 項に示したアクティビティ図上では論理的な動きのみを表現するに留まるため,物理現象も含めた検証にはシミュレータが必要である.従来は,シミュレーション担当者が開発チームメンバからの依頼を受け,ドキュメントから必要な情報を読み取りモデルを構築し,実行したため,解釈齟齬や古いパラメータを組み込んでしまうなどの課題があった.そこで,MBSE の利点を生かして,システムモデルから物理シミュレーションと連携する方法を検討した.

シミュレーションでは,解析モデルを構築し,時系列に沿ったシナリオを評価することで,要求への充足を判断する.そこで,SysML の要求項目をシミュレーション側に提供し,要求の充足条件のトレースが取れるようにした.また,SysML の内部ブロック図によりシステムの構成要素と要素間の関係やデータのやり取りをブラックボックスとして定義,シミュレーション側は解析モデルとしてその内部ロジックをホワイトボックスのように記載することでトレースを取った．最後に,シミュレーション結果は SysML へ反映することで,MBSE 主導のシミュレーション環境構築が出来る.今回はデモ環境を構築し,共有データベースを介して,要求と構造の連携が可能であることを確認した（図 3）.

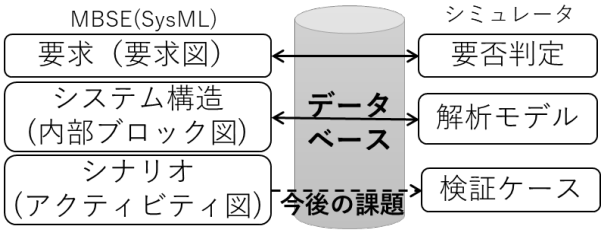

図 3　MBSE とシミュレーション連携

今後の課題は,振る舞いの連携であり,3.1 項で示したアクティビティ図用いて,ノミナル,オフノミナルシナリオに基づくシミュレーションの実行を行う.

4. まとめ

自動ドッキングシステムの開発に向けて,安全解析ツールと連携したオフノミナルシナリオのモデル化手法,及びシミュレーションとの連携に向けた取り組みについて紹介した.

参考文献

[1] 白坂成功 ,堀田成紀, 蒲原信治:階層化 FDIR による高安全性航法誘導制御系の提案と宇宙ステーション補給機「こうのとり」での実現, 計測自動制御学会産業論文集 Vol.10, pp91-99
[2] 染谷一徳, 舟生豊朗, 山田興人, 石濱直樹:運用設計を主体とするモデルベース開発技術,第 62 回宇宙科学連, 3H06