モデル検査を用いたFRAMモデルの解析

青木　善貴[1,a)]

概要：本研究は、FRAM(Functional Resonance Analysis Method) モデルにおける機能共鳴の振る舞いを，確率を扱えるモデル検査ツール PRISM により数値化し，解析することにより，事故の要因分析を容易にすることを目的としている．FRAM モデルを PRISM モデルへ変換する手法，PRISM を使った機能共鳴の振る舞いを数値化する検証手法を示し，その提案手法を事例へ適用して有効性を確認する．

Analysis of FRAM Model using Model Checking

1. はじめに

現代のシステムは，IoT や CPS をはじめとして構成要素間の相互作用が複雑である．これらの相互作用が複雑なシステムの信頼性・安全性を検証する手法については，振る舞いの把握の難しさもあり，確立されているとは言えない．効率的なシステムの開発・運用のために，信頼性・安全性を検証する手法の確立が望まれている．

相互作用が複雑なシステムの安全性解析においては，FRAM(Functional Resonance Analysis Method)[1] が特に期待されている．FRAM は，レジリエンスエンジニアリングに基づく分析手法である．機能を定義してそれらを六つの側面で関連付けることにより，事故の要因を分析できる．システムを構成する機能を積み上げて分析を行うボトムアップの手法である．

FRAM は，機能が多くなるとモデルが複雑になるため機能共鳴の振る舞いの把握が難しくなる．評価が難しい機能共鳴の振る舞いを数値化することができれば，客観的に解析ができるようになり，複雑なシステムの安全性の向上に貢献できると考える．

本稿では，モデル検査を用いて FRAM モデルの機能共鳴の振る舞いを数値化する手法を提案する．さらに，提案手法を事例に適用して提案手法の有効性の確認を行う．

2. FRAM

2.1 FRAM とは

FRAM は Hollnagel により提唱されたレジリエンスエンジニアリングの考え方に基づいた分析手法である．システムの振る舞いに着目し，システムを構成する機能を抽出して，それらの関係性を六つの側面で捉えモデル化する．このモデルを評価し，その結果に基づき分析を行う．

機能のモデルは図 2.1 に示す六角形の記述である．各機能をこの六つの側面で関連付けることによりシステムの振る舞いをモデル化する．六つの側面の定義を表 2.1 に示す．基本的には入力が機能実行のトリガと捉えるが，他の側面がトリガとなる場合もある．

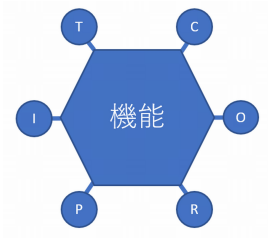

図 2.1　機能のモデル

表 2.1　六つの側面

I：入力	機能の動作トリガー
P：前提	機能が動作開始するための事前条件
C：制御	機能の挙動方法を操作する事後条件
R：資源	機能の動作に必要な資源
T：時間	機能実行可能時間
O：出力	機能の出力

各機能の六つの側面を関連付けたモデルを作成し，それらを基に想定される仕事 WAI(work as imagined) と実際の仕事 WAD(work as done) をモデル化し，その違いをギャップとして捉え，機能間の関係性から事故の要因を分析する．

2.2 FRAM モデルの評価の難しさ

FRAM は六つの側面を用いてモデルを作成するため，複雑な関係性が記述できるが，一方でモデルの振る舞いが捉えにくくなる一面もある．

[1] 日本ユニシス株式会社 Nihon Unisys,Ltd.
[a)] yoshitaka.aoki@unisys.co.jp

図 2.2 は，三つのループが組み合わさった複雑なモデルの例である [2]．いったん分かれた後，合流して元の場所に戻るため，合流部分 (図 2.2 機能 3 の I:入力部分) の同期については留意する必要がある．

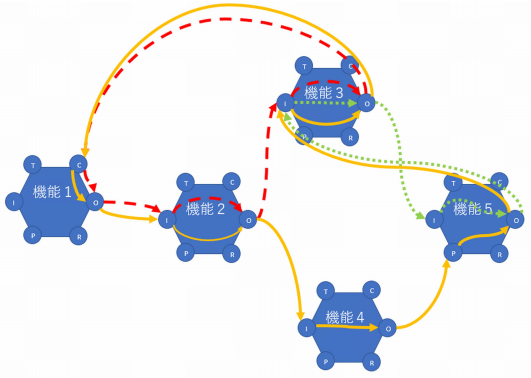

図 2.2　複雑な FRAM モデルの例

3. 本研究の目的

FRAM を用いて対象を分析する際に，分析者が行う機能共鳴の振る舞いの解析は，個々のドメイン知識やスキルへの依存度が高いため客観的な評価が難しい．

本研究の目的は，機能共鳴の振る舞いを数値化することにより客観的な評価のための指標を提供することである．これにより，着目すべきポイントの指摘や WAI と WAD の比較が容易になると考える．

モデル検査の使用が有効と考える [3] が，時相論理式による検証だけでは数値化という点で不十分であるため，確率も扱えるモデル検査ツール PRISM を用いることとした．

4. モデル検査ツール PRISM

PRISM は，確率も扱えるモデル検査ツールである．以下の特徴がある．

- 検証結果を確率で表せる
- reward（報酬）を得ることができる
- 確率 (rate) で遷移の発生頻度を操作できる

5. 提案手法

5.1 検査モデルの構築

検査モデルは，六つの側面と機能自体の状態を変数としてもち，これらの変数は二つの状態（待機中，実行中）を表すものとする．図 5.1 に FRAM モデルの状態遷移の例を示す．機能 1 と機能 2 の二つの機能があり，機能 1 の出力が機能 2 の入力に入り，機能 2 が実行中になる例である．

① 機能 1 自体が待機中から実行中になる
② 機能 1 の出力が待機中から実行中になる
③ 機能 2 の入力が待機中から実行中になる
　同時に機能 1 の出力が実行中から待機中になる
④ 機能 2 自体が待機中から実行中になる

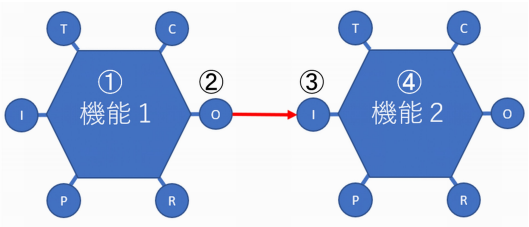

図 5.1　FRAM モデルの例

上記の状態遷移手順をベースにして PRISM で検査モデルを構築する．

5.2 検証手法

reward を用いて FRAM モデルの振る舞いを数値化して，想定している振る舞いとの間に差分があるかを検証する．

2.2 で示した三つのループを持つ FRAM モデルに提案手法を適用した結果を図 5.2 に示す．図 5.2 中の値は，100 単位時間以内の各遷移の reward の累積結果である．

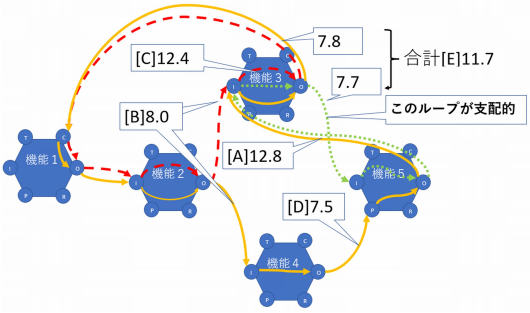

図 5.2　提案手法の適用結果の例

機能 3 が実行の条件は，完全に同期しなくてもよいこととした．この条件の場合，機能 3 に対して [A]12.8 と [B]8 の入力があるが，機能 3 の実行の reward は [C]12.4 となり，一番小さいループが支配的になることが確認できる．また，機能 3 の実行の条件を変えるとループの特性が変わることも確認できた．

6. まとめ

reward を用いる検証手法について述べたが，確率を用いる方法も有効と思われるため，今後検討する予定である．

参考文献

[1] Hollnagel, E,「Barriers and Accident Prevention」,2004.
[2] 野本 秀樹, 道浦 康貴, 石濱 直樹, 片平 真史, FRAM（機能共鳴分析手法）による成功学に基づく安全工学，SEC journal , Vol.14, No.1, pp.42-49, 2018.
[3] Yoshitaka Aoki, Shinpei Ogata, Kazuki Kobayashi and Hiroyuki Nakagawa, Verification of CPS Based on Control Loop using Model Checking, 25th Asia-Pacific Software Engineering Conference (ASPEC 2018), 2018.