Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

MATLAB/SimulinkモデルのFRAMモデルへの変換手法

掛下　真通[1,a)]　久住　憲嗣[1]　道浦　康貴[2]　酒見　慶太[2]　松本　充広[2]　安藤　崇央[1]　福田　晃[1]

概要：近年制御系組込みシステムにおいてモデルベース開発（MBD: Model Based Development）の普及が進み，MATLAB/Simulink 等によって開発仕様書が記述され，曖昧な記述を排除できるようになった．機能共鳴分析手法（FRAM: Functional Resonance Analysis Method）は，社会技術システムにおける安全分析手法の一種である．機能の変動に注目したモデルを作成し分析を行うことで，失敗に囚われず成功要因を育てることもできる分析を実施できる．このように新たな設計技術と分析手法が台頭しつつあるが，MBD の開発仕様書に FRAM を適用するには様々な課題が存在するため MBD における FRAM の明確な適用手法は未だに確立されていない．そこで本研究は MATLAB/Simulink モデルの FRAM モデルへの変換手法を提案する．MATLAB/Simulink モデルにおける FRAM モデルの機能同定方法や機能の側面の同定基準を明確にすることで FRAM モデルへ変換できるようにする．

A MATLAB/Simulink Model to FRAM Model Conversion Method

1. はじめに

1.1 研究背景

これまでは制御系組込みシステムにおいて，要求分析を行ってから設計するという流れで自然言語により開発仕様書を記述していた．しかし近年ではモデルベース開発（MBD: Model Based Development）の普及が進み，MATLAB/Simulink [1] 等によって開発仕様書（以下断りがなければ MATLAB/Simulink によって記述された開発仕様書を指し，Simulink モデルと呼ぶ）が記述されるようになった．従来は自然言語を用いて開発仕様書が記述されていたが，曖昧な記述のために人によって仕様書の解釈が異なってしまうリスクが存在した．これに対して Simulink モデルは精緻に表現されるため，そのようなリスクを排除できる．

機能共鳴分析手法（FRAM: Functional Resonance Analysis Method）[2] は，社会技術システムにおける安全分析手法の一種である．従来の安全分析手法は，悪い結果は失敗から生じると言う思想に基づくものであった．しかし実際にはイベント全体に対しては成功事象が大半を占めており，さらにその中には想定外のイベントが発生していたにも関わらず成功した事象が存在している場合が多い．そのため，失敗のみに着目をする思想は必ずしも合理的であるとは言えない．一方 FRAM は機能を定義し，各機能を 6 種類の側面によって特徴付けることでモデルを作成し，機能の変動に注目した分析を行う．これにより失敗に囚われず，「なぜうまく行っているのか」という成功要因を育てることもできる分析を実施できる．

このように新たな安全分析手法が台頭しつつあり，Simulink モデルに適用することで新しい発見を得られる可能性がある．しかし今日まで，Simulink モデルを対象とした FRAM の適用手法は確立されていない．実際 Simulink モデルに FRAM を適用するには様々な課題が存在する．MBD による開発仕様書はしばしば抽象度が低くなる．そのため，本質的に重要な要素を識別し関連の本質を見出すという，FRAM を実施する上で必要となるステップを満足に行うことは難しい．そこで Simulink モデルに対して，FRAM を実施するための手法を構築することが求められる．

1.2 研究目的

Simulink モデルに FRAM を実施するためには，Simulink モデルから FRAM モデルに変換する必要がある．これを可能にするために，以下の 3 つの目標を達成する必要が

[1] 九州大学
Kyushu University, Fukuoka 819–0395, Japan
[2] 有人宇宙システム株式会社
Japan Manned Space Systems Corporation
[a)] kakeshita@f.ait.kyushu-u.ac.jp

Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

ある．

1 つ目は，Simulink モデルから FRAM モデルに関わる重要な要素を識別する方法を構築することである．Simulink モデルは，システムを動作可能なレベルまで具体的に表現しているため，複雑度が高い．このようなモデルから，安全上重要な要素をどのように識別して FRAM モデルとして表現すれば良いかを検討することで，MBD から FRAM モデルの機能への変換を行える．

2 つ目は，Simulink モデルの入出力を FRAM モデルの 6 つの側面に結びつける方法を構築することである．FRAM は機能を Input，Precondition，Control，Resource，Time，Output という 6 つの側面によって特徴付けることにより機能間の関連を分類し，分析を行う．その分類を行うためには，Simulink モデルの入出力がどのように扱われているかを把握する必要がある．この入出力の扱いを把握する方法を構築することで，Simulink モデルから FRAM モデルの関連への変換を行える．

3 つ目は，Simulink モデルから FRAM モデルに移植できない情報を識別し，その情報をどのように扱うかを明確にすることである．Simulink モデルの状態遷移ロジックなど，機能の中身のロジックについては，FRAM モデルに変換することができない．このように，FRAM モデルに移植できないものを把握し，またそれについて他の整理方法があるかどうかを検討することで，Simulink モデルの情報を無駄なく分析できる．

1.3 論文構成

本論文の構成は以下の通りである．2 節では，本研究を理解するために必要な関連技術について詳しく説明する．3 節では，提案手法の概要と，提案手法におけるステップについて詳しく述べる．4 節では，提案手法のケーススタディについて述べる．最後に 5 節で，本論文のまとめと今後の展望を述べる．

2. 関連技術

2.1 MATLAB/Simulink

MATLAB/Simulink では，ブロック線図形式のモデル（以下 Simulink モデル）で制御ロジックを記述する．そして，作成したモデルのシミュレーション検証を行うことで，制御ロジック誤りの早期発見や費用のかかるプロトタイプの回数の削減が可能となる．さらに，制御ロジックをモデルで表すことで，曖昧な記述のために人により解釈が異なるという，自然言語により記述された開発仕様書だと起こりうるリスクを排除できる．

Simulink モデルの記述は自由度が高く，用途や設計者により様々な記述方法を用いることが可能である．しかし製品開発における制御設計では，制御ロジックの理解のしやすさや制御モデルの再利用性を考慮して，一定の基準に基づいた記述を行うべきである．

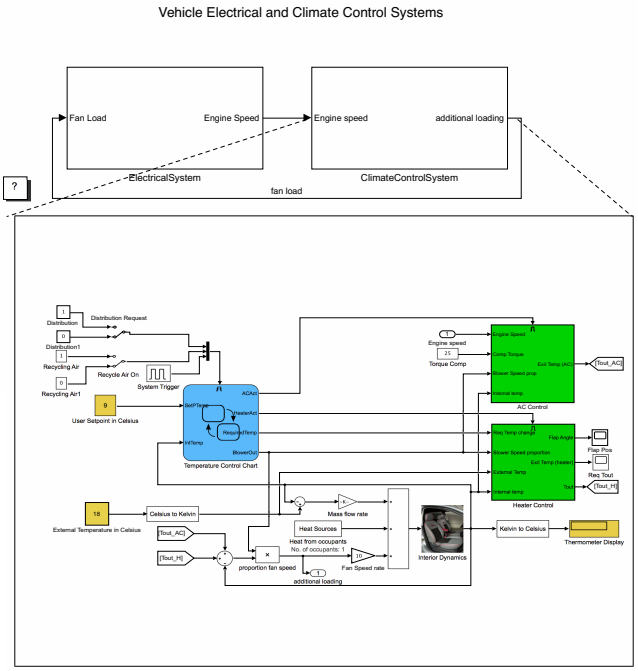

図 1 階層化した Simulink モデルの例（ [3] の図面を参考に作成）

Simulink では，Subsystem ブロック [4] を用いてモデルの階層化を行う．Subsystem ブロックは，制御ロジックにおいて重要な意味を持つデータを出力するように構成され，Subsystem ブロックの下位階層にはそのデータを算出するための処理が記述される．これにより，Simulink モデルを Subsystem 単位で再利用可能な構造にできる．図 1 に階層化した Simulink モデルの例 [3] を示す．

また，最上位階層に現れるデータには名前をつける．前述の通り，通常は制御ロジックにおいて重要な意味を持つデータにデータ名が与えられる．まず入力を表す Inport ブロックから出ているデータの名前を Inport ブロック名に記述する．次に Subsystem ブロックから出ているデータの名前を，Subsystem ブロック内にあり出力を表す Outport ブロックの名前に記述する．このことにより Subsystem ブロックにデータ名が表示される．データの型情報を付けたい場合は，そのデータを表すラインのライン名にデータの型を記述する．

2.2 Safety-I 及び Safety-II

Safety-I 及び Safety-II [5] はいずれも安全性を高めるための思想であるが，両者には大きな違いがある．Safety-I は，物事がうまくいかなくなる原因を取り除いていくことで安全性を高めるという考え方である．これに対して Safety-II は，なぜ物事が上手くいくのかということにも着目することで安全性を高めるという考え方である．

Safety-I は，成功と失敗の原因とは完全に異なるものであり，失敗の原因を取り除くことで安全性を高めるという考え方である．これは従来の多くの安全分析手法の根底

Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

にあった考え方である．FTA [6] は失敗の原因を明示的に求める．また STAMP/STPA [7] は，機能間の相互作用が「遅れる」「間違う」などといった故障以外の要因を求めるが，いずれにせよ「失敗」に着目している．しかし近年，システムや社会の複雑さが増したことで，外乱は複雑なものになった．この外乱に適応するためにオペレータは変動を起こす．この変動が非常に柔軟なもの同士の干渉であるため，結果として上手くいく可能性もある一方で事故になる可能性もあるという状況が出てきた．2 つの結果は同じ要因の元で生じたものであるため，成功も失敗も同等であると見なすことができる．この状況下では，失敗だけに焦点を当てることは安全性を高めることにおいて効果的とは言えない．さらに通常は全体のイベントに対して事故などの容認できないイベントは極めて少なく，ほとんどは正常なイベントないし成功したイベントで占められる．したがって失敗だけでなく，正常なイベントや成功したイベントにも注目をする意義がある．そして適切なことに焦点を当てて追求することで安全性の向上を果たすという考え方が Safety-II である．ここで，Safety-II はイベント全体を考慮するものであり，Safety-I を無視しないことに注意する．

2.3 FRAM

機能共鳴分析手法（FRAM: Functional Resonance Analysis Method）とは，社会技術システムにおける安全分析のための手法である．機能共鳴とは，複数の機能が相互に作用した結果外乱に柔軟に対応する一方で，逆に変動の増大などを起こし，安全を脅かすことを指す．FRAM ではこの部分に着目をし，機能の関係性の中から安全に関わるシステムの長所と短所を見出す．

FRAM による分析には FRAM モデルを用いる．FRAM モデルは機能およびその機能を特徴付ける側面を定義することで作成する．

表 1 6 つの側面

側面	側面の説明
入力（I）	出力の材料及び機能のトリガ
出力（O）	機能が動作した結果
前提条件（P）	機能が動作するための前提条件
制御（C）	機能の動作の制御
資源（R）	機能が動作し続ける条件
時間（T）	機能の動作の時間的制約

表 1 に，機能を特徴付ける 6 つの側面について示す．このうち 5 つの側面 I，P，C，R，T は他の機能の出力を表す側面である O に対応すべきであるという原則がある．これは側面が単に機能の 1 つの「端子」であり，FRAM モデルを完成させるために必要な機能を見つけることを支援するものである．

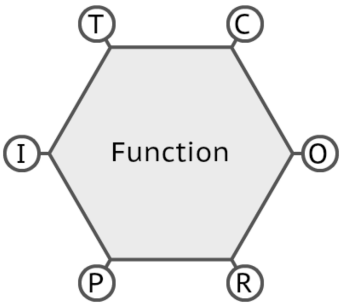

図 2 FRAM モデル図における機能の六角形表現

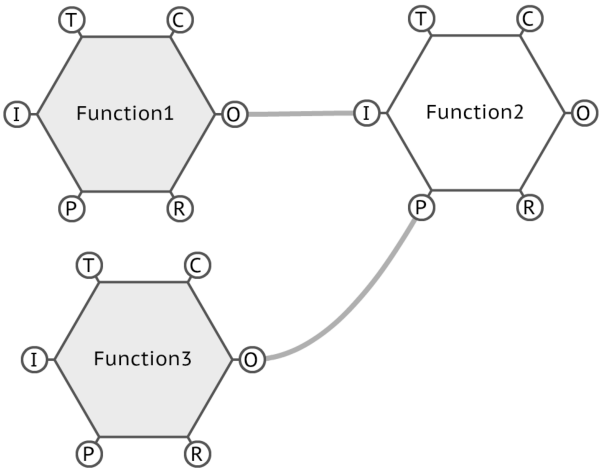

図 3 FRAM モデル図

また，機能間の結合を視覚的に表すために，図 2 のような六角形を用いて機能を表現する．この六角形の各頂点は機能の 6 つの側面に対応している．この六角形を図 3 のように繋げることで，機能間の関連を表現できる．このようにして機能がどのように結合されうるのか明らかにすることで，パフォーマンスの変動の同定や，その変動がいかにして予期しない規格外の結果を生み出すのかについての理解を可能にする．

3. 提案手法

3.1 概要

本節では，Simulink モデルから FRAM モデルに変換するための方法について提案する．機能を定義し，その機能を側面によって特徴付けることによって FRAM モデルを作成する．Simulink モデルの変換においては，まず 2.1 項で述べた Subsystem ブロックを参照しつつ機能の同定を行う．そして Simulink モデルに記述されている要素間の関連を基準に従って分類することで機能の側面を定義する．以下では，これらのステップについて詳しく説明する．

Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

3.2 ステップ 1：機能の同定

ステップ 1 では，FRAM モデルにおける機能の同定を行う．Simulink モデルは Subsystem ブロックにより階層化されていることを前提とする．まず，Subsystem ブロックを動力系，センサ系，制御系という 3 つの系に分類する．ここで動力系とは，電源や発電機などといった動力を生み出す Subsystem と定義する．センサ系は，気温や湿度などのデータを計測する Subsystem と定義する．制御系はいわゆるプラントモデル及びコントロールモデルであると定義する．これにより各 Subsystem の目的を明確にする．次に動力系，センサ系の Subsystem ブロックを展開する．抽象度としては原則として最上位の階層，すなわち限りなく高いものにする．しかし動力系とセンサ系がシステム全体に対して他のそれらとは明らかに独立した目的を持つ場合は，その部分を分解して取り扱う．これは原則として注目すべき Subsystem は制御系であり，他の 2 つの系の Subsystem はそれを補助するものに過ぎないという考えによるものである．さらに制御系の Subsystem ブロックを展開する．制御系 Subsystem ブロックにおいては FRAM モデルの可読性も考慮し，各最上階の制御系 Subsystem につき 5 ± 2 個程度で構成されるように分解されるのが望ましい．以上によって展開された Subsystem に加え，その階層における残りの Simulink ブロックや Stateflow チャートを機能として同定する．

3.3 ステップ 2：入出力の分類

ステップ 2 では，ステップ 1 で同定した機能同士の関連を 6 つの側面に分類する．これは 2.3 項で述べた，側面は機能の「端子」と見做すことができるということから，その端子同士のインタラクションが機能同士の関連に対応できるという考え方によるものである．また Simulink モデルのラインもブロック間の関連を明示するものであるため，FRAM モデルの機能同士の関連と対応させることができる．ゆえにステップ 1 で同定した際に着目した Subsystem ブロック間のラインを分類することができれば，その情報を FRAM モデルの機能の側面に反映させることができる．この関連を分類する際の基準を以下に示す．なお，Simulink にはバスと呼ばれる複数の信号をまとめた信号がある．そのバスの中で他のまとめられている信号と違う側面を持つ信号が存在した場合は，その信号のみを独立させてフローを抽出する．記述法としては，信号 S_1,S_2,S_3,... をまとめたバス B が存在し，その中で S_i,S_j が他の信号と異なる側面に分類され，残りの信号が同じ側面に分類された場合，信号 S_i,S_j はそのまま独立して記述し，残りの信号に関しては B-$\{S_i,S_j\}$ という形で記述する．

関連の分類手順の概要を図 4 に示す．まず，機能の出力は定義に従い O に分類する．次に，動力系から受け取る入力は R に分類する．これはその入力は出力に直接的に

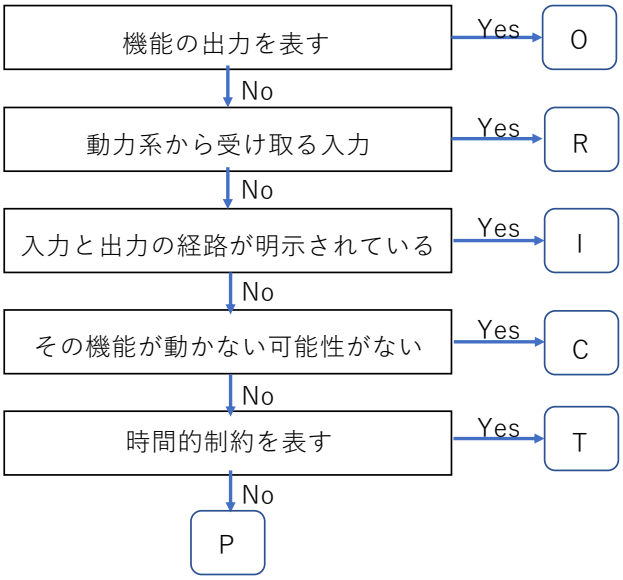

図 4　関連の分類手順

は関与しないが，その出力を生み出す機能が動作するに必要なためである．続いて，入力と出力の経路が明示されているものは I に分類する．これは入力が出力の材料として用いられていることが明らかなためである．ここまでの過程で分類されなかった入力は，残りの側面 P，C，T に分類される．この 3 つの側面に分類される入力は出力に直接変換されるものではないが，出力の結果を変えうるものであるという意味で「条件的入力」と呼ぶことにする．特に Stateflow チャートによって決まるステートは条件的入力に該当する．条件的入力のうち，その入力が何であれ機能が全く動作しないという可能性がないものは C に分類する．これは他の側面である P，T がその機能の動作条件に関与するものである一方で，C は機能が求められる動作方法を提供するものであるという性質の差異を用いたものである．そして残った入力のうち，時間的制約を持つものは定義に従い T に分類される．そして最後に残った入力が P に分類される．以上の操作により FRAM モデルを作成する．

4. ケーススタディ

4.1 今回取り扱う Simulink モデルについて

今回は，Simulink Drone Reference Application [8] というプロジェクトを題材に扱う．これは，ドローンや UAV などといった遠隔操縦無線制御固定翼航空機の飛行安定化のための自動操縦およびその軌道を制御するためのオペレータインタフェースの実装を示したものである．図 5 にこのプロジェクトの Simulink モデルを示す．Simulink モデルの最上階は無人航空機のオペレータを表す Unmanned Airplane Flight Operator，自動操縦モデルを表す AutopilotControlSystem，プラントモデルを表す PlantModel の

Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

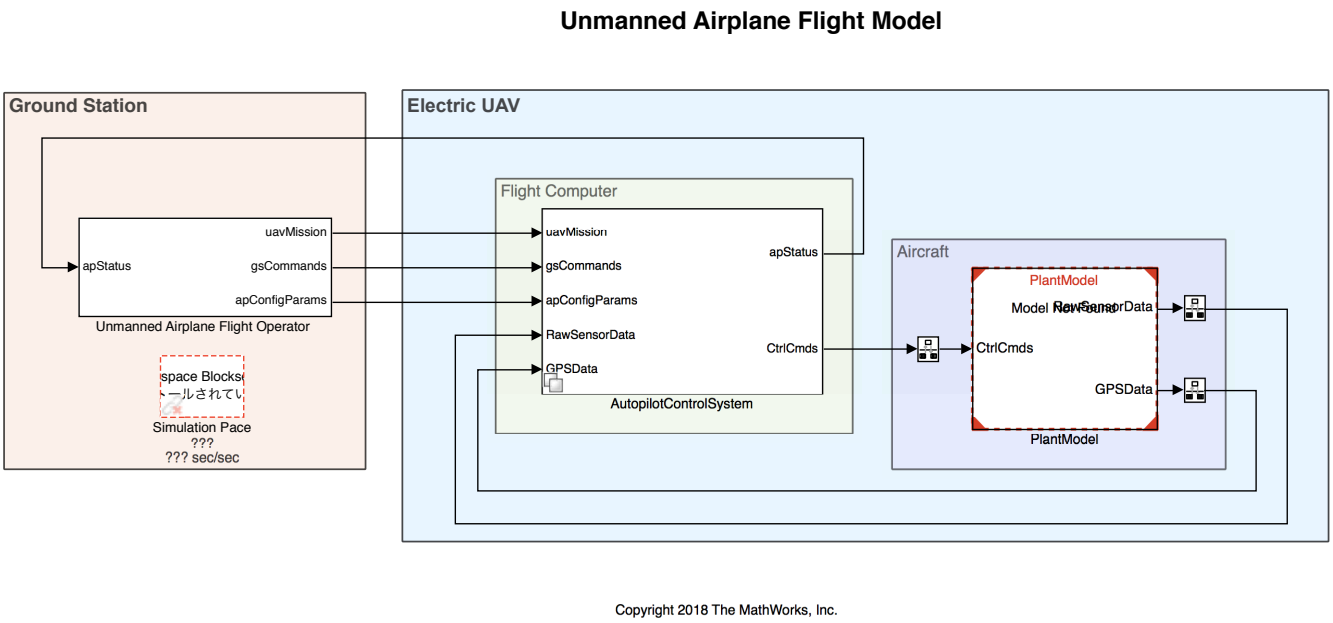

図 5 今回取り扱う Simulink モデル（ [8] から引用）

3 つの Subsystem ブロックで構成されている．Unmanned Airplane Flight Operator には GS Commands Variant という Subsystem が存在し，その内部は何によって操縦を行うかによって振る舞いを変更できるように 4 つの Subsystem で構成されている．AutopilotControlSystem 内部には設計プロセスの途中でも設計の検証を可能にするために様々な抽象度で記述された Subsystem が 3 つ存在するが，いずれもほとんど同様の制御を行なっているため一つの AutopilotControlSystem とみなす．進行方法を指定する GuidanceLogic や自動操縦が行えるようスロットルの出力及び補助翼の角度などのパラメータを調節する InnerLoopAutopilot などで構成され，各 Subsystem 内もそれぞれの目的を果たすための Subsystem ブロックで構成されている．例えば航空機の位置と速度を計測する Navigation Filter 内には，GPS により計測された緯度，経度，高度から平面上の現在地を算出する LLA to Flat Earth という Subsystem が存在する．PlantModel は，天気モデルを表す Weather Model やアクチュエータを表す Actuator Model などのプラントモデルとなる Subsystem で構成されている．

4.2 適用

4.1 節の Simulink モデルに提案した変換手法を適用し，完成した FRAM モデル図及びそのモデルの詳細について説明する．

4.2.1 完成した FRAM モデル図

FRAM モデル図は，**図 6** のようになった．モデル図を見ると 3 段構成になっており，上から順に無人航空機のオペレータ，自動操縦モデル，プラントモデルを表す．そしてその段の機能が，それぞれのモデルを構成する要素となっている．まず最上位の階層において現われている各 Subsystem ブロックは全部で 3 個であり，全て制御系であるため各 Subsystem について展開する．すると Unmanned Airplane Flight Operator からは 1 つ，AutopilotControlSystem からは 4 つ，PlantModel からは 5 つ，合計で 10 個の制御系 Subsystem が現れた．そのため抽象度としては適度であると考え，この階層における Subsystem を機能として同定した．またほとんどの機能の入力は出力との明確な関連が存在するため I に分類されているが，GPSData.gps_fix は出力との関連は見当たらず，また閾値を超えていなければ Navigation Filter の内部に含まれるサブシステムである LLA to Flat Earth は動作することができず，さらに時間的制約を持つものではないため，P と分類される．

表 2 Navigation Filter の FRAM モデル

機能名	Navigation Filter
記述	
側面	側面の記述
入力（I）	GPSData-{GPSData.gps_fix}
	uavMission
	FilteredSensorData
出力（O）	PosVel_hat
前提条件（P）	GPSData.gps_fix
制御（C）	
資源（R）	
時間（T）	

Vol.2019-ARC-240 No.44
Vol.2019-SLDM-191 No.44
Vol.2019-EMB-53 No.44
2019/2/28

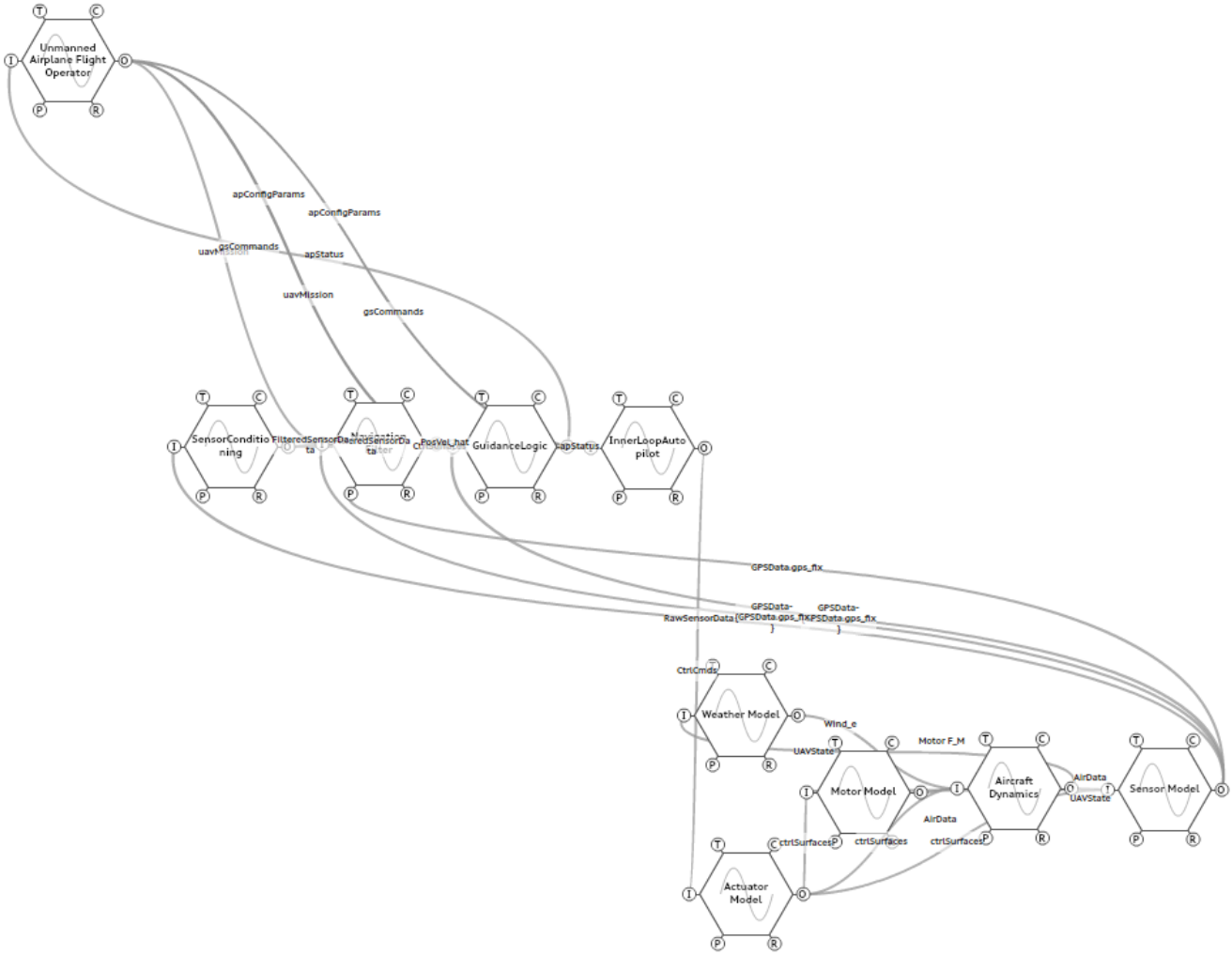

図 6 Simulink Drone Reference Application に提案手法を適用し作成した FRAM モデル図

Navigation Filter の FRAM モデルの詳細を表 2 に示す．

4.2.2 モデル分析

4.2.1 項で作成された FRAM モデルに対して安全分析を行った．GPSData.gps_fix が正常に伝わらなかった場合，Navigation Filter は内部のサブシステムが動作する予定であったにも関わらず動作しないなどというような予期しない挙動を起こし，間違った出力を発行する可能性がある．その結果プラントモデルの挙動が変動し，不適切な挙動を行った結果，その後の制動も不安定なものになる可能性がある．この変動可能性を踏まえると，例えば不適切な GPSData.gps_fix が転送されないようにするために，他の入力と同期させる機能を追加するなどといった対策が考えられる．

4.3 適用結果

3 節で提案した手法を Simulink モデルに用いることで FRAM モデルを作成し，それを分析することで対策を講じることができた．一方で機能を同定する際に，一見似たような状況であっても場合によって扱い方が異なる場合に Simulink モデルの理解を必要とした．Unmanned Airplane Flight Operator のように似たような Subsystem が存在し，コンテキストによってどの Subsystem を利用するかが変わることで制御の内容も大きく変わってしまうものは，同じ入力を受け取り同じ意味の出力を発行するにも関わらず展開するのは非合理だと考え，それ以上 FRAM モデルで詳細に記述しなかった．一方で AutopilotControlSystem のように，似たような Subsystem が存在するが記述法が異なるだけなどの理由で内容はほとんど同等である場合には，それらの Subsystem は全て同じ Subsystem とみなした．そしてこの時点で AutopilotControlSystem における Subsystem の個数は 3.2 項で述べた望ましい基準とされる 5 ± 2 個には届いていなかったため，さらに FRAM モデルで詳細に記述するようにした．Subsystem が似ているかどうか及びその中身の制御が同等であるかどうか，そして Subsystem を展開することが合理的であるかどうかについては，筆者の感覚に基づいて判断した．そのため，分析者によっては全く異なる FRAM モデルが作成される恐れがある．

5. おわりに

5.1 まとめ

Subsystem ブロックを利用して機能の同定を行い，Subsystem 間のラインを分類することにより機能の側面を定義することで MATLAB/Simulink モデルを FRAM モデルに変換できるようにした．それを実際の Simulink モデルに適用することで FRAM モデルを作成することができた．また作成した FRAM モデルに対して分析を行うことでシステムの問題点を発見し，改善策を提案することができた．一方で機能を同定する上では，Simulink モデルの内容を理解していなければ抽象度をどうすべきかを決定することが難しい場合があった．また分析者の感覚によって，同じ Simulink モデルから異なる FRAM モデルが作成される可能性があることが分かった．

5.2 今後の課題

FRAM モデルの機能を定義する上で，現状は Subsystem ブロックによる分類という設計者の記述に依存した方法をとっている．そのため，目的や設計者によって Subsystem ブロックが極端に多くなったり少なくなったりする場合に，機能の同定が難しくなることが考えられる．したがって Simulink モデルの規模や抽象度に関わらず機能の同定を行えるようにすることが要求される．また，本論文では限られた Simulink モデルについてのみ有効性を確認している．そして FRAM モデルが妥当なものであるかについて具体的な指標は未だに確立されていない．そのため，任意の Simulink モデルを有効な FRAM モデルに正しく変換できるのかについて提案手法の信頼性の検証を行うとともに，実際に手法を適用できるよう信頼性を向上させる必要がある．

参考文献

[1] The MathWorks Inc.: MATLAB/Simulink, http://www.mathworks.com/.
[2] Hollnagel, E.: *FRAM: the functional resonance analysis method: modelling complex socio-technical systems*, CRC Press (2017).
[3] The MathWorks Inc.: Vehicle Electrical and Climate Control Systems, https://jp.mathworks.com/help/simulink/slref/vehicle-electrical-and-climate-control-systems.html?lang=en.
[4] The MathWorks Inc.: Subsystems, https://jp.mathworks.com/help/simulink/subsystems.html?lang=en.
[5] Hollnagel, E.: *Safety-I and Safety-II: The Past and Future of Safety Management*, CRC Press (2016).
[6] FAA: *FAA System Safety Handbook*, chapter 9: Analysis Techniques, FAA (2000).
[7] Leveson, N.: *Safety-I and Safety-II: The Past and Future of Safety Management*, CRC Press (2016).
[8] The MathWorks Inc.: simulinkDroneReferenceApp, https://github.com/mathworks/simulinkDroneReferenceApp.