G-19

システム開発過程での変更の影響度から見る安全解析手法の比較検討

入江 琴子 [1]　片平 真史 [2]　石濱 直樹 [2]　柿本 和希 [3]　崔 恩瀞 [1]　飯田元 [1]

1. はじめに

航空機や宇宙機など，非常に高い安全性が求められるセーフティクリティカルなシステムでは，その開発と並行して安全解析が段階的に行われる[1]．セーフティクリティカルなシステム開発の中で，既に実施された開発工程の成果物に変更が適用される場合，その変更に対応する影響が安全解析にも及び得る．例えば，システム要求の変更はセーフティクリティカルなシステムの開発過程において頻繁に適用され，変更された要求に関連する安全解析にも変更の影響が生じる．しかし，このような場合に，既に行われた安全解析への影響箇所および影響の度合いに関する評価は熟練者の経験と知識に依るところが大きく，体系的な研究が未だ少ないというのが現状である．

また，開発の成果物が変更され，特定の安全性に関するリスクが存在するか判断する際には，安全解析手法であるFMEA(Failure Mode and Effect Analysis)の解析結果が用いられることが多い[2]．しかし，FMEA には，多重故障の影響を考慮しない，故障モードを全て把握した上で解析を行わなければ未知の故障モードに起因するハザードを見逃す恐れがある，などの短所がこれまでにも指摘されており[3]，FMEA のみでは識別しきれない影響箇所が存在するのではないかと考えられる．

そこで，本研究ではセーフティクリティカルなシステムを対象とし，その開発過程での変更に伴う既存の安全解析への影響評価について調査する．具体的には，FMEA とともによく用いられる安全解析手法である FTA(Fault Tree Analysis)と変更の影響分析において評価の差異が出そうな箇所を挙げて仮説を立て，それぞれの仮説を検証することで両手法の結果を影響分析に用いた際の効果を示す．

本論文の構成は以下の通りである．まず 2 章では，安全解析の目的および既存の安全解析手法として FTA と FMEA を比較調査した結果を示す．3 章ではこれらを前提に，変更に伴う安全解析への影響評価において，両安全解析手法の間に評価のしやすさの差異が現れると考えられる点を複数の仮説として，その理由とともに示す．4 章では前章で示した仮説を検証するための実験方法の構想について検討し，最後に 5 章でまとめと今後の展望を述べて結言とする．

2. 安全解析手法について

本章では，まず安全解析を行う目的とその必要性について説明し，代表的な安全解析手法である FTA と FMEA について示した後に，それらを比較した結果とともに述べる．また，安全解析の成果物が開発の成果物とどのように関係しているのかを示す．

2.1. 安全解析の目的

安全解析の最も重要な目標は，システムの状態がハザードとなることを避ける，または抑制することにある．ここでハザードとは，人間の生命の喪失または傷害や物的損害や機密情報の漏洩などの損失に繋がるようなシステムの状態または条件を指す．システム開発と並行して行われる安全解析は，起こりうるハザードを識別または評価し，開発しているシステムからそれらを除去するか制御する目的を持つ．[1]すなわち，開発中のシステムにハザードを引き起こす要素が組み込まれている可能性がある場合，該当する要素を除去または制御することでハザードの発生を防止する役割を担っている．

2.2. FTA(Fault Tree Analysis)と FMEA(Failure Mode and Effect Analysis)

FTA は，システムにとって望ましくない事象や条件(損失やハザードなど)をトップ事象として最上位に置き，上位の事象をより基本的な下位の事象の組み合わせとして表現するという規則のもとにフォールトツリーと呼ばれる木を構成していくことでトップ事象の原因系を求める安全解析手法である[3][4].

図 1 に FTA の例を示す．この例では「爆発」という事象をシステムの望ましくない事象としてトップ事象に置いている．システムの設計などを考慮して爆発につながると考えられる条件を論理演算子で組み合わせてフォールトツリーを形成することで原因系を表現している．このフォールトツリーの 2 段目までに説明を限定するなら，「圧力が高すぎる」「逃がし弁#1 が動作しない」「逃がし弁#2 が動作しない」という条件が組み合わさることで「爆発」という望ましくない事象が起きていることがわかる．

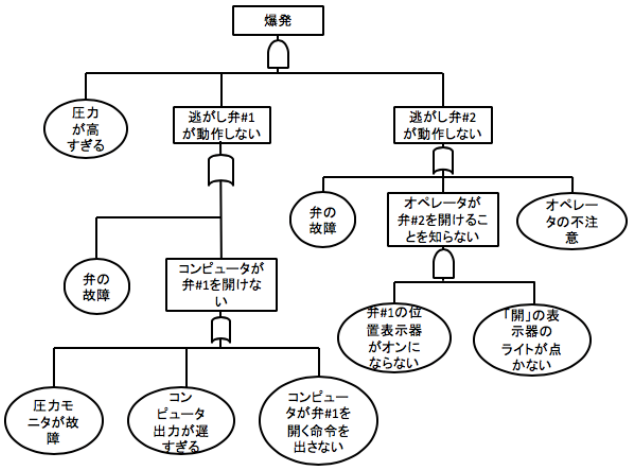

図 1. FTA の例[4].

1 奈良先端科学技術大学院大学, Nara Institute of Science and Technology
2 宇宙航空研究開発機構, Japan Aerospace Exploration Agency
3 有人宇宙システム株式会社，Japan Manned Space Systems Corporation

FTA の特徴の 1 つとして，AND や OR などの演算子を用いることにより，下位のより基本的な事象を組み合わせて上位の事象の原因系を表現できることが挙げられる．すなわち，フォールトツリーの各レベルの事象は，より上位の事象が示す問題の原因となる基本的な事象の集合となる．

また，FTA における安全解析の起点となるトップ事象はあらかじめ識別されていた損失やハザードにより定義される，ということも FTA の特徴の 1 つである．つまり，FTA は発生しうる損失やハザードを事前に識別する解析手法というより，それらの原因系を求めることに主眼を置いた解析手法である．

一方，FMEAは，システムを構成する個々のコンポーネントの故障モードを安全解析の起点とし，それぞれの故障モードについて，その原因およびシステム全体への影響を分析していく手法である．ここで故障モードとは故障状態の形式による分類である[3][4]．

図2にFMEAの例を示す．FMEAではまずコンポーネントごとに起こりうる故障モードが定義され，定義した故障モードが発生する確率とその影響について分析する．なお，この例では故障影響の分析は影響が重大か否かの視点からの記載のみにとどまっているが，通常はより幅広い視点から故障のシステムへの影響を分析し，それらの影響への対策までを含めてFMEAの安全解析結果としてまとめるのが一般的である．

コンポーネント	故障率	故障モード	モード別故障割合(%)	影響	
				重大	重大ではない
A	1×10^{-3}	断線 短絡 その他	90 5 5	5×10^{-3}	√
B	1×10^{-3}	断線 短絡 その他	90 5 5	5×10^{-3}	√

図2. FMEAの例[4].

FMEAは，単一コンポーネントの故障モードから解析を始めて最終的に故障のシステム全体への影響を評価するため，個々のコンポーネントが引き起こすハザードを発見するには最も適した安全解析手法と言える．一方で，コンポーネントの組み合わせに対する解析はFMEAでは想定していないため，複数のコンポーネントの故障の組み合わせが引き起こすハザードの識別については限定的である．

また，FMEAではコンポーネントの故障モードを解析の起点としているため，コンポーネントの故障状態が(暗黙的にであっても)定義されていることを前提とする．すなわち，「故障」という状態が定義できない，もしくは定義が困難なコンポーネント(ソフトウェアなど)にはFMEAを適用するのが難しいと言える．

本章の最後に，FTAとFMEAについてのこれらの比較をまとめたものを表 1 に示す．

表1. FTAとFMEAの概要比較

	FTA	FMEA
概要	システムにとって望ましくない事象(トップ事象)の原因系を，より基本的な事象を組み合わせることで表現する	システムに含まれる全てのコンポーネントの故障モードに対して，故障がシステムに与える影響を洗い出す
長所	因果関係が分かりやすい 論理演算子で組み合わせることで複数コンポーネントが引き起こす影響も析できる	単一コンポーネントの故障の影響を直接参照できる FMEAを完全に実施することで構成品目の全てについて故障の検討ができる
短所	ハザードそのものを識別する手法ではなく，ハザードは別の手法であらかじめ識別されている必要がある	複数のコンポーネントの組み合わせで起こる多重故障についてはサポートされていない

2. 3. 安全解析結果と開発の成果物の関係

図 3 に，本研究の前提となる安全解析結果と開発の成果物の関係を示す．

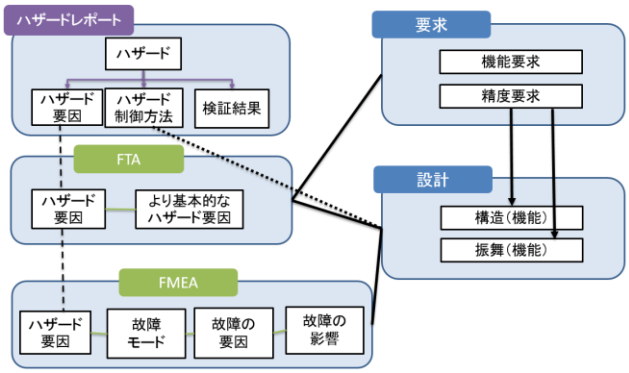

図 3. 安全解析結果と開発の成果物の関係

図 3 の左側が安全解析の成果物，右側が開発の成果物である．まず，図 3 実線が示すとおり，開発の成果物である要求や設計の情報を元に，FTA や FMEA といった手法でハザードの解析が行われる．システムの故障要因となるハザードを洗い出した後に，各ハザードを除去または制御する方法が識別される．システムの設計は，図 3 点線部で関連を示しているように，ハザードを除去または制御できるものになっている必要がある．設計がハザードに対応しているかの検証も安全解析において行われる．ここで識別・検証された情報はハザードレポートにまとめられている．ハザードレポートに記載されているハザード要因と FTA，FMEA で識別されるハザード要因は全て同一である(図 3 破線)．

安全解析が行われた後に，システムの要求や設計などの安全解析の元となる情報が変更されるとき，

- 変更が現在識別されている特定のハザードに関係するか，関係する場合，ハザードは除去または制御できるか
- 変更が現在識別されていないハザードを引き起こす可能性があるか，可能性がある場合，そのハザードはどのように除去または制御されるべきか

といった観点から検討が行われ，必要な場合，追加の安全解析が行われる．

なお，システムの開発における変更が特定のハザードに関係するかどうか識別するために，FMEA での解析結果が頻繁に参照されていることが先行研究によって明らかになっている[2]．

3. 安全解析手法の影響度評価比較に向けた仮説

本章では，システム開発過程での変更に伴う安全解析への影響評価において，FTA と FMEA という 2 つの安全解析手法の間に評価のしやすさの差異が現れると考えられる点を仮説として立て，仮説とするに至った理由とともに示す．なおこれらの仮説は，宇宙航空研究開発機構(Japan Aerospace Exploration Agency;以下 JAXA)で実際にセーフティクリティカルなシステムの安全解析に携わる熟練者を含む筆者らが議論を行った結果，妥当と判断したものである．

まず FTA の方が影響評価をしやすいと考えられる仮説として以下の 2 件を得た．

仮説 1.1. FTA の方がコンポーネントの組み合わせレベルでの変更に対する影響評価をしやすい．

理由：FMEA は単一コンポーネントの故障モードが解析の起点であり，かつそれらの組み合わせをサポートしていないため，複数のコンポーネントが組み合わさったことによる変更の影響評価は困難であると推測される．一方，FTA では AND や OR などでハザードに至る故障要因の組み合わせが可能であるため，それらの組み合わせからトップ事象に遡って対応するハザードを識別しやすく，変更に対して影響評価がしやすいと考えられる．

仮説 1.2. FTA の方がシステムの要求に対する影響評価やハザードへのトレースをしやすい．

理由：ボトムアップ分析である FMEA では，要求の変更における影響を調べる場合，変更する要求をいったんコンポーネントレベルの故障モードまで分解した後に要求レベルまで戻って評価を行う必要があると考えられる．すなわち，FMEA ではこの場合要求-コンポーネント間での往復的なトレースを必要とするため，影響の評価に時間がかかることが予想されるほか，往復的トレースで 2 段階の手順を経るため，影響評価の抜け漏れも生じやすいのではないかと推測される．一方，FTA ではトップダウン分析のため階層上位の事象に要求と対応する事象があり，そこからより基本的な事象へと階層を下げて参照していくことで影響範囲を段階的に直接トレースでき，FMEA での影響評価において推測される上記のような問題は起こりにくいと考えられる．

次に，FMEA の方が影響評価をしやすいと考える仮説は以下の 1 件である．

仮説 2. FMEA の方がコンポーネント単位での変更に対する安全解析への影響評価をしやすい．

理由：FMEA はコンポーネント単位での故障に対する安全への影響を分析しているので，コンポーネント単位の変更がシステムに及ぼす影響を評価したい場合は起点となるコンポーネントの故障モードから直接参照できると考えられる．

4. 実験計画

本章では，前章で示した仮説を検証するための評価実験について述べる．まず 4.1 節で実験の対象となるシステムについて述べ，次に 4.2 節で実験方法の詳細を示す．

4.1 実験対象のシステム概要

本評価実験では，実践的な評価実験を行うため，JAXA で開発された宇宙ステーション補給機「こうのとり」(H-II Transfer Vehicle;以下 HTV)における FTA・FMEA の既存の安全解析結果を用いる予定である．

HTV は，国際宇宙ステーションへ物資を補給する無人の宇宙船である．2009 年に 1 号機が打ち上げられ，2017 年までに 6 号機までが安全に運用を終了し，2018 年 9 月には 7 号機の打ち上げが予定されている．HTV の物資補給先である国際宇宙ステーションは有人の実験施設であることから，運用におけるハザードには人命が関わる可能性のあるものも含まれるため，HTV の安全解析は非常に高いレベルで行われている．

HTV の安全解析は FTA と FMEA の両手法を用いて行われ，うち FTA を用いた解析結果はハザードレポートとしてまとめられている．各安全解析結果の繋がりおよび開発の成果物との関係性は 2.4 節で示したとおりである．

4.2 実験方法概要

本評価実験では 10 名程度の被験者を対象に，HTV に関する変更が特定の安全リスクに影響するかどうかについて，既存するシステムの安全解析結果を参照しながら調査していただき，複数の問題に解答していただくことを考えている．この実験においては，問題として与えた特定の変更に対する影響評価をしやすい安全解析手法を識別することが目的である．この実験の結果を比較することで，3 章で述べた 3 つの仮説を検証する予定である．

被験者は，FTA の安全解析結果を用いて問題を解くグループと，FMEA の安全解析結果を用いて問題を解くグループの 2 つに 5 名程度ずつ分けることを考えている．なお，グループ分けは対象システムや安全解析に関する知識水準に大きな偏りがないよう配慮する予定である．実験実施時間は 1 時間程度を想定している．

被験者には，解答していただく問題として「システム開発における変更」と「システムの安全解析結果」の 2 つを配布する予定である．ここで，システム開発における変更として出題する内容は，それぞれの仮説を検証できるよう以下のような内容を想定している．

- 複数コンポーネントの組み合わせの設計に対する変更 (3 章仮説 1.1 に対応)

- ハードウェア上の設計に影響する要求の変更，およびシステム内部のアルゴリズムに影響する要求の変更(同仮説 1.2 に対応)
- 単一コンポーネントの変更(同仮説 2.1 に対応)

実験で得られた回答をもとに仮説を検証する際，問題として与えた特定の変更に対して各安全解析手法の影響評価のしやすさを測る指標として，問題の正答率および被験者が問題を解くのにかかった時間を計測し，これらの指標を用いて各安全解析手法を比較・評価する予定である．

5. おわりに

本章では，まとめと今後の展望を述べる．

本研究では，変更に伴う安全解析への影響評価について，既存の安全解析手法である FTA と FMEA の間で評価のしやすさに関する差異があると考えられる仮説を立て，その理由とともに述べた．また，仮説を検証するための実験方法を示した．今後は提案した実験方法に基づいて評価実験を行って仮説を検証し，結果に対して考察を行っていきたいと考えている．

参考文献

[1] Nancy G. Leveson, John P. Thomas: STPA Handbook, http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf（2018 年 7 月 26 日）.

[2] Mirayla Goodrum, Jinghui Cheng, Ronald Metoyer, Jane Cleland-Huang, and Robyn Lutz: What Requirements Knowledge Do Developers Need to Manage Change in Safety-Critical Systems? In Proc. of RE, 2017, pp. 90–99.

[3] 鈴木順二郎，牧野鉄治，石坂茂樹: FMEA・FTA 実施法信頼性・安全性解析と評価, 日科技連出版社, 1982.

[4] Nancy G. Leveson: Safeware: System Safety and Computers, Addison-Wesley Professional, 1995.