修士論文

システム安全解析における
変更影響評価手法の改善に関する調査・検討

入江 琴子

2019年3月15日

奈良先端科学技術大学院大学
情報科学研究科

本論文は奈良先端科学技術大学院大学情報科学研究科に
修士 (工学) 授与の要件として提出した修士論文である。

入江 琴子

審査委員：

飯田 元 教授	（主指導教員）
松本 健一 教授	（副指導教員）
片平 真史 教授	（副指導教員）
石濱 直樹 准教授	（副指導教員）

システム安全解析における
変更影響評価手法の改善に関する調査・検討*

入江 琴子

内容梗概

代表的なシステム安全解析手法として，FTA (Fault Tree Analysis) や FMEA (Failure Mode and Effects Analysis) がある．安全解析手法はそれぞれ異なる特性を持っており，システムの変更に対しても特性に応じて複数の手法を用いた影響評価が実施されるのが適当である． しかし，先行研究において，変更に関する安全への影響を評価する際に，FMEA のみが頻繁に参照されていることが明らかになっている．そこで，FMEA のみを用いた変更影響評価を行う場合に発生する問題を明らかにするため，本研究では FMEA の比較対象として FTA を置き，安全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や有効性の差異といった特性が現れると考える点を仮説として立て，実験による検証を行った．実験の結果，仮説通り FMEA より FTA の方が設計や検証への変更影響評価をしやすい傾向にある点がが明らかになり，変更影響評価をする際は FMEA のみを参照するのではなく，FTA を用いた影響評価作業を行うべきであることが分かった．また，実験において変更に影響のあるハザードの番号を選択する問題で，FMEA を用いて影響分析をしたグループは，FTA を用いたグループと比べて，影響のあるハザード以外に影響のないハザードまで選択して回答してしまう，すなわち適合度が低くなる傾向がみられ，FMEA で変更影響評価をする際は，影響範囲を適切に絞り込めるよう追加で支援を行う必要があることが明らかになった．

*奈良先端科学技術大学院大学 情報科学研究科 修士論文, 2019 年 3 月 15 日.

キーワード

セーフティクリティカルシステム，安全解析，FTA，FMEA，変更影響分析

Investigation for Improving Change Impact Assesment Methods in System Safety Analysis*

Kotoko Irie

Abstract

FTA (Fault Tree Analysis) and FMEA (Failure Mode and Effects Analysis) are safety analysis methods which have been widely used. Those methods are conducted for preventing hazards, which mean system states or set of conditions that will lead to a loss. Each safety analysis method has different characteristics, and then, in safety-critical systems, safety analysis is conducted in multiple methods according to their characteristics. Therefore, it is necessary to evaluate change impact analysis on multiple safety analysis methods according to their characteristics. However, previous research has reported that only the results of FMEA have been frequently referred to when estimating the change impacts on safety analysis.

To tackle this problem, this study conducted two experiments based on hypotheses to investigate whether using only the results of FMEA in evaluating change impacts is appropriate or not. The hypotheses were built in the following way that, FTA was compared with FMEA, and they were based on the assumptions that would be possible to cause a difference in evaluating change impacts between FTA and FMEA. In the experiments, we prepared the problem about changes caused in system development corresponding with the hypotheses for experiments. Participants of the experiments are divided into two groups; one

*Master's Thesis, Graduate School of Information Science, Nara Institute of Science and Technology, March 15, 2019.

group that only used FTA results, and another group that only used FMEA results. And the participants answered the problems in evaluating the impacts of those changes on design or verification of the system with the results of each safety analysis method.

The results of impact analysis on design and verification showed the similar results with the hypotheses. This means that FTA has points with which more easily evaluate impacts than FMEA, in other words, at those points, engineers should conduct impact analysis by using not only FMEA but also FTA.

The results also showed that, in selecting the hazard number which is related to a change of the system, participants in FMEA group tended to answer hazard numbers including that were not affected by changes. This study defined precision as the ratio of the hazard numbers that are really affected by the change in all of the selected hazard numbers; In this way, we can say the results showed that using FMEA for change impact analysis lowered precision. Low precision means that engineers may conduct their work of impact analysis on design or verification without narrowing the range of the change impact, in short, it is inefficient. So, this makes it clear that additional support is needed to narrow the range of a change impact properly when using only FMEA for change impact analysis.

Keywords:

Safety Critical System, Safety Analysis, Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), Change Impact Analysis

目 次

図 目 次

表 目 次

1. はじめに

あるシステムの障害が人的または経済的に損失をもたらすことが予想される場合，そのシステムの開発と並行して安全解析が行われる [1]．安全解析は，システムの状態がハザードと呼ばれる損失に繋がる状態となることを避けるために実施される．

安全解析手法としては様々な手法が提案されており，代表的な手法として FTA (Fault Tree Analysis) や FMEA(Failure Mode and Effects Analysis) がある．安全解析手法にはそれぞれ異なる特性があり，特に安全が重要となるシステムではハザードを漏れなく識別するために特性に応じて複数の手法を用いた解析が行われるため，システムの変更に対しても特性に応じて複数の手法を参照した影響評価が実施されるのが適当である．

しかし，先行研究において，変更に関する安全解析への影響を評価する際に，FMEA のみが頻繁に参照されていることが明らかになっており [2]，複数の安全解析手法を参照した影響評価は実際には行われていない．このことによって影響の評価に漏れが発生したり，また影響評価の作業そのものが非効率的に実施されたりしている可能性がある．

そこで本研究では，現状の FMEA のみを用いた安全への変更影響評価が漏れなく，また効率的に行われているかを調査した．

具体的にはまず，FMEA とその比較対象とする FTA について，変更の影響評価のしやすさに差異が現れ特性が明らかになると考える点を仮説として立てた．このうち変更影響評価において FTA の優位性が確認できる点が実験で明らかになれば，影響評価において FMEA のみを用いることは問題であるといえると考え，このようなアプローチをとった． 次に，仮説に対応するシステムの変更を実験の問題として作成した．実施した実験では，被験者のうち半数に FTA の安全解析結果を，残りの半数に FMEA の安全解析結果を配布し，被験者には配布資料を参照しながら問題に記載されたシステムの変更による影響の評価を行ってもらった．最後に実験結果を分析し考察を行った．

以下に本論文の構成を示す．まず 2 章では，本論文の背景知識となる安全解析および安全解析手法について述べる．3 章では仮説について説明する．4 章では

本研究で実施した 2 つの評価実験について述べ，最後に 5 章で全体のまとめを述べる．

2. 背景

本章では，本研究の背景となる安全解析および安全解析手法について述べる．以降，2.1 節ではシステム開発と安全解析について述べ，そのあと 2.2 節では各安全解析手法を説明する．最後に 2.3 節では，安全解析手法の比較を行った上で，本研究の起点となる課題を述べる．

2.1 システム開発と安全解析

すべてのシステムは損失をもたらすものであってはならない．システムによる損失を防ぐため，開発者はまず現在のシステムがどの程度の損失を引き起こす可能性があるのかを把握する必要がある．特に，システムの障害が人的または経済的にきわめて大きな損失をもたらすことが予想される場合，それらは安全性の維持・確保がより重要視されるシステムと識別されセーフティクリティカルシステムと呼ばれる．セーフティクリティカルシステムの例としては，自動車や鉄道，航空機などの輸送機械や宇宙機，原子力発電などのプラントが挙げられる．セーフティクリティカルシステムでは，開発と並行して安全解析が段階的に行われる．

安全解析の最も重要な目的は，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すなわち人的損失や，物的損失，機密情報の漏洩など経済的な損失につながるようなシステムの状態または条件を指す [3]．システム開発と並行して行われる安全解析においては，発生する可能性のあるハザードを識別した上でそのハザードの影響度を評価し，開発しているシステムからそれらを除去または制御する必要がある．

図 1 に，本研究で想定する開発の成果物と安全解析の成果物の関係性を示す．

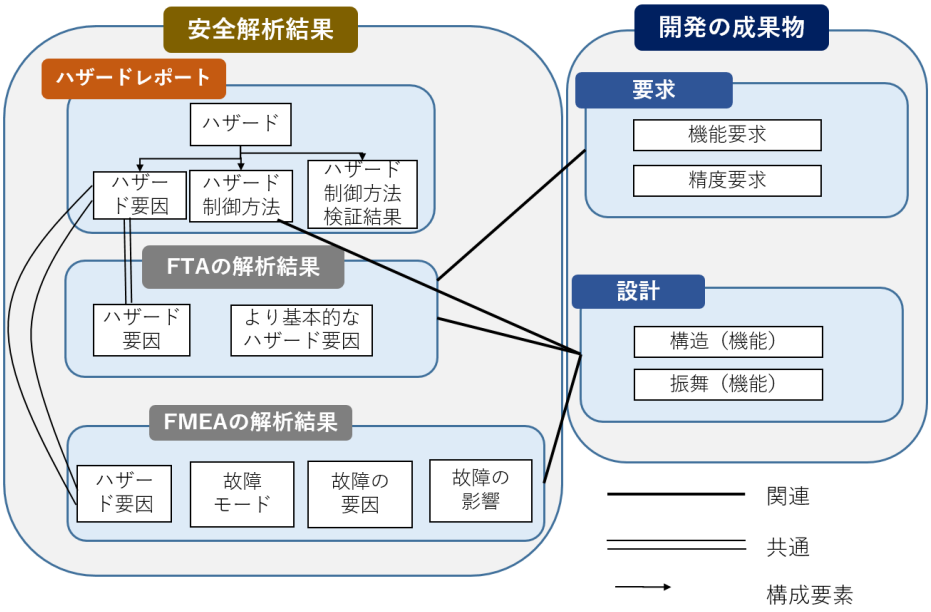

図 1　開発の成果物と安全解析の成果物の関係

この図の左側が安全解析結果，右側が開発の成果物である．安全解析手法は 2.2 節で後述する FMEA (Fault Mode and Effect Analysis) や FTA (Fault Tree Analysis) を一例として示した．まず，図 1 の実線が示すとおり，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，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確認される．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．ハザードレポートとは図 2 のような形式で，ハザードとそれを引き起こす要因が，ハザードを制御するためにとられた行為 (例：設計) と，システムがハザードを制御していることの検証方法および検証結果とともに記載された文書である．

システム＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ ハザードレベル＿＿＿＿＿＿＿＿ サブシステム＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿ 日付 ＿＿＿＿＿＿＿＿ 運用/フェーズ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿		
ハザード		
ハザード要因/前提		
ハザードの制御	状態	参照
検証方法	状態	参照
備考		

図 2 ハザードレポートの書式例 [3]

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 1 二重線).

2.2 安全解析手法

安全解析手法として提案されているものは多く，その大まかな特性に応じてさまざまな手法が実際の解析に用いられている．ここでは，現在セーフティクリティカルシステムの安全解析に頻繁に用いられている FTA (Fault Tree Analysis) と FMEA (Fault Mode and Effect Analysis) について述べる．

2.2.1 FTA (Fault Tree Analysis)

FTA は，システムにとって望ましくない事象や条件 (例：損失，ハザード) 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 [4].

図 3 で FTA の例を示す．この図では「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．図 3 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.

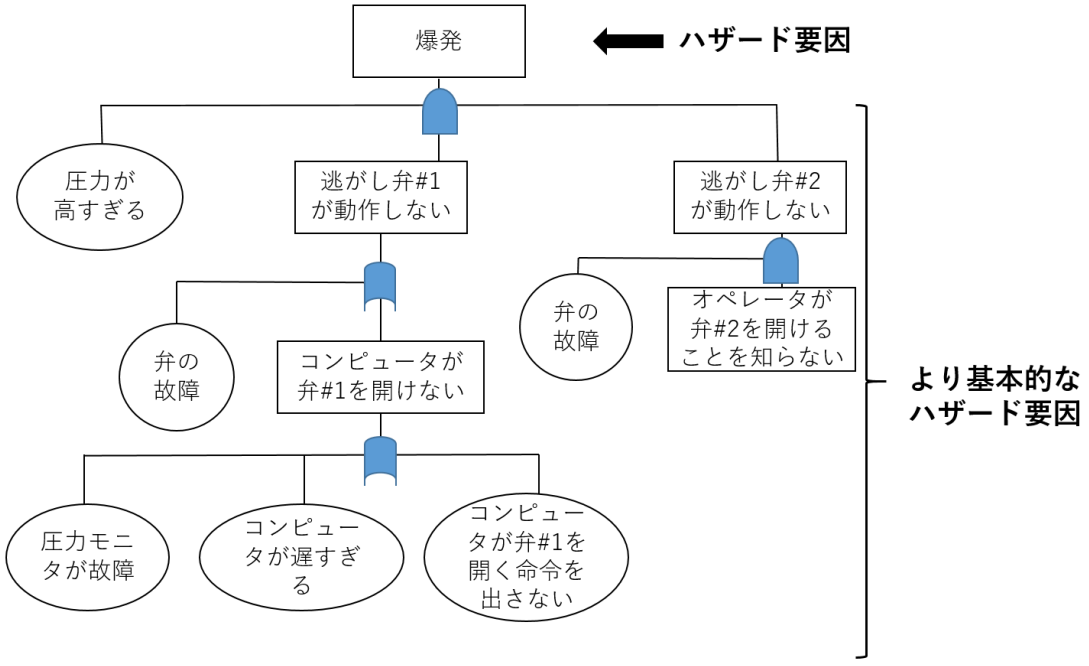

図 3 FTA の例 [3]

FTA の手順は以下のとおりである [5].

1. 故障の木構造の根となるハザードや事故や欠陥を識別する
2. 根となるノードを引き起こす事象または条件を識別してそれぞれ子ノードとし，論理演算子を用いてそれらを組み合わせる
3. 子ノードをより基本的な事象または条件に分解する
4. 事象が最小のセットになるまで (3) を繰り返す

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．

2.2.2 FMEA (Fault Mode and Effect Analysis)

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．

図 4 は 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，定義され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，この図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	故障モード	故障の要因	故障の影響を受けるハザード	ハザードに至る要因
A	断線 短絡 その他			
B	断線 短絡 その他			

図 4 FMEA の例

FMEA の手順は以下のとおりである [5].

1. 解析の対象を決める
2. 各コンポーネントの故障モードを識別する
3. 起こりうるそれぞれの故障モードについて，システムに及ぼす影響とその原因を定める
4. 各故障モードについて，それが起こった場合の致命度および起こりうる可能性をもとに対処すべき優先度を算出する

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 (例：ソフトウェア) には FMEA を適用するのが難しいと言える．

2.2.3 FTA と FMEA の比較

2.2 節で述べた FTA と FMEA の特徴をもとに，両安全解析手法を比較しまとめたものを表 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すべ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解析できる	・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

FTA と FMEA にはこのように異なる長所と短所を持っており，特性が異なることから，両方の手法を用いて安全解析を行いそれぞれの有効性を補い合えることが望ましい.

複数の安全解析手法を用いることが望ましい例として以下が挙げられる．平均的なシステムでは開発時に要求の約 25 %が変更されることが分かっている [7]. このような開発上の変更に伴って安全解析結果も再検討の必要が生じる．具体的には,

- システムの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

- システムの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．このような再検討の際に，変更の種類や各手法の特性を理解した上で参照する結果を使い分ければ再検討の効率が上がるだけでなく，より当該変更の特性に適した手法を参照することで検討事項の漏れを防ぐこともできる．

しかし実際には，システムの変更によって発生しうるハザードおよびハザードの発生要因を識別するために FMEA のみを用いた安全解析結果が頻繁に参照されている [2]．現在，特性に応じて参照する安全解析手法を使い分けることは一般的でないか，またはそれぞれの安全解析手法の特性を十分に理解しないまま行われていると考えられる．単一の手法を用いて変更影響分析を行うことは，影響の見落としや作業の非効率につながっている可能性があり，課題だと考えた．

3. 仮説

2.2.3 節で述べたとおり，システムの変更に関する安全への影響を分析する際に FMEA のみを用いた解析が頻繁に行われている．単一の手法を用いて変更影響分析を行うことは，影響の見落としや作業の非効率につながっている可能性があるが，具体的にどういった影響が見落とされるのかや，ある手法で見落とされた変更の影響が別の手法で識別できるのかについては未だ明らかになっていない．

そこで本研究では，FMEA のみを用いた変更影響分析に問題点があるという考えのもとに，仮説を立て，システム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を行った．具体的には，FMEA と共によく用いられている FTA とを比較して，FTA の方が影響評価をしやすいと考えられる点と，FMEA の方が影響評価をしやすいと考えられる点をそれぞれ挙げて仮説を立てた．これらの仮説を実験で検証し仮説が正しいことが実証されれば，FMEA のみでなく FTA も用いた変更影響分析をした方がよい点が解明できる．

以降，本章では，これらの仮説についてそれぞれ説明したうえで，仮説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とともに，2.3 節で述べた FTA と FMEA の比較結果をもとに議論を行い妥当と判断し立てた仮説である．

また，仮説の範囲は一般的に FTA や FMEA で扱うシステムレベルのものとし，ソフトウェアのソースコード上における呼出や参照といった関係の変更など，ソフトウェア内部の変更については通常 FTA や FMEA で扱う範囲ではないため対象外とした．

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： 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．一方，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．

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る．よって，対応する事象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られる仮説として以下の 1 件を得た．

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ため，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

4.1 実験の位置づけ

本研究は，3 章において述べた仮説を検証し，FTA と FMEA の変更影響分析における特性を明らかにすることを目的として，実際の宇宙機を題材とした実践的な実験と家電を題材とした実験の 2 つを実施した．これらのシステムを題材とした実験を行った理由は，FTA や FMEA を用いた安全解析が行われる複数のドメインで実験を行うことによって仮説の一般性を検証するためである．

4.2 宇宙機を題材とした実験

4.2.1 宇宙機を題材とした実験の概要

この実験はセーフティクリティカルシステムである実際の宇宙機を題材とした実践的な実験で，3 章において述べた仮説を検証し，FTA と FMEA の変更影響分析における特性を明らかにすることを目的として行った．本実験では，被験者となる JAXA 技術職員の方を対象として，安全解析に関する課題を解いてもらった．

実験対象としては，宇宙ステーション補給機こうのとり (H-II Transfer Vehicle; 以下，HTV と記載する) を選んだ．HTV は地球から約 400 km 上空の軌道上を周回する国際宇宙ステーション (International Space Station; 以下，ISS と記載する) にドッキングし，物資を送り届ける無人の宇宙機である [13]．HTV は無人の宇宙機であるが，ISS には宇宙飛行士が搭乗しているため，運用を考えて人命にかかわるハザードを考慮した安全設計・安全解析がなされている [14]．したがって，HTV は宇宙機の中でも人命の損失に関するリスクを含むセーフティクリティカルシステムであり，開発で繰り返し変更が発生しているため，実験対象とした．

本実験の被験者は 10 名で，実験では FTA の安全解析結果を用いるグループと FMEA の安全結果を用いるグループの各 5 名ずつに分けた．被験者の選出に際して，各手法に対する知識や経験が偏っている人，すなわち，FTA を業務で用いた経験は多いが FMEA に関しては未経験などの偏りがある人の選出は避け，両手法に対してある程度の知識を持った人に被験をお願いし，グループ分けにおいて

も安全解析の知識や経験に偏りがないようにした．また，実験対象のシステムとなる HTV に一定以上の知識を有する人の選出は避けた．回答時間は全問合わせて 1 時間を目安とした．

被験者には，HTV の歴代号機で実際に行われた開発・運用上の変更をもとに作成した架空の開発上の変更について，安全解析に関する資料をもとに以下の設問を解いてもらい，回答データを収集した．

- **設問** 1 変更の影響を受けるハザードはどれか (ハザード番号選択式)
- **設問** 2 変更が適用された場合，現状の設計でハザードは制御されているか否か．制御されていない場合，追加の制御としてどのようなものが考えられるか (自由記述式)
- **設問** 3 変更の適用後もハザードが制御できていることを検証する方法は現在挙げられているもので足りるか否か．現在の方法で検証できない場合，追加の検証方法としてどのようなものが考えられるか (自由記述式)

被験者に与えられた変更は 3 つで，課題は各変更に対応する大問 3 問にそれぞれ上記 3 問の設問がついて合計 9 問であった．

HTV の開発上の変更は，仮説を検証することを想定して仮説と対応付けた．以下に各大問の詳細と仮説との対応および模範回答例を示す．

大問 1 緊急時のコマンド送信元端末変更

- **詳細**:
  ISS の搭乗員は，HTV が ISS に接近する際に ISS への衝突等のハザードが起きる可能性があると判断した場合，HTV へ緊急コマンドを送信して接近を中止させることができる [14]．従来はこのコマンドを HTV 専用の端末 (Hardware Command Panel) から送信していたが，この端末をに代わり汎用のノート PC から緊急コマンドを送信することになった，という変更を想定した問題とした．なお，これは HTV7 号機で実際に採用された変更をもとに作成した [10]．

- **仮説との対応**:
  仮説 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) に対応
  仮説 1 と対応させた理由は，この変更によりコマンド応答時間が長くなり，HTV-ISS 間の近傍運用時の通信システム (PROX) 全体に影響するため [10]，コンポーネントの組み合わせレベルでの変更と捉えることができると判断したためである．

- **模範回答例**
  - **設問** 1: HTV-0008 (HTV の ISS への衝突に関するハザード)
  - **設問** 2: 現状の設計でハザードは制御されていない．ランデブ (接近) 時の運用を変更する必要がある．(近傍運用開始の位置を ISS からより遠方に設置する，ランデブ速度を小さくする等)
  - **設問** 3: 現在の検証方法で検証可能である

大問 2 レーザリフレクタの配置変更

- **詳細**:
  ISS には下部にレーザリフレクタと呼ばれるレーザ反射鏡が取り付けられている．これは HTV から照射されたレーザ光を複数のレーザリフレクタが反射することで，ISS と HTV の間の距離を測定して接近時の誘導制御にフィードバックするための装置である．このレーザリフレクタの配置が変更されたことを想定した問題として本大問を作成した． なお，これは HTV5 号機で実際に採用された変更をもとに作成した [11].

- **仮説との対応**:
  仮説 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) に対応
  仮説 2 と対応させるにあたり，この変更について「現在のレーザリフレクタの配置では距離を誤検知するおそれがあり，配置を変更するこ

とになった」という理由付けを行った．この変更により，誘導制御アルゴリズムを従来のものから変更する必要があり，設計に影響する．

- 回答例
  - **設問** 1: HTV-0008 (HTV の ISS への衝突に関するハザード)
  - **設問** 2: 現状の設計でハザードは制御されていない．誘導制御アルゴリズムを変更する必要がある．
  - **設問** 3: 現在の検証方法で検証可能である

大問 3 推進系の変更

- 詳細

  HTV の推進系は，主に推力を得るためのメインエンジンと姿勢制御用に用いられるスラスタで構成される．このスラスタを従来の型のものから新規開発されたものへ変更するという想定で本問題を作成した．なお，これは HTV3 号機で実際に採用されたスラスタの変更をもとに作成した [12].

- 仮説との対応

  仮説 3(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) に対応

  スラスタを含めた推進系では，ISS 衝突安全および再突入安全のため，ミッションを通じてタンク内にある推薬量の把握が必要である [15]．スラスタを新型のものへ変更することにより，残推薬量計算のためのアルゴリズムを変更する必要があり，設計に影響する．

- 回答例
  - **設問** 1 HTV-0008 (HTV の ISS への衝突に関するハザード)
  - **設問** 2 現状の設計でハザードは制御されていない．残推薬推定のためのアルゴリズムを変更する必要がある
  - **設問** 3 現在の検証方法で検証可能である

4.2.2 宇宙機を題材とした実験における結果

前節で述べた実験の結果を以下に示す.

まず，設問 1 (変更の影響を受けるハザードがどれか番号選択式で回答させる設問) について，各大問ごとの正答率を表 5 と表 8 に示す.

表 2 設問 1 平均正答率比較

	FTA グループ	FMEA グループ
大問 1	100 %	100 %
大問 2	100 %	100 %
大問 3	100 %	100 %

FTA を用いて安全への影響評価をしたグループと，FMEA を用いて影響評価をしたグループでは，正答率に大きな差はなかったが，適合率に大きな差が表れた．仮説で予想した変更の種類による各安全解析手法ごとの影響評価のしやすさに反して，適合率はすべての大問において FMEA のグループの方が低い結果となった.

次に，設問 2(設計への影響を自由記述式で回答させる設問) と設問 3 (検証方法への影響を自由記述式で回答させる設問) の採点結果を表 6 と表 9 に示す.

なお，設問 2 と設問 3 に関しては，採点を以下の基準で行った.

- 空欄もしくは影響の有無・根拠ともに不正解：0 点
- 影響の有無のみ正解：1 点
- 影響の有無と根拠の両方が正解：3 点 (傾斜配点)

4.2.3 宇宙機を題材とした実験における考察

本節では，前節で述べた実験結果をもとに考察を行う.

表 3 設問 2 結果比較

	FTA グループ 合計点	FMEA グループ 合計点
大問 1	8	2
大問 2	7	3
大問 3	7	10

表 4 設問 3 結果比較

	FTA グループ 合計点	FMEA グループ 合計点
大問 1	10	6
大問 2	9	4
大問 3	5	10

大問 1 に関する考察

コンポーネントの組み合わせレベルでの変更を出題した大問 1 の結果は，他の 2 つの大問と比べると，表 3 に示すとおり，特に設計に関する変更の影響を問う設問 2 で FTA を用いたグループと FMEA を用いたグループの差が大きく表れ，FTA を用いたグループの方が得点が高い結果となった．大問 1 は FTA を用いた方が影響評価をしやすいと予想した仮説 1 と対応するため，本結果は仮説に沿ったものとなった．

仮説に沿った結果が得られた理由として，影響を受けるサブシステムを特定しやすかったことが考えられる．FTA を用いて影響評価をした被験者グループには，自由記述で「誘導制御系への影響」という観点から設計・検証への影響を考えることができている被験者が多かった．すなわち，被験者が影響を受けるサブシステムを的確に特定した上で分析作業を進められたことで正答に繋がりやすかったと考えられる．この要因として，仮説 1 を立てる際に予想したとおり，FTA の上位事象にコンポーネントの組み合わせとしてのサブシステムレベルのノードが存在するため，変更と対応するサブシステムを発見すればその後の影響分析を進めやすいことが推測される．

一方，FMEA を用いた場合はコンポーネントの故障モードから影響分析を始めることになる．FMEA にはコンポーネントの故障がサブシステムおよびシステム全体に及ぼす影響に関する情報も記載されているが，コンポーネントを始点としたトレースでは限られた時間の中でサブシステムに関する情報まで追うことが難しかったのではないかと考えられる．

大問 2 に関する考察

システムの要求レベルから発生した変更を出題した大問 2 の結果は，設計や検証への変更影響を問うた設問 2 と設問 3 では，それぞれ表 3 と表 4 に示すとおり，FTA を用いたグループの方が得点が高かった．大問 2 は FTA を用いた方が影響評価しやすいと予想した仮説 2 と対応しているため，結果は仮説に沿ったものとなったが，FTA を用いたグループと FMEA を用いたグループの得点差は期待されたものより小さかった．

この理由として，実験で使用した変更がコンポーネントレベルに近い変更とも読み取れたことが考えられる．大問 2 では，レーザリフレクタの配置変更を題材に出題した．この変更の影響がレーザリフレクタそのもの以外にも及ぶこと，また要求レベルから発生した変更であることを示す理由付けを行ったことで，仮説 2 に基づき FTA を用いた方が影響評価がしやすいと予想された．しかし，レーザリフレクタが HTV の ISS 近傍運用時の誘導制御の用途で用いられることは，FMEA のコンポーネント情報を参照しても知ることができるため，コンポーネントを解析の始点として大問 2 を解いても一定レベルの影響評価を行うことができたのではないかと考えられる．

本問は FTA と FMEA の両方で一定レベル以上の優位性が出る問題となっており，両者の差異を明確に識別するという点では適切といえなかった可能性がある．このことから，家電を題材とした実験では差異を明確にできるよう作問した．

大問 3 に関する考察

大問 3 の結果は，設問 2，3 の設計や検証への変更影響を問う課題では FMEA を用いたグループの方が得点が高かった．大問 3 はコンポーネント単位での変更に関する問題であり，FMEA を用いた方が影響評価しやすいと予想した仮説 3 と対応するため，仮説に沿ったものであったが，FTA を用いたグループと FMEA を用いたグループの得点差は期待されたものより小さかった．

この理由として，FMEA に記載のコンポーネント情報に近いものが FTA からも読み取れることが考えられる．FTA は木構造の根となるトップ事象にシステム全体のレベルのハザードが記述されており，より基本的な下位の事象であればあるほどハザード要因が分解される．すなわち，FTA の下位事象にはコンポーネントレベルに近いハザードの要因が記述されている場合がある．大問 3 はこの場合にあたり，一定レベルの変更影響評価が FTA でも行えたのではないかと推測される．

一方で，FTA の下位事象がコンポーネントレベルまで分解されている保証はなく，FMEA に記載されているようなコンポーネント情報が必ず FTA にも記載されているわけではない．すなわち，FMEA のコンポーネント情報が全て FTA に記載されているということはないため，FMEA のコンポーネント情報を直接参照することにも十分な意義があると考えられる．

また，設問 1 の適合率に関しては，表 3 に示すとおり FTA を用いたグループの方が適合率が高い結果となった．適合率は，設問 1 の被験者の回答に書かれたハザード番号の総数のうち，正解となる番号が占める割合を示すものである．仮説 1〜3 で各安全解析手法の有効性を予想し，大問 1，2 では FTA を影響評価に用いたグループの方が適合率が高く，大問 3 では FMEA を用いたグループの方が適合率が高いと考えたが，実際には大問 3 で仮説に反して FTA を用いたグループの方が適合率が高い結果となった．

4.3 家電を題材とした実験

4.3.1 家電を題材とした実験の概要

この実験は家電を題材とした実験で，3 章において述べた仮説を検証し，FTA と FMEA の変更影響分析における特性を明らかにすることを目的として行った．本実験では，被験者となる奈良先端科学技術大学院大学の修士学生 6 名を対象として，安全解析に関する課題を解いてもらった．

実験対象としては，架空の電子レンジに関する仕様書と安全解析結果を作成し

実験で使用した．本実験の被験者 6 名は，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各 3 名ずつに分けた．被験者の選出に際して，全被験者が安全解析に関しては初心者であったが，システムに関して一定以上の理解力を有する情報科学を専攻する学生を選出した．また学年などが偏らないよう留意して知識の偏りがないようにした．回答時間は全問合わせて 1 時間を目安とした．　被験者には，実験対象となる架空のシステムにおける開発上の変更について，安全解析に関する資料をもとに以下の設問を解いてもらい，回答データを収集した．

- **設問** 1 変更の影響を受けるハザードはどれか (ハザード番号選択式)
- **設問** 2 変更が適用された場合，現状の設計でハザードは制御されているか否か．制御されていない場合，追加の制御としてどのようなものが考えられるか (自由記述式)
- **設問** 3 変更の適用後もハザードが制御できていることを検証する方法は現在挙げられているもので足りるか否か．現在の方法で検証できない場合，追加の検証方法としてどのようなものが考えられるか (自由記述式)

被験者に与えられた変更は 3 つで，課題は各変更に対応する大問 3 問にそれぞれ上記 3 問の設問がついて合計 9 問であった．

開発上の変更は，仮説を検証することを想定して仮説と対応付けた．以下に各大問の詳細と仮説との対応および模範回答例を示す．

大問 1 マイクロ波誤射防止に関する変更

- **詳細**:
  電子レンジはマイクロ波を被加熱物に照射することで加熱を行う．加熱実施中に電子レンジのドアを開け，同時に加熱開始ボタンを押すと，ドアが開いたままなのに加熱処理が開始し停止せず継続されてしまい，マイクロ波が外部に多量に漏れるおそれがありハザードとなるため，ドアオープンの異常検知が稼働した場合は必ず「加熱が継続して行われていないか」を確認するエラーチェックと連携させることとした．す

なわち，加熱中にドアが開く異常検知の終了とエラーチェックの稼働を 50ms の間隔で行う，という変更を想定した．

- **仮説との対応**:
  仮説 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) に対応
  ドア開閉の検知とエラーチェックという 2 つの機能を組み合わせたものと考え，仮説 1 と対応付けた．
- **模範回答例**
  - **設問** 1: 2(マイクロ波漏洩)
  - **設問** 2: 現状の設計でハザードは制御されていない．マイクロ波照射機構がエラーチェックの結果 OFF になるよう設計すべきである．
  - **設問** 3: ドアオープンと同時に操作をした際に異常処理とエラーチェックが連携するか検証する必要がある

大問 2 連続異常への対処

- **詳細**:
  対象システムとなる電子レンジにおいて異常対応処理が連続した場合，前に発生した異常に対する処理が完了しないままとなることが分かり，前タスクに異常検知が稼働している場合は該当処理が完了した後に新たな異常に対応する処理を稼働させるようにする，という変更を想定した．
- **仮説との対応**:
  仮説 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) に対応
  異常処理を行いハザードを制御することはシステムの安全要求を満たす条件となるため，本変更を仮説 2 と対応付けた．
- **模範回答例**
  - **設問** 1: 1(過加熱)，2(マイクロ波漏洩)

- **設問** 2: 現状の設計でハザードは制御されていない．タスク処理にかかる時間等を考慮し各タスクに優先度を設定した上で本変更を適用すべきである
- **設問** 3: すべての異常検知機能 (ドア展開，温度センサ異常等) を組み合わせて稼働させ，一方のタスクの処理が完了しないという事象が発生しないことを検証する必要がある

大問 3 ターンテーブルの重量変更

- **詳細**:
  ターンテーブルは電子レンジ内部で被加熱物を加熱中に水平方向に回転させ，被加熱物が均等に温まるようにするものである．このターンテーブルの素材変更によりターンテーブルの重量が変わった，という変更を想定した．
- **仮説との対応**:
  仮説 3(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) に対応
  ターンテーブル単体に関する変更であるため，仮説 3 と対応付けた．
- **模範回答例**
  - **設問** 1: 1 (過加熱)
  - **設問** 2: 現状の設計でハザードは制御されていない．ソフトウェアにおいてターンテーブルの重量を書き換える必要がある
  - **設問** 3: 現在の検証方法で検証可能である

4.3.2 家電を題材とした実験における結果

前節で述べた実験を実施した結果を以下に示す．

まず，設問 1 (変更の影響を受けるハザードがどれか番号選択式で回答させる設問) について，各大問ごとの正答率を表 5 と表 8 に示す．

表 5 設問 1 平均正答率比較

	FTA グループ	FMEA グループ
大問 1	100 %	67 %
大問 2	83 %	67 %
大問 3	100 %	67 %

次に，設問 2(設計への影響を自由記述式で回答させる設問) と設問 3 (検証方法への影響を自由記述式で回答させる設問) の採点結果を表 6 と表 9 に示す.

なお，設問 2 と設問 3 に関しては，採点を以下の基準で行った.

- 空欄もしくは影響の有無・根拠ともに不正解：0 点
- 影響の有無のみ正解：1 点
- 影響の有無と根拠の両方が正解：3 点 (傾斜配点)

表 6 設問 2 結果比較

	FTA グループ 合計点	FMEA グループ 合計点
大問 1	5	1
大問 2	7	3
大問 3	6	7

表 7 設問 3 結果比較

	FTA グループ 合計点	FMEA グループ 合計点
大問 1	7	2
大問 2	7	0
大問 3	1	3

4.3.3 家電を題材とした実験における考察

家電を題材とした実験において，設計や検証への影響に関する設問 2 と設問 3 では，それぞれ表 6 と表 7 で示すとおり，結果が仮説で予想した変更影響評価に

おける有効性に沿った傾向を示した．ただし大問3については，結果は仮説に沿った傾向を示したが，FTA を用いたグループと FMEA を用いたグループの得点差が期待したよりも小さかった．この理由として，宇宙機を題材とした実験と同じく，FMEA に記載のコンポーネント情報に近いものが FTA からも読み取れることが考えられる．また，大問2については，宇宙機を題材とした実験で両安全手法ともに一定以上の優位性が出る問題となっていたため，家電を題材とした実験では両者の差異をより明確に識別できるよう作問したところ，仮説に沿った差異を示す結果となった．

4.4 総合考察

宇宙機，家電の両題材を対象とした実験において，設計や検証への影響を自由記述させる設問では仮説で予想した FTA と FMEA の変更影響評価における有効性の傾向を示す結果が得られた．これらの結果から，システムに求められる安全のレベルやドメインには関係なく，両安全解析手法が仮説で予想した各変更点への有効性を実際に持っていると考えられる．すなわち，FTA と FMEA がシステムの安全解析に用いられている場合，現在頻繁に行われているような FMEA のみを用いた変更影響評価は必ずしも適切ではなく，FTA の方が影響評価に有効性を持つ変更点では FTA を用いた設計・検証への影響評価作業を行うべきであるといえる．

また，両実験の設問1の結果について適合率という指標で評価を行ったところ，以下のような結果が得られた．なお，適合率は被験者の回答に書かれたハザード番号の総数のうち正解となる番号が占める割合を示す．例えば正解となるハザード番号が「1」のみの場合,「1，3，5」という回答については，正解である「1」が含まれているので正答率は 100 %となるが，正解でない，すなわち変更の影響を受けないハザード番号も回答に含まれているため，適合率は $1/3 = 33$ %となる．つまり，適合率は (影響のあるハザード番号の総数/選択したハザード番号の総数)*100 (%) で表される．

変更に影響のあるハザードの適合率については，両実験ともにすべての大問に

表 8　宇宙機実験設問 1 平均適合率比較

	FTA グループ	FMEA グループ
大問 1	100 %	65 %
大問 2	100 %	80 %
大問 3	69 %	46 %

表 9 家電実験設問 1 平均適合率比較

	FTA グループ	FMEA グループ
大問 1	100 %	28 %
大問 2	61 %	50 %
大問 3	67 %	67 %

おいて FMEA の有効性が FTA を上回らなかった．この理由を考察すると，FMEA を用いたグループの被験者が，FMEA で変更に関連するコンポーネントに紐付けられたハザードの番号をすべて羅列していたことが推測される．例えば，スラスタに関する変更の場合,「スラスタ」というコンポーネント項目に記述されている番号のハザードがすべて変更の影響を受ける可能性を含むと考えてしまい，記載されたすべての番号のハザードについて総当たりで影響分析作業に入ったのではないかと考えられる．すなわち，限られた時間内で「ハザードに影響があるかどうか」という視点から関連するハザードの番号を絞り込むことが難しいと考えられる．また，今回の調査は実験という環境で時間を区切って影響評価を行ってもらったため，その結果 FMEA を用いたグループの適合率が低く出た可能性も考えられる．

適合率が高いことは，変更の影響範囲を最初から適切に絞り込み効率的に安全解析を行うことであり，重要である．変更の影響範囲を広く識別することは，影響の見落としを防ぐほか，影響がなかった箇所についても，影響がないことを確認できた分析結果が残るためエビデンスを残す意味でも有効であるが，影響を分析する上で必要十分な範囲を超えて参照範囲を広げることは，分析作業の効率を下げ，限られた時間の中で分析をするという観点からいえばかえって影響の見落としを招く可能性があると考える．取り扱う変更の影響範囲を最初からある程度適切に絞り込んで参照することができれば，結果的に限られた時間で変更の影響を適切に絞り込むことにつながり，影響分析の作業効率を上げる上で有用といえる．以上のことから，FMEA で変更影響評価をしやすいコンポーネント単位での変更

についても，参照する影響範囲をある程度絞り込んで適合率を上げるため，追加の支援を検討する必要があると考えられる．追加の支援方法の例としては，本研究の範囲であれば FTA を部分的に併用して参照し変更の影響範囲を絞り込むことなどが考えられるが，近年安全解析における使用が進んでいる STPA (System Theoretic Process Analysis)[14] なども損失やハザードを起点として解析を行う安全解析手法であり，FMEA と併用して変更の影響範囲を絞り込むうえで有効ではないかと考えられ，さらなる発展が期待される．

5. おわりに

本研究では，FMEA という単一の安全解析手法を用いた変更影響評価を行う場合に発生する問題を明らかにするため，FMEA の比較対象として FTA を置き，安全解析への影響評価において 2 つの安全解析手法の間に有効性の差異が現れると考える点を仮説として立てて実験での仮説検証を行った．実験の結果，変更が設計や検証におよぼす影響を問う問題において結果が仮説に沿った傾向を示した．すなわち，FTA を用いて影響分析をした方が有効な変更点と，FMEA を用いて影響分析をした方が有効な変更点を明らかにすることができた．このことから，システムの安全解析に FTA と FMEA が使われている場合，FTA の方が影響評価をしやすい傾向にある変更点では FTA を用いた影響評価作業を行うべきであり，FMEA のみを用いた変更影響評価を行うことは適切ではないといえる．また，FMEA を用いた影響評価では，変更に影響のあるハザードを選択回答した際の適合率が出題したすべての変更において FTA より低かった．このことから，影響評価を行う場合には，FMEA で設計や検証への影響評価をしやすいコンポーネント単位での変更についても，FMEA を参照するだけでなく，影響範囲をある程度絞り込んで適合率を上げるために追加の支援を行う必要があると考えられることが分かった．

謝辞

本研究を進めるにあたり，ご指導，ご協力いただきました方々に心より御礼申し上げます．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア設計学研究室 飯田元 教授 には，日々の研究活動を通して，研究に対する姿勢から論文のまとめ方，発表の仕方にいたるまで多岐にわたり助言をいただきました．厚く御礼申し上げます．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 超高信頼ソフトウエアシステム検証学研究室 (宇宙航空研究開発機構 第三研究ユニット) 片平 真史 教授 には，2 年間一貫して様々な知見から研究に関するご指導をいただきました．ここに感謝の意を表します．また，学部では情報系専攻でなくソフトウェア工学の知識が浅かった私を研究室に受け入れて下さったことを心より感謝いたします．入学当初，知識も何もない状態で「開発の問題を解決したい」とお話しさせていただいたとき，真剣に耳を傾けてくださったことを今でも覚えております．2 年経っても至らぬ点は多いままですが，入学時の気持ちを忘れず，学んだことを生かして社会人生活を送りたいと思います．本当にありがとうございました．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア工学研究室 松本健一 教授 には，研究をまとめるにあたり大変貴重なご意見をいただきました．厚く御礼申し上げます．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 超高信頼ソフトウエアシステム検証学研究室 (宇宙航空研究開発機構 第三研究ユニット) 石濱 直樹 准教授 には，研究の進め方やまとめ方について数多くの助言をいただきました．特に評価実験の際は，お忙しい中実験の準備など多大なご尽力を賜り大変お世話になりました．深く感謝申し上げます．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア設計学研究室 市川昊平 准教授 には，研究に関する有意義な質問を数多くいただいたほか，発表の仕方や発表資料のまとめ方についても多くのご指導を賜りました．また情報処理学会に関しましては大変お世話になりました．厚く御礼申し上げます．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア設計学研究室 高井利憲 准教授 には，安全解析に関する知見から多くのご意見をいただきました．また視野を広げる意味で研究会への参加を勧めていただくなど，ご配慮を賜りました．心より感謝いたします．

奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域 ソフトウェア設計学研究室 崔恩瀞 助教 には，研究の方針や内容，論文の書き方に関する数多くの相談に乗っていただきました．深く感謝申し上げます．また，研究の内容に関してだけでなく，研究や就職活動などで精神的にプレッシャーを感じた際に支えていただいたことにも大変感謝しております．

川口真司 先生 には，研究の方向性を検討する中で多くの助言を賜りました．また厳しくも温かいご指導のおかげでソフトウェア工学のみならず情報系全体の知識を深めることができました．心より御礼申し上げます．

有人宇宙システム株式会社 柿本和希 様 には，研究に関して数多くのご助言をいただいただけでなく，同じ超高信頼ソフトウエアシステム検証学研究室の卒業生として行き届いたご指導を賜りました．心より感謝を申し上げます．

宇宙航空研究開発機構 第三研究ユニットの皆様 には，つくばでの研究活動の際にいつも温かく迎えていただきました．厚く御礼申し上げます．特に大久保梨思子 様には細やかなお心遣いを賜りました．心より感謝いたします．また，実験の際に被験者としてご協力くださった皆様には，大変貴重なデータをいただきました．本当にありがとうございました．

奈良先端科学技術大学院大学 小川暁子 様，仲田綾奈 様 には，研究出張の際の事務処理などで大変お世話になりました．また，お忙しい中でも「研究に疲れたらいつでも話しに来てくださいね」と心が和らぐようご配慮いただいたことが印象に残っています．心より感謝申し上げます．

就職担当の浜田真理 様 には，就職活動と並行して研究を進められるようにとのお心遣いから，就職活動中に様々なご支援を賜りました．心より御礼申し上げます．

ソフトウェア設計学研究室および超高信頼ソフトウエアシステム検証学研究室の皆様 には，実験の被験者となっていただいたほか，研究室生活を通して多くの

ことを学ばせていただきました．感謝申し上げます．特に博士後期課程の上村恭平 様 には論文の添削や研究に関するご指導のみならず，就職の相談など多岐にわたりお世話になりました．心より感謝しております．また，超高信頼ソフトウエアシステム検証学研究室の後輩である辻光顕 様 には，日々の研究に関する議論を行う中で多くの気づきを与えていただきました．ありがとうございました．

最後に，超高信頼ソフトウエアシステム検証学研究室に配属されたとき誰よりも喜んでくれ，また様々な面で支えてくれた母，大学院で外部進学という選択をしても何も言わず経済的に支えてくれた父，そして亡き祖母に心から感謝の意を表して，謝辞とさせていただきます．

参考文献

[1] Nancy G. Leveson, John P. Thomas: STPA Handbook, http://psas.scripts.mit.edu/home （2019 年 1 月 31 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] Nancy G. Leveson: Safeware: System Safety and Computers, Addison-Wesley Professional, 1995.

[4] 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.

[5] Asim Abdulkhaleq, Stefan Wagner: A Controlled Experiment for the Empirical Evaluatoin of Safety Analysis for Safety-Critical Software, 2015

[6] Xiangyu Han, Jun Zhang: A Combined Analysis Method of FMEA and FTA for Improving The Safety Analysis Quality of Safety-Critical Software: 2013 IEEE International Conference on Granular Computing (GrC)

[7] スティーブ・マコネル: (株) クイープ訳: CODE COMPLETE 第 2 版 上 完全なプログラミングを目指して，日経 BP ソフトプレス，2005

[8] Jerod W. Wilkerson: A Software Change Impact Analysis Taxonomy，28th IEEE International Conference on Software Maintenance，2012

[9] Nancy G.Leveson: Engineering a Safer World, http://sunnyday.mit.edu/safer-world.pdf (2019 年 1 月 31 日)

[10] 宇宙ステーション補給機「こうのとり」7 号機 (HTV7) に係る安全対策について (調査審議結果) (案) http://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu2/059/shiryo/__icsFiles/afieldfile/2018/07/05/1406375_1.pdf (2019 年 1 月 31 日)

[11] 宇宙ステーション補給機「こうのとり」5 号機 (HTV5) の接近・係留・離脱フェーズに係る安全検証結果について
http://www.mext.go.jp/component/b_menu/shingi/toushin/__icsFiles/afieldfile/2015/08/03/1344577_2.pdf (2019 年 1 月 31 日現在)

[12] 宇宙ステーション補給機「こうのとり」3 号機 (HTV3) の再突入に係る安全評価について
http://www.mext.go.jp/b_menu/shingi/uchuu/017/001/gijiroku/__icsFiles/afieldfile/2012/04/23/1319491_02.pdf (2019 年 1 月 31 日現在)

[13] 宇宙ステーション補給機「こうのとり」7 号機 (HTV7) 【ミッションプレスキット】，国立研究開発法人宇宙航空研究開発機構，2018 年 7 月 20 日初版

[14] Takuto Ishimatsu, Nancy G.leveson, John P. Thomas, Cody H.Fleming, Masafumi Katahira, Yuko Miyamoto, Ryo Ujiie, Haruka Nakao, Nobuyuki Hoshino: Hazard Analysis of Complex Spacecraft using Systems-Theoretic Process Analysis, Journal of Spacecraft and Rockets, Vol. 51, No. 2 (2014), pp. 509-522

[15] 中井 俊一郎，椎木泰三，山本美緒，奥寺裕之，石崎真一郎: HTV (宇宙ステーション補給機) 推進系の開発，IHI 技報 Vol.49 No.3 (2009) pp.143-149

[16] Todd Sedano, Paul Ralph, Cecile Peraire: Software Development Waste: 2017 IEEE/ACM 39th International Conference on Software Engineering

[17] L.C.Briand, Y.Labiche, O'Sullivan: Impact Analysis and Change Management of UML Models: Proceedings of the International Conference on Software Maintenance(ICSM 03)

[18] Chetan Arora, Mehrdad Sabetzadeh, Arda Goknil, Lionel C. Briand: Change Impact Analysis for Natural Language Requirements; An NLP Approach: Requirements Engineering Conference (RE), 2015 IEEE 23rd International

[19] Alheri Longji Dakwat, Emilia Villani: System Safety Assesment Based on STPA and Model Checking: Safety Science 109 (2018)130-143

[20] JAXA　IV & V 教育教材　電子レンジ仕様書, JAXA

発表リスト

[1] 入江琴子，片平真史，石濱直樹，柿本和希，崔恩瀞，飯田元，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，2018 年度 情報処理学会関西支部大会，2018 年 9 月

付録

A. HTV の概要

B. 宇宙機を題材とした実験で使用した資料

C. 家電を題材とした実験で使用した資料

A. HTV の概要

宇宙ステーション補給機こうのとり (H-II Transfer Vehible;HTV) は地球から約 400km 上空の軌道上を周回する国際宇宙ステーション (International Space Station;ISS) にドッキングし，食料，水，酸素，ISS で行う実験装置などの物資を送り届ける無人の宇宙機である [13].

A.1 HTV のシステム構成

HTV は，図 5 のとおり「補給キャリア与圧部」「補給キャリア非与圧部」「曝露パレット」「電気モジュール」「推進モジュール」から構成される.

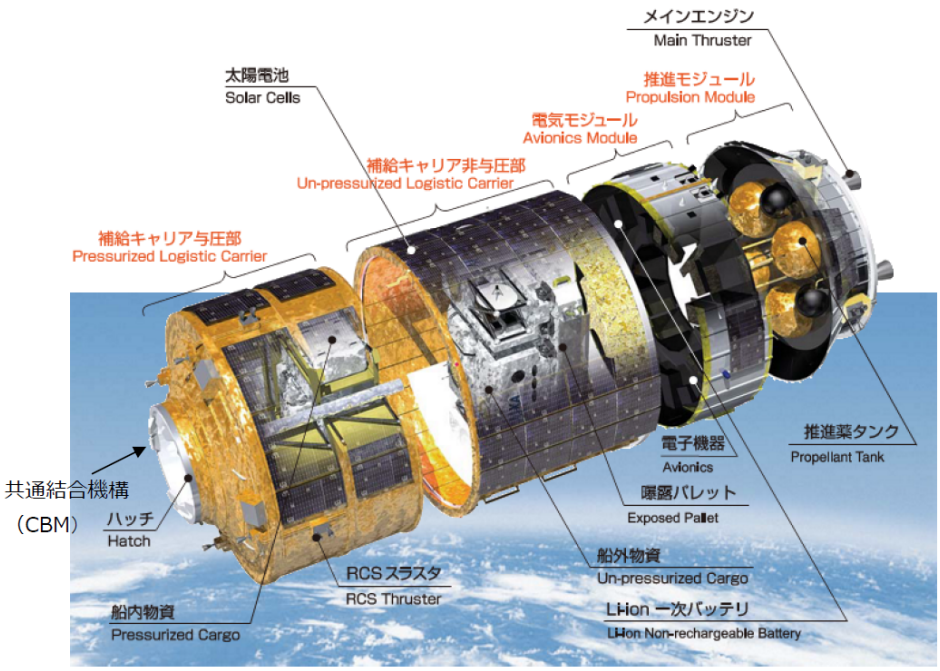

図 5 HTV のシステム構成

HTV の主要諸元は以下である.

表 10 HTV の主要緒言

項目	仕様
全長	約 10.0 m
直径	約 4.4 m
補給品を除いた機体の質量	約 10.5 トン
総質量	最大 16.5 トン
推進薬	燃料：MMH (モノメチルヒドラジン) 酸化剤：MON-3 (一酸化窒素添加四酸化二窒素)
補給能力	合計　最大約 6 トン 与圧部：船内物資　最大約 4.1 トン (ISS クルーの食料，衣服，飲料水，実験ラック，実験用品など，船内で使用する物資等を搭載) 非与圧部：船外物資　最大約 1.9 トン (船外実験装置や ISS 船外で使用される交換機器等を搭載)
廃棄品搭載能力	最大約 6 トン
目標軌道	高度：350 km〜460 km 軌道傾斜角：約 51.6 度
ミッション期間	ランデブ飛行期間：通常 5 日間 ISS 滞在期間：最長 45 日間 軌道上緊急待機期間：最長 7 日間

ここでは，実験で出題した電気モジュールと推進モジュール，そして ISS 側に設置されている HTV と ISS の近傍通信システム PROX について説明する．

電気モジュール

電気モジュールは，誘導制御，通信，電力系などの電子機器を搭載し，自律的あるいは地上からの指令に従ってHTVの広報制御を行う．また，HTV各部への電力供給を行う．
電気モジュールのサブシステムを以下に列挙する．

航法誘導制御系

- HTVの軌道投入後，位置・姿勢センサを用いて航法情報を入手し，地上からのコマンドで，HTVの単独飛行を実施するためのシステムである．
- 主に，GPSアンテナ，ランデブセンサ，地球センサ，誘導制御コンピュータなどから構成されている．
- ISSの下部にはレーザレーダリフレクタ (反射器) と呼ばれるレーザ反射鏡がついている．HTVがISSの下方 (地球方向) から接近する際にHTVのランデブセンサから照射されたレーザ光を反射することでISSとHTVの間の距離を測定し，それに基づいて航法誘導制御を行う．

通信系

- データ中継衛星を介して地上局と通信を行うための衛星間通信装置と，ISS近辺にてISSと通信を行うための近傍通信装置から構成されている．

データ処理系

- コマンド受信，テレメトリ送信機能を有する．
- 電気モジュール・推進モジュールの熱制御，補給キャリア与圧部の環境制御，HTV各所の異常検知・通知等，他サブシステムのデータ処理を支援する．

電力系

- 日照時に太陽電池パネルで発電した電力を制御して各部に提供するとともに，余剰電力をバッテリに蓄電する．
- 日陰時にはバッテリから HTV 各部に電力を供給する．
- ISS とドッキングしている間は ISS から電力が供給されるが，電力供給が途絶えた場合はバッテリの電力を各部に投入する．

太陽電池

- 日照時に発電を行う．
- HTV7 号機には計 48 枚の太陽電池パネルが搭載されている．

A.1.1 推進モジュール

推進モジュールは，4 基のメインエンジン (2 基× 2 系統) および 28 基の姿勢制御用のスラスタと呼ばれるエンジン (14 基× 2 系統) に推進薬が供給され，電気モジュールから送られてくる信号に従って，軌道変更や姿勢制御のための推力を発生する．

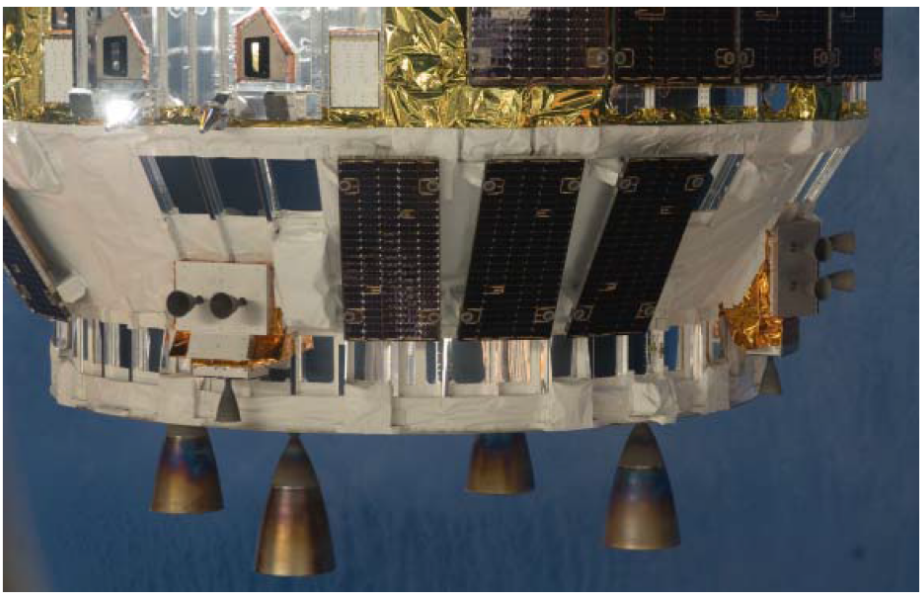

図 6 推進モジュール外観

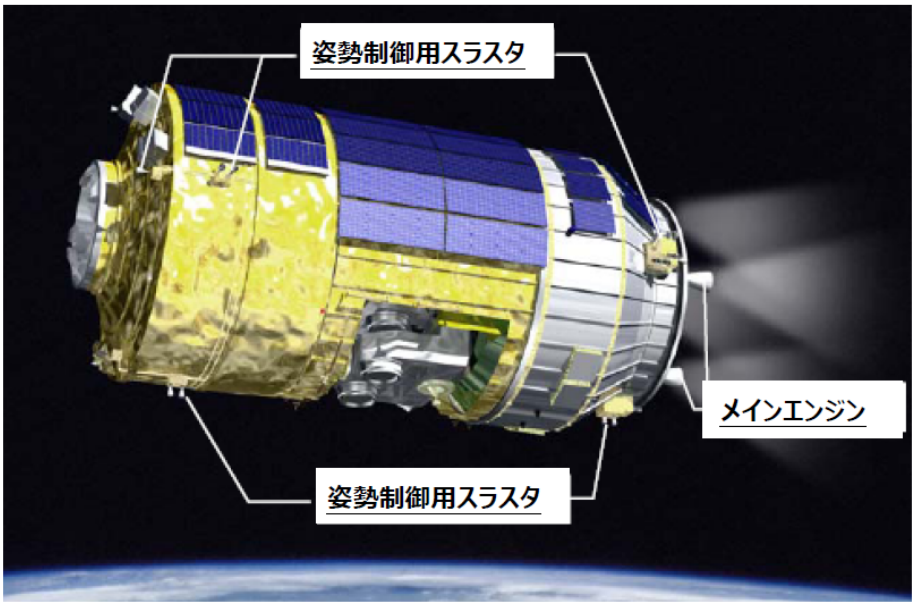

図 7 メインエンジンとスラスタの配置

A.1.2 近傍通信システム

HTV 近傍通信システム (Proximity Communication System;PROX) は，HTV が ISS と通信するための無線通信装置であり，ISS 側に設置されている．
PROX は通信，データ処理，GPS 各機器，ISS 搭乗員が HTV にコマンドを送るための装置，通信アンテナ，GPS アンテナで構成されている．
ISS 搭乗員が HTV にコマンドを送るための装置としては，図 8 のような搭乗員用コマンドパネル (Hardware Control Panel;HCP) が使われてきた．これは HTV の近傍運用中異常が発生した際に HTV に接近中止コマンドを送信するなど，緊急性の高いコマンドを HCP のボタンを押すことで HTV に送信できる機能をもつ操作パネルである．しかし，HTV7 号機では HCP の運用を止め，ISS で用いられているノートパソコンが緊急コマンドの送信装置として使用された．

図 8 搭乗員用コマンドパネル (HCP)

A.2 HTV の運用

HTV の運用は以下のフェーズから構成されている.

打ち上げ

- HTV が H-IIB ロケットに搭載されて打ち上げられるフェーズ

ランデブ

- 高度を徐々に上げながら ISS に接近していくフェーズ

把持・結合

- ISS に対して相対停止し，ISS のロボットアームで把持され結合されるフェーズ

係留

- ISS に結合し，ISS に対する物資の補給などが行われるフェーズ

ISS からの分離

- 把持が解放され， ISS 軌道から離脱するフェーズ

再突入

- 大気圏に再突入し燃え尽きるフェーズ

ここでは，実験で出題した課題に関連するランデブフェーズにおける近傍運用および把持・結合フェーズについて詳述する．
HTV は打ち上げ後約 4 日かけて高度を上げながら ISS に接近する．ISS と HTV が直接通信可能な領域に到達すると，HTV は PROX との通信を確立し誘導制御を実施して ISS の後方約 5 km の接近開始点に到達する．
AI 地点から ISS の下方 250m 到達時と 30m 到達時の 2 回，HTV は自動的にいったん停止を行い，最終的に ISS の下方 10m 付近で相対停止する．なお，この一連の近傍運用中に HTV が ISS に衝突する危険性が高まるなど緊急事態が生じた場合には，ISS の搭乗員が HTV にコマンドを送るための装置から緊急コマンド (強制退避 (ABORT) など) を PROX を通じて送信することにより，HTV を制御することができる．
地上局では，HTV が ISS の下方 10 m 布巾で ISS に対して相対的に停止したことを確認すると，HTV のスラスタを停止する．その後，ISS のロボットアームで ISS を把持し結合させる．

HTV の近傍運用の流れを図 9 に示す．

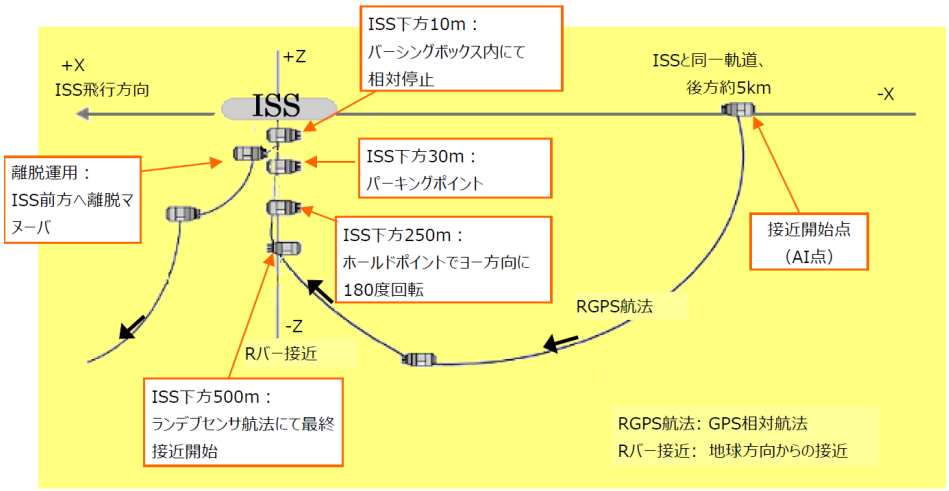

図 9　HTV 近傍運用の流れ

B. 宇宙機を題材とした実験で使用した資料

B.1 ハザードレポートの一例

以下に，実験で使用したハザードレポートの一例を示す [10].

HR No.	ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 （検証については下線を付す）	HTV7号機の対応及び検証結果
HTV-0008	HTVのISSへの衝突	I （カタストロフィック）	飛行管制、分離機構等のHTVの安全上重要なソフトウエア機能の誤動作により、HTVのISSへの衝突、機器の意図しない分離により他のISS機器へ衝突し、居住モジュールの破損による搭乗員の死傷にいたる。	【故障許容またはリスク最小化設計】 ISS共通のソフトウェア安全要求を適用した。 • 機能喪失がハザードとなる場合、独立した複数機能を搭載する。 • 不意起動がハザードとなる場合、危険な機能の起動に対する3重インヒビットを設ける。 ソフトウェアの検証として以下を実施した。 • ソースコードの審査 • ソフトウエア単体試験 • シミュレータ試験 • 独立部門による独立評価（IV&V） • ハードウェア搭載後のシステム試験	• 更新したソフトウェアに対し、以下の試験を実施し変更の妥当性を確認した。 • ソースコードの審査 • ソフトウエア単体試験 • シミュレータ試験 • フライトソフトウェアインストール後のシステム試験（6項5番）
			誘導制御系の故障によりHTVが正しく制御できなくなりISSに衝突してしまう。	【 2故障許容設計】 a. 上記計算機やコントローラの機能性能についてはソフトウェアを組み合わせた試験で確認した。 b. 誘導制御計算機内で2故障が発生した際に、自動で緊急離脱系へ切り替わることについて試験で確認した。	a. HTV7号機のフライトハードウェアが所定の機能を提供できることについて、機器単体及びソフトウェアを組み合わせた試験で確認した。 b. HTV7号機の誘導制御計算機及び緊急離脱装置間のインタフェース試験において、自動で緊急離脱系へ切り替わることを試験で確認した。
			センサ系の異常によりHTVが正しく制御できなくなりISSに衝突してしまう。	【 2故障許容設計】 a. 誘導制御に必要なセンサは、すべて2個以上設置し、計測値の比較等も踏まえて1故障許容設計とした。センサの機能性能等については購入時の製品検査や機能試験で確認した。 b. センサが2故障した場合、すなわちセンサの出力値が信頼できないような場合は、誘導制御計算機から緊急離脱制御装置に切り替わり、緊急離脱できることを試験で検証した。	a.HTV7号機のフライト品センサについて、機能性能に問題が無いことを製品検査及び機能試験で確認した。 b.センサ異常に対応する処理ロジックは誘導制御計算機に搭載されソフトウェアに組み込まれているが、該当する処理ロジックに変更がないことを確認した。

図 10 HTV ハザードレポート例 1 [10]

HR No.	ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 （検証については下線を付す）	HTV7号機の対応及び検証結果
HTV-0008	HTVのISSへの衝突	I （カタストロフィック）	推進系の故障でHTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 a. 姿勢制御系統を構成するバルブ・推進系の圧力、温度センサ等の機能部品が故障した場合、別系統に切り替えることで1故障許容とできる設計とした。各系統の機能や系統切り替えが問題無くできることについて試験で確認した。 b. 2故障時は、自動で緊急離脱系へ切り替わることについて試験で確認した。	a./b. HTV7号機の誘導制御計算機試験及び緊急離脱装置間のインタフェース試験において、各系統の機能や系統切り替えおよび自動で緊急離脱系へ切り替わることを確認した。
			推進系配管の凍結、破損後の漏洩により、HTVが正しく制御できなくなりISSに衝突してしまう。	【2故障許容設計】 姿勢制御系統、メインエンジン系統が繋がっている主要な配管／バルブ／推進薬タンクへのヒータ3重化の施工により、2故障許容設計とした。熱解析の結果、ヒータ1系統だけでも凍結が防止できることを確認した。また、ヒータシステムの機能性能についてはシステム試験等で問題無いことを確認した。	ヒータ故障時の凍結防止に係る温度解析については、環境条件や熱設計に変更がないため従来の解析が有効である。熱解析の前提条件ともなっているヒータシステムの機能については、機能試験で問題ないことを確認する。（6項4番）
			HTVがISSロボットアームで把持される際は、所定の領域内に相対停止し、位置・姿勢制御機能を完全停止する必要がある。もし所定の領域を外れた場所で把持された場合、最悪ISSロボットアームが損傷し、結果的にISSに衝突させてしまう可能性が生じる。	【リスク最小化設計】 a. 姿勢やセンサの誤差を考慮した適切な把持領域が設定できたことを、NASA及びカナダと協力して解析で確認した。 b. 予定外の姿勢でHTVが放出された場合でも、HTVの制御機能を搭乗員や運用者が起動して姿勢制御を実施できることを解析および試験で検証した。	ISS搭乗員から接近中断等のコマンドを送信するための機器がHTV専用の端末から共用のISS搭載可搬型PCに変更になったことを反映した。（13頁参照） a.把持領域の設定についてはHTV1号機以降変更はない。 b.ISS搭載可搬型PCに変更になったことを考慮しても、放出後のHTVの姿勢制御を実施できることを誘導制御系解析で確認した。また、専用端末の使用がなくなったことに伴い、モジュール間を跨ぐケーブルに対する安全要求の不適合報告書が不要となった。

図 11　HTV ハザードレポート例 2 [10]

HR No.	ハザードタイトル	被害の度合い	ハザード内容	HTV1号機の対応 （検証については下線を付す）	HTV7号機の対応及び検証結果
HTV-0008	HTVのISSへの衝突	I （カタストロフィック）	HTV近傍域通信システムとのリンク遮断により、HTVに異常が確認された際の緊急コマンドが打てず、ISSに衝突させてしまう。	【２故障許容設計】 HTVは「きぼう」に設置された近傍通信システム（PROX）と2系統の通信リンクをする他、バックアップとして衛星間通信衛星との直接通信リンクを確保できるようにしている。このため、通信系統の機器が2重故障を起こしても通信手段を失うことはない。各通信系統の機能については機器単体の受け入れ検査やシステムレベルの機能試験で問題が無いことを確認した他、異常があった場合に自動で系統が切り替えられることについても確認している。通信・伝送系統全体の確認としてはNASA地上局やISSを模擬した設備も含めたEnd-to-End試験も実施して良好な結果を得た。	HTV7号機に搭載する通信系機器及びシステム機能について、受け入れ検査や機能試験で問題が無いことを確認した。
			電源系の異常によりHTVが機能喪失してISSに衝突してしまう。	【２故障許容設計】 単独飛行中は、太陽電池及び二次電池並びに一次電池からの供給電力で飛行する。一次電池の個数は、運用上必要な容量を解析評価した上で2故障時の最悪シナリオを賄える個数のセルを搭載した。バッテリ及びその周辺回路がISS共通の要求に適合していることについては検査及び試験で確認した。	HTV1号機は一次電池を11台搭載していたが、実際の運用で太陽電池と二次電池だけでほとんど賄えたため、マージンを見直した。この結果、一次電池の台数はHTV7号機では5台とした。電力リソース解析を更新し、安全への影響がないことを確認した。 HTV7号機に搭載されるバッテリ及びその周辺回路がISS共通の要求に適合していることについて、検査及び試験で確認した。打上げ前にバッテリが適切に充電されることについては射場で確認する予定。（6項4番）

図 12　HTV ハザードレポート例 3 [10]

C. 家電を題材とした実験で使用した資料

本実験では，JAXA が IV & V 教育教材として作成した電子レンジ仕様書等を活用し，家電仕様書等を作成した． 以下に実験で使用した資料を示す.

C.1 仕様書

電子レンジ仕様書

1. 製品概要

電子レンジの外観を下図に示す。

内部には回転式テーブルがあり、ドアは横に開くタイプで垂直方向に取り付けてある。操作するものとして主電源ボタン、加熱開始ボタン、取消ボタンという３つのボタンが装備されているほか、あたためる時間を設定できるダイヤルが装備されている。また、ボタンを押した時および異常検知時に音を出力するスピーカが側面に装備されている。

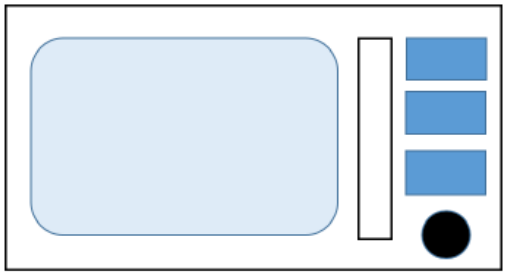

図１．電子レンジ外観

2. 製品機能

2.1. 製品機能

本電子レンジの基本機能は食べ物等を温めるために必要な機能で、調理とキャンセルの２機能である。

2.2. 安全機能

電子レンジは人に危害を加える状態を検知した時に稼働を停止する安全機能を有する。

・加熱中にドアオープンを検知した場合、自動的に加熱を止める機能

・加熱中に被加熱物に温度/振動異常を検知した場合、自動的に加熱を止める機能

3. サブシステム概要

電子レンジのサブシステム構成図を下図に示す。

図 13 電子レンジ仕様書１

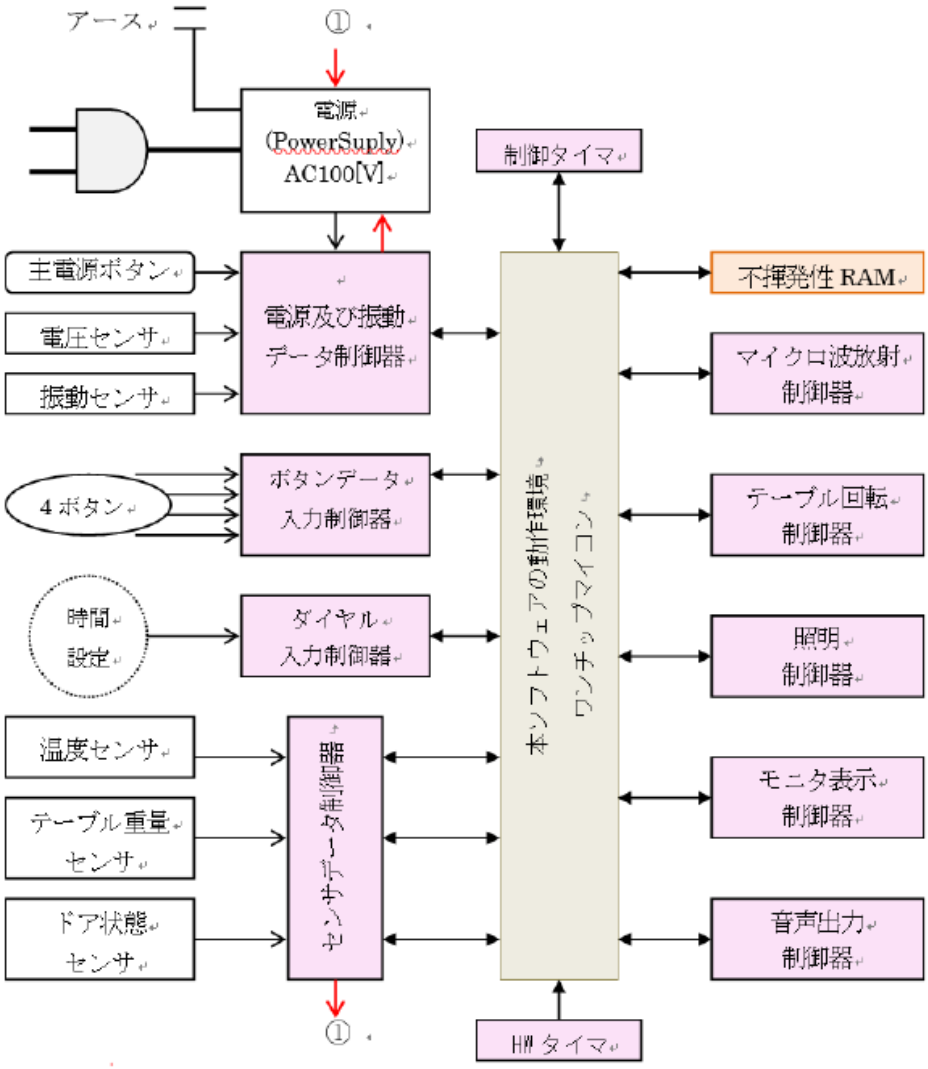

図 2. 電子レンジのサブシステム構成図

図 14　電子レンジ仕様書 2

4. ハードウェアコンポーネントの機能概要

No.	コンポーネント	機能概要
1	ボタン	・主電源ボタン 電子レンジのコンセントが電源に刺さった状態でボタンを押すと電子レンジの電源が ON になる。もう一度押すと OFF になる ・あたためボタン 加熱を開始する ・キャンセルボタン 加熱を途中で停止する
2	ドアセンサ	ドアが開いているかどうかを検知する
3	温度センサ	被加熱物の温度を計測する
4	振動センサ	被加熱物の振動の有無を検知する
5	重量センサ	ターンテーブルに乗った被加熱物の重量を計測する。 **(初期重量はターンテーブルの重量に設定されており、被加熱物の重量＋ターンテーブルの重量をセンサデータ制御器に出力する。)**
6	ダイヤル入力制御器	ダイヤル操作を検知して設定時間をソフトウェアに出力する
7	電源および 振動データ制御器	主電源ボタンが押された時、電子レンジの電源の ONOFF を行う 電源遮断時にソフトウェアに主電源オフ割込を発生する
8	ボタンデータ 入力制御器	ボタン操作から優先ボタンデータを決定してソフトウェアに出力する。 **デフォルトの状態を no-touch(使用者のボタン操作がない状態)とし、1 つのボタンにタッチがあった場合、100 [ms] 待って次のタッチがない場合、そのボタンの操作を採択する。ただし、キャンセルボタンは即座に採択する。**
9	センサデータ 制御器	・温度センサからの入力をもとに電子レンジ内部の温度を値でソフトウェアに出力する。 ・テーブル重量センサからの入力をもとにテーブルに乗った被加熱物の重量をソフトウェアに出力する。 ・加熱中の被加熱物の異常高温を検知して稼働を停止する
10	マイクロ波 放射制御器	加熱のためのマイクロ波放射オンオフを行う

図 15 電子レンジ仕様書 3

11	テーブル回転制御器	電子レンジ内部のターンテーブルを回転させる。回転のオンオフを行う。
12	照明制御器	電子レンジ内部の照明のオンオフを行う。
13	音出力制御器	・ボタンを押したときに確認のため音を出力する ・加熱中に異常を検知した場合、稼働を停止するとともに音を出力して知らせる
14	タイマー	設定された加熱時間を計測し、設定時間経過でタイマー割り込みを発生させ加熱を停止する

5. ソフトウェア概要

本ソフトウェアは、電源投入をトリガとして ROM の 0 番地からパワーオンスタートし、パワーオン初期化処理を実施する。正常に起動した後は、コマンド入力(ボタンタッチ)とセンサデータ入力を周期的に監視する。電子レンジでの加熱時は、ダイヤル制御器からの入力で加熱時間の設定を取得、ドアクローズを確認後、テーブル回転制御、照明制御、及びマイクロ波放射制御を実施した後、電源制御器にマイクロ波放射パワーを指定する。

割込み発生時(加熱中のドアオープン時など)は、即座に割込み処理を実施する。システムの状態に異常があった場合、音を出力して使用者にアナウンスする。また、ボタンタッチ時には音を出力させる。

図 16 電子レンジ仕様書 4

C.2 ハザードレポート

ハザード一覧

1. 被過加熱に対する過加熱
2. マイクロ波の漏洩
3. 異常高温
   （ア）製品の発火
   （イ）使用者のやけど

1. 過加熱

過加熱とは、液体を加熱するときに沸点を超えても沸騰を起こさず液相が維持される状態をいう。過加熱状態にある液体は突然激しく沸騰する「突沸」と呼ばれる現象を引き起こす。突沸によって被加熱物が容器からこぼれるなどし、使用者の火傷につながる場合がある。過加熱の要因として、加熱時間が長すぎることが挙げられる。加熱時間が長い要因としては、使用者により設定された加熱時間が長すぎることと、タイマー機能の不具合により使用者が設定した時間を超えた加熱が行われることが挙げられる。タイマー機能が不具合となり加熱時間が設定を超過した場合でも、温度センサによる計測で被加熱物の温度が一定値を超えた場合に加熱を停止することで過加熱を防ぐ仕様とした。

【設計によるハザード制御】

・被加熱物の温度が一定値を超えると加熱を停止するよう設計する。
・設定した時間を超えて加熱を行わないようタイマー機能を冗長化する。
・被加熱物の振動を検知した場合、加熱を停止するよう設計する。

【検証】

・冗長化されたタイマー機能が両方とも正常に動作し、また、一方が機能しない場合に即時にもう一方が動作を開始することが確認された。
・被加熱物の温度が一定値を超えた場合、設定された加熱時間の途中であっても加熱を中止し、稼働を停止するとともに、音を出力して知らせる動作を行うことを確認した。

図 17 ハザードレポート 1

2. マイクロ波の漏洩

電子レンジは 2.45 GHz のマイクロ波を発生させ、この振動数で被加熱物中の水分子を振動させて熱を発生させる。このため、加熱中にレンジ外部にマイクロ波が漏洩すると使用者など近くにいる人間等に火傷を負わせる等、受傷させる可能性がある。本項ではドアがある面方向からのマイクロ波の漏洩についてハザード解析をおこなった。

【設計によるハザード制御】

(1) マイクロ波出力 ON/OFF 機構

1) スイッチは継電器（電磁リレー)を用いて実現する(図 1)

2) ON 信号の入力で、スイッチ ON (CLOSE)

3) OFF 信号の入力で、スイッチ OFF(OPEN)

4) スイッチの機構にハードウェアバネを用いているため、ON 信号を意味する電圧の印加がない限り、スイッチは OFF 状態を維持する。(FAIL SAFE 機構)

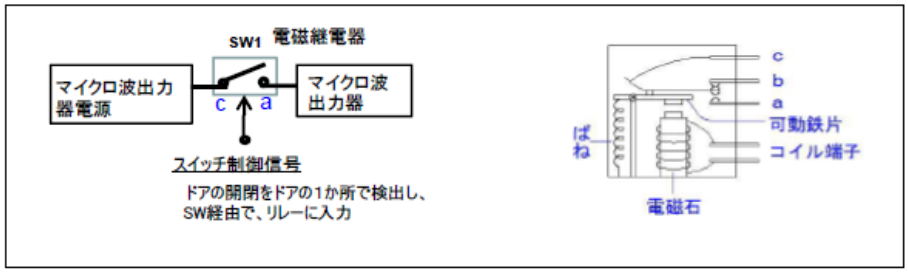

図 1　マイクロ波 ON/OF（スイッチ）の機構

(2) マイクロ波誤照射防止インターロック/インヒビット機構の実装

ドアオープン時にマイクロ波が照射されること(意図しない照射)を防ぐため、ソフトウェアで制御できるインヒビットを含むインターロック機構の実装が、設計で決定されている。その機構を以下に示す。

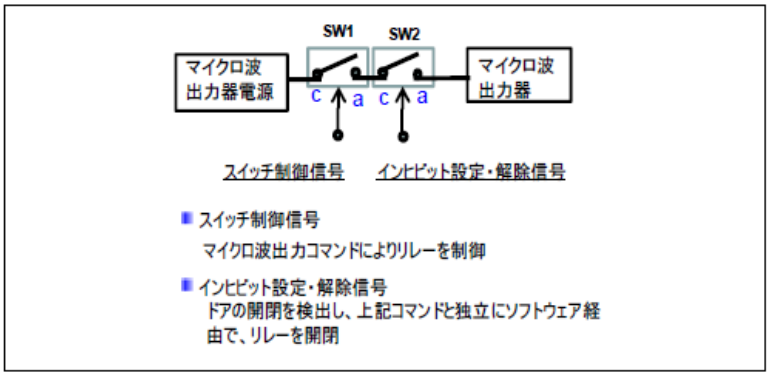

図 2 マイクロ波誤照射防止のためのインヒビット機構

図 18　ハザードレポート 2

(3)ドアセンサの冗長化

【検証】

・マイクロ波 ON/OFF 機構において、ON 信号を意味する電圧の印加以外でスイッチは OFF 状態を維持することが確認された。

・ドアセンサの一方が機能しない場合でも、もう一方が動作することが確認された。

図 19 ハザードレポート 3

3.異常高温

（ア)製品の発火

電子レンジから発火した場合、火事の原因となるほか、使用者のやけど等受傷にも繋がり大変危険である。本項では電子レンジ本体が高温となり発火する、または被加熱物が発火する場合を扱う。

発火を防ぐため、1 節で記載した被加熱物の温度を計測する温度センサとは別に、電子レンジ内部の温度を計測するセンサを設置し、温度が一定値を超えた場合に加熱を停止することとした。また、温度センサによる被加熱物の温度計測も被加熱物からの発火を防ぐ上で対策となる。

さらに、電子レンジの大きな振動を検知して加熱を停止し電源を遮断することで、発火をともなう爆発を事前に検知することが可能であるとした。

【設計によるハザード制御】

・被加熱物の温度が一定値を超えると加熱を停止するよう設計する。
・電子レンジ内部の温度をセンサで計測し、一定値を超えた場合に加熱を停止する。
・振動センサで一定以上の大きな振動を検知した場合、音を出力して使用者に知らせ、500 [ms]後に加熱を停止して電源を遮断する。

【検証】

・被加熱物の温度が一定以上となった場合、加熱を停止することを確認した。
・電子レンジ内部の温度が一定値を超えた場合、設定された加熱時間の途中であっても加熱を停止し、音を出力して使用者に知らせることを確認した。
・電子レンジに大きな振動を与えた場合、加熱の停止と電源の遮断が行われることを確認した。

図 20　ハザードレポート 4

(イ)使用者のやけど

本項で扱う使用者のやけどは、電子レンジで本来熱くならない部分(ドアなど)が高温となり使用者がそれに触れてやけどをする場合を指す。(被加熱物が異常高温となるハザードについては 1 節の記述を参照、電子レンジの発火による受傷については 3(ア)項を参照)

このハザードへの対策として、(ア)節と同様に電子レンジ内部の温度が一定以上となった場合に加熱を停止することとした。また、マイクロ波に晒され高温となる電子レンジ庫内の表面部が外部に熱伝達しにくい素材であることなど、システムを構成する素材にも安全面から要求を出した。

【設計によるハザード制御】

・電子レンジ内部の温度をセンサで計測し、一定値を超えた場合に加熱を停止する。
・電子レンジ庫内の表面部となる素材を耐熱性の高いものとする。また、電子レンジの外部側面を含め庫内より外に熱を伝達しない素材とする。
・電子レンジの外部側面やドア取っ手など使用者が触れやすい部分は、熱を吸収しにくい素材とする。

【検証】

・電子レンジの温度が一定値を超えた場合に電子レンジが加熱を停止することを確認した。
・電子レンジ内部が加熱を停止しない上限の温度に達しても、電子レンジの外部側面やドア部分などは使用者が触れて安全な温度であることを確認した。

図 21　ハザードレポート 5

C.3 FTA

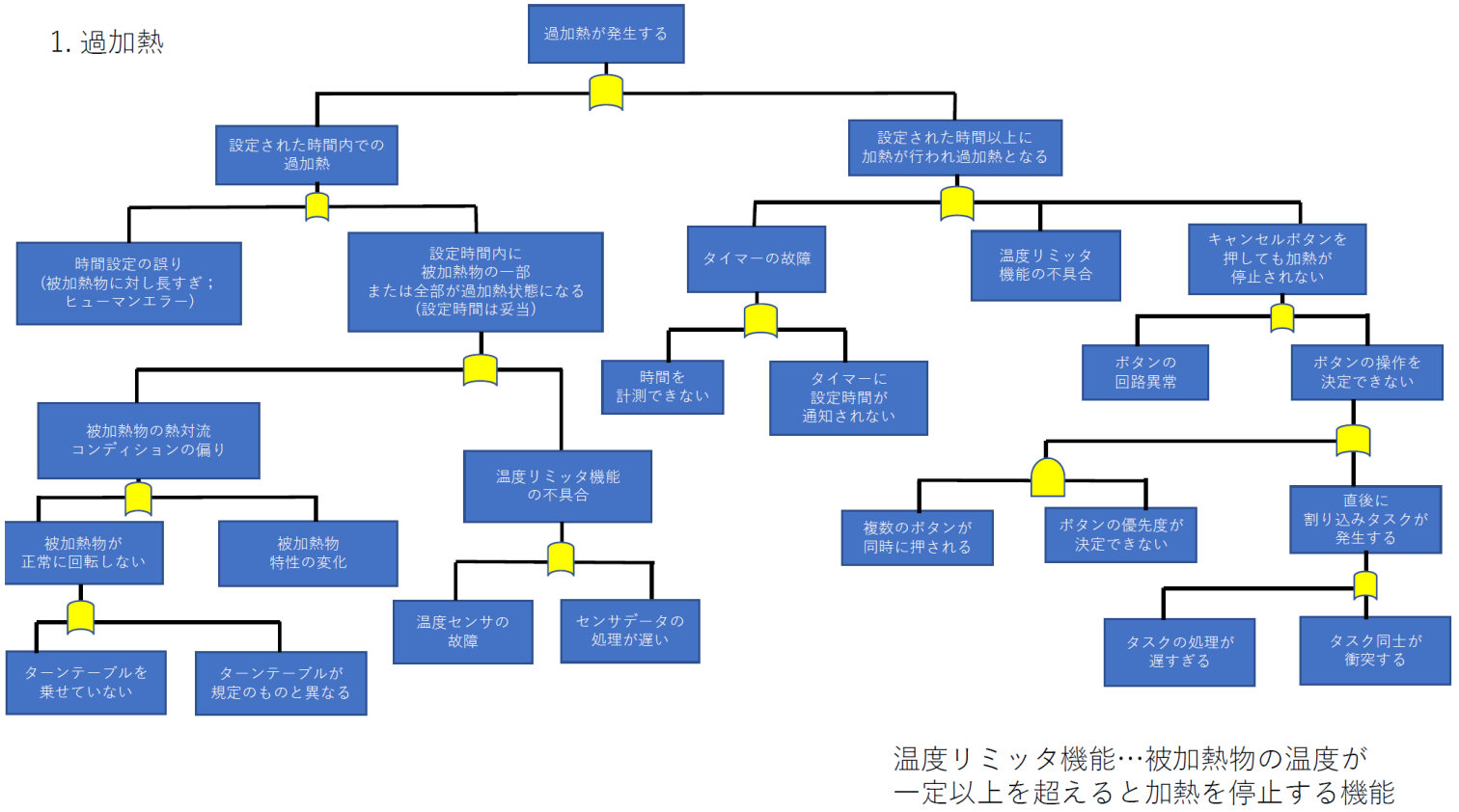
1. 過加熱
過加熱が発生する
設定された時間内での
過加熱
設定された時間以上に
加熱が行われ過加熱となる
時間設定の誤り
(被加熱物に対し長すぎ；
ヒューマンエラー)
設定時間内に
被加熱物の一部
または全部が過加熱状態になる
(設定時間は妥当)
タイマーの故障
温度リミッタ
機能の不具合
キャンセルボタンを
押しても加熱が
停止されない
時間を
計測できない
タイマーに
設定時間が
通知されない
ボタンの
回路異常
ボタンの操作を
決定できない
被加熱物の熱対流
コンディションの偏り
温度リミッタ機能
の不具合
複数のボタンが
同時に押される
ボタンの優先度が
決定できない
直後に
割り込みタスクが
発生する
被加熱物が
正常に回転しない
被加熱物
特性の変化
温度センサの
故障
センサデータの
処理が遅い
タスクの処理が
遅すぎる
タスク同士が
衝突する
ターンテーブルを
乗せていない
ターンテーブルが
規定のものと異なる
温度リミッタ機能…被加熱物の温度が
一定以上を超えると加熱を停止する機能

図 22　FTA1

2. マイクロ波の漏洩

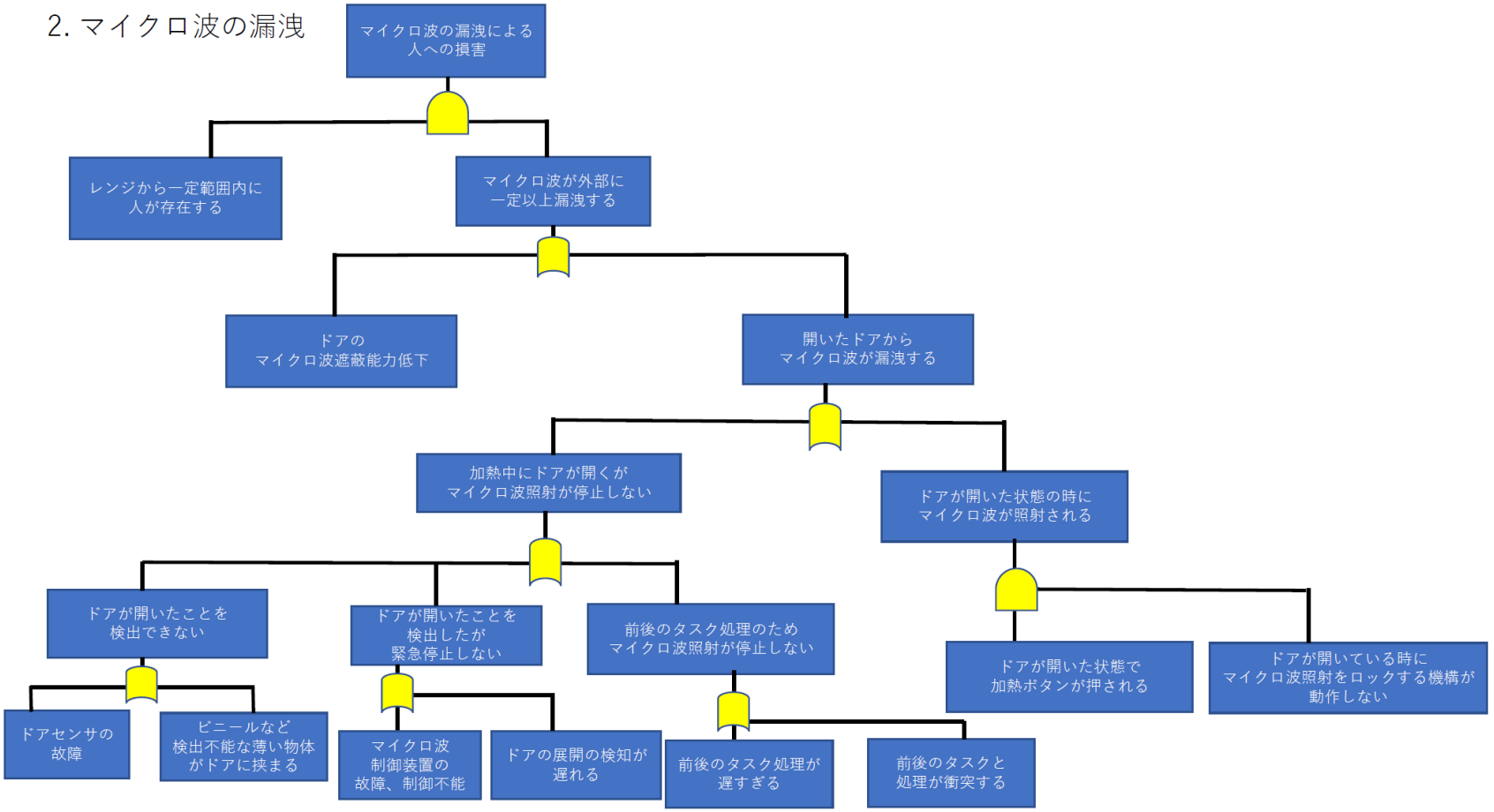

図 23 FTA2

3. 異常高温ー製品の発火

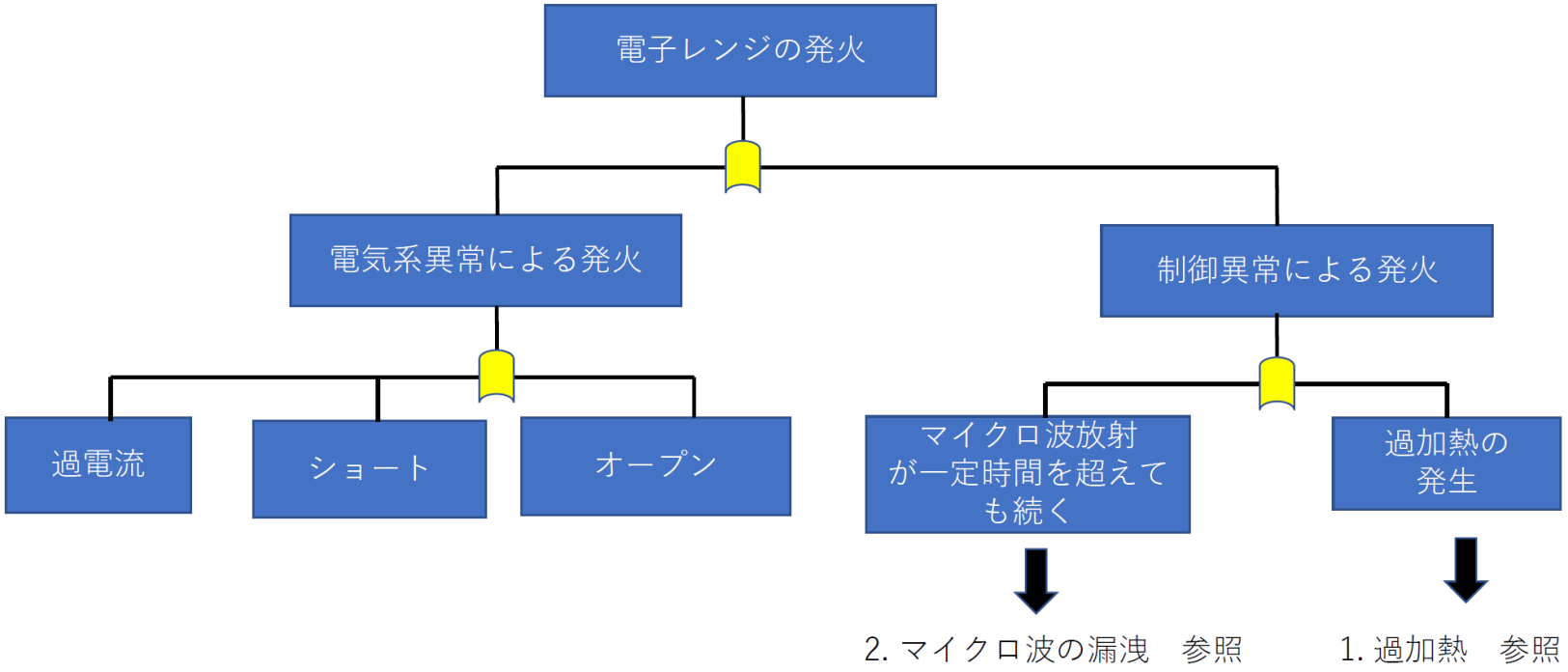

図 24　FTA3

3. 異常高温ー使用者のやけど

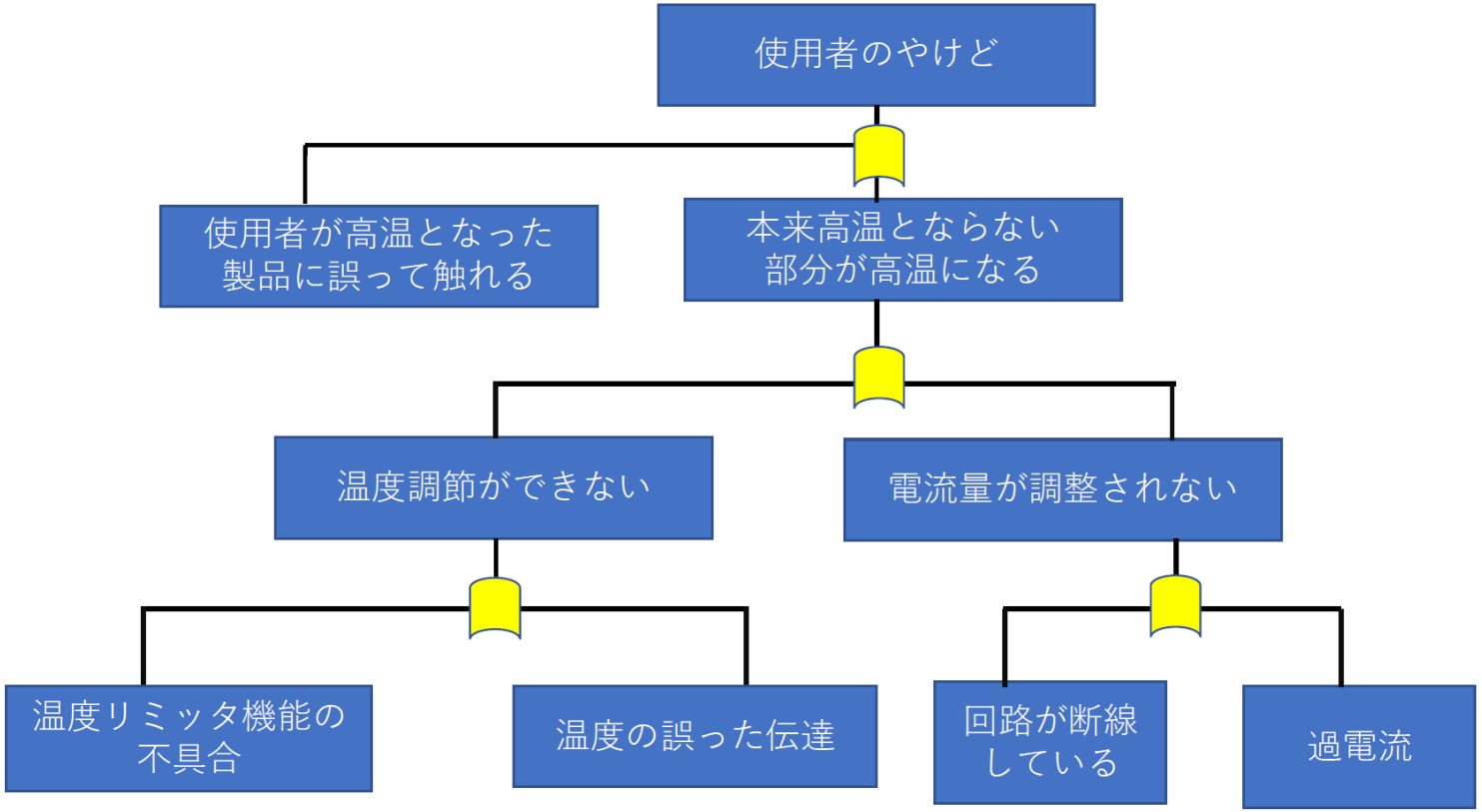

図 25 FTA4

C.4 FMEA

機器名	機能	故障の状態	故障の原因	故障の影響	システム全体への影響
タイマー	時間の計測	スイッチが 入らない	断線、動作不良	加熱できない	ー
		スイッチが 切れない	断線、動作不良	過熱される	他コンポーネントの 過熱による破損 過加熱、発火
		正しく時間が 計れない	・タイマー内の歯車の破損 ・ダイヤルからタイマーへ設定した時間が送られない	設定した時間で 加熱されない 過熱の可能性	
ボタン	使用者の 操作の伝達	ボタンを押すが 反応しない	断線など	使用者が 電子レンジに 意図した操作ができない	異常時に キャンセルボタンが 反応しない場合 過加熱や発火に至る恐れ
ドアセンサ	ドアが開いて いるかを検知	ドアオープンを 検知できない	・導線の不良 ・検知する閾値以下の物体がドアに挟まる(ビニールなど)	ドアが開いても 加熱を続ける	加熱が停止せず過加熱 またはマイクロ波誤射
振動センサ	振動の有無を検知	振動を検知しない	導線不良	過加熱状態を 検知できない	過加熱に気づかず 使用者がやけど、発火等 の可能性
ダイヤル	加熱時間の設定を出力	ダイヤルが回せない	破損、摩耗など	使用者が 時間設定できない	ー
		設定時間がタイマー機能に 通知されない	ダイヤルの回転をソフトウェアが検知しない →回路の不良など	時間設定が 行われない	期待した加熱が 行われない

図 26　FMEA1

機器名	機能	故障の状態	故障の原因	故障の影響	システム全体への影響
マイクロ波 放射制御器	加熱のための マイクロ波を放射	マイクロ波を 放射できない	マイクロ波ON/OFF機構の破損	加熱が行われない	ー
センサデータ 制御器	各センサのデータから 異常を検知する	センサから データを受け取れない	導線不良 センサの故障(各センサの項参照)	異常を検知しない	過加熱の可能性
		異常が検知されない	・センサデータの処理が間に合わない	異常を検知しない	過加熱の可能性
ボタンデータ 制御器	ボタン操作を ソフトウェアに出力	操作が出力されない	・断線など導線の不良 ・優先ボタンデータを決定できない	操作が正常に 行われない	過加熱、発火に至る可能性
テーブル回転 制御器	被加熱物を ターンテーブルに乗せて 回転させる	テーブルが 回転しない	・制御不能 ・ターンテーブルを乗せていない or規定と異なるターンテーブルを乗せている (重量センサの出力がターンテーブルの重量を デフォルト値としており、重量が変化した場合 エラーとなり回転しない)	加熱されない	テーブルが回転しないまま 加熱が行われた場合 熱対流の偏り→過加熱
		回転が正常に 行われない	・破損 ・重量センサに出力された重量と 実際の被加熱物の重量が異なる	期待した加熱が 行われない	過加熱の可能性
音出力制御器	操作時や異常時に 音を出力して知らせる	音が出力されない	スピーカの経年劣化 断線　など	使用者が異常に 気付かない	ー

図 27　FMEA2