博士学位論文

システム理論に基づく安全解析手法（STAMP/STPA）の要件定義工程への適用評価

Evaluation of the Application of the Safety Analysis Method Based on System Theory “STAMP/STPA” to Requirement Development Phase

2019 年 9 月

慶應義塾大学大学院

システムデザイン・マネジメント研究科

システムデザイン・マネジメント専攻

山口　晋一

要旨

近年のシステム開発は大規模／複雑化の一途を辿っており，多様なシステム構成要素が複雑に関係している．その状況下においても，従来の安全解析手法が使用され続け，システムに深刻な事故や損失を引き起こしている．そのため，システムの構成要素間の相互作用に着目した，新しい安全解析手法となる STAMP/STPA が注目されている．しかし，特に日本では，まだ広く使用されるに至っていない．近年の深刻な事故や損失は，要件定義工程起因のものが増加している．このような状況を踏まえて，本論文では，要件定義工程での STAMP/STPA の適用に着目し，開発早期でのより安全性の高いシステム開発を目指して，STAMP/STPA の現場適用に効果的な，要件定義書へ追記する記載項目及びその記載ルールを示した．また，要件定義工程において，STAMP/STPA を適用することにより得られた，損失シナリオから導出したコンポーネント安全要求を開発へ直ちにフィードバックすることは重要である．そこで，STAMP/STPA での解析対象となるコントロールアクションに優先順位をつけて解析を実施する手法を示した．さらに，それらの手法の適用プロセスも示した．システム全体を構成する各要素に対し，本論文で提案する手法で STAMP/STPA をシステムの要件定義工程へ適用し，優先順位の高いコントロールアクションから順次，損失シナリオを識別し，安全解析を実施する．その結果として得られた，損失シナリオから導出したコンポーネント安全要求を要件定義工程へ逐次的にフィードバックする．それにより，システム開発における早期工程で，より安全性の高いシステム開発を目指すことができる．

近年の医療産業では，より最先端で効果的かつ安全な医療技術を医療従事者に供給できるように急速に進歩している．しかしながらその進歩に伴い，医療技術，治療及び医療機器等はより複雑となっている．アメリカの Food and Drug Administration（FDA）によると，治療において深刻な被害を引き起こす不具合のあるものとしてリコールされている医療機器の数は，増加傾向にあると報告されている．本論文では，より安全性の高いシステム開発が要求される医療装置として，放射線治療装置を本提案の適用対象とした．それにより，STAMP/STPA の現場適用への課題の解決方法を提示することができた．また，本論文における提案内容の適用を通して，医療機における安全性解析の従来手法として広く使用されている Failure Mode and Effect Analysis（FMEA）との適用結果と比較する事で，STAMP/STPA での適用結果では，よりシステムホリスティックな解析結果を得ることができた．

Abstract

In recent years, the scale and development of systems have become larger and more complex, and various components of the system have more complicated relationships. Regardless of the situation, the traditional safety analysis method has been maintained, and the systems have continuously caused serious accidents and losses. Because of this, a relatively new safety analysis method STAMP/STPA, which focuses on the mutual interaction among the components of the system, has been garnering more attention. Specifically, even until now in Japan, this method has not been applied to systems in various industries.

Recent serious accidents and losses have been caused by the defects made in the requirement development phase, and the number of such defects has been increasing. The focus of this research is the application of STAMP/STPA to the requirement development phase, and it is aimed to develop a system that is highly safe in an early development phase.

For these purposes, we propose (1) additional items for requirements definition and rules for describing requirements, (2) an application process for using STAMP/STPA in actual development projects, and (3) a method to prioritize the identified unsafe control actions (UCAs) for safety analysis.

The technology in the medical industry has been advancing in recent years to provide safe and systematic medical care. However, the system of medical technologies and treatments has become more complicated year by year, which increases the risks of defects in the system. For example, the U.S. Food and Drug Administration's Center for Devices and Radiological Health has reported recalls of medical devices that may lead to serious injury or death because of malfunctions. To reduce the risks, developers and producers of medical devices have been applying a wide spectrum of methodologies to improve quality.

However, the growing complexity of medical systems, including devices, medical staff, organizations, and regulators, causes problems that current safety engineering techniques are inadequate to prevent, which can result in tragic medical accidents. Therefore, it is important to apply new approaches to ensure the system safety of medical devices.

Considering this situation, this thesis identifies the basic design of tomographic treatment. We propose to show the solutions to solve problems regarding the use of STAMP/STPA in actual development projects by applying our proposals to the TomoTherapy radiation treatment system in the requirement development phase.

This tomographic treatment system treats hard-to-reach tumors and reduces radiation exposure to nearby healthy tissues. To ensure the quality of TomoTherapy, STPA is an effective means to conduct hazard analyses because, through this research, STPA is found to be an effective means to ensure the quality of TomoTherapy and to conduct a holistic

hazard analysis. This includes both human and technical factors, a comparison of STPA, and one of the most popular approaches in the medical device industry, Failure Mode and Effect Analysis (FMEA), with STPA. A comparison of STPA and FMEA results found that STPA can identify a larger set of causal scenarios. The interactions of humans, hardware, and software was highlighted through this application.

目次

図表一覧[図]

図表一覧[表]

略語一覧

AAPM	American Association of Physicists in Medicine
A-CAST	Automated tool support for CAST
A-STPA	Automated tool support for STPA
CA	Criticality Analysis
CAST	Causal Analysis using System Theory
CC	Controller Constraints
ConOps	Concept of Operation
CT	Computed Tomography
ESPR	Embedded System development Process Reference
ETA	Event Tree Analysis
FDA	Food and Drug Administration
FMEA	Failure Mode and Effect Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
FTA	Fault Tree Analysis
GUI	Graphical User Interface
HAZOP	Hazard and Operability Study
IAEA	International Atomic Energy Agency
ICRP	International Commission on Radiological Protection
IEC	International Electrotechnical Commission
IGRT	Image-Guided Radiation Therapy
IMRT	Intensity-Modulated Radiation Therapy
LA	Linear Accelerator
MCO	Mars Climate Orbiter
MLC	Multi-Leaf Collimator
OPM	Object Process Methodology
RCP	Rich Client Platform
PDE	Plugin Development Environment
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
RPN	Risk Priority Number
SAP	Safety Engineering Process
STAMP	Systems Theoretic Accident Model and Process
STECA	Systems-Theoretic Early Concept Analysis
STPA	System Theoretic Process Analysis

SysML	Systems Modeling Language
UCA	Unsafe Control Action
UML	Unified Modeling Language
USDM	Universal Specification Describing Manner
XSTAMPP	eXtensible STAMP Platform
XSTPA	Extended Approach to STPA

第1章　緒論

1.1 本論文の背景

近年の大規模／複雑化するシステムにおいて，事故を未然に防ぐためには，システムを構成する様々な要素間の相互作用の関係に着目することが必要になってきた（Leveson, 2004）．そのための有効な手法として，新しい安全解析手法である Systems Theoretic Accident Model and Process（STAMP)に基づく System Theoretic Process Analysis（STPA）（Leveson, 2012）が着目されている．STAMP/STPA は，事故や損失を，システムを構成する単一要素の故障の問題として扱うのではなく，構成要素間における制御の問題として扱う事を特徴とし，MIT の Leveson により提唱されたシステム理論に基づく安全解析手法である．

STAMP/STPA は，2004 年に STAMP モデルがアクシデントモデルとして提唱され，2012 年に STPA である安全解析手法として手法化された．一方，従来の安全解析手法の多くは 1940 年代に提唱されている．そのため，STAMP/STPA は比較的新しい手法であると言えるが，日本ではまだ適用事例は多くなく，広く活用されるに至っていない．STAMP/STPA はシステムを構成する様々な要素間の相互作用の関係に着目した解析手法である．

近年のシステムにおける深刻な事故や損失は，このような要素間の相互作用の関係が阻害されることにより引き起こされており，特に，要件定義工程起因のものが増加している現状がある（日本情報システムユーザー協会（JUAS), 2014）．

このような事例として，1999 年に発生した，NASA によって打ち上げられた火星探査機での 2 つの事故が挙げられる（NASA, 2005）．まず，1999 年 9 月，Mars Climate Orbiter（以下，MCO）は火星の周辺軌道投入の際に炎上し，その軌道上で消失した．この火星の周囲軌道投入に失敗した MCO の原因は，非常に単純なものであり，2 つのソフトウェアモジュールの要件に起因するものと推測されている．この MCO はアメリカのコロラド州にある Lockheed-Martin Astronautics 社によって開発され，NASA により火星へと打ち上げられた．そして，その打ち上げ後においては，同国のカリフォルニア州にある Jet Propulsion Laboratory の Mission Navigation Team によって，その追跡データが分析され，火星への軌道修正が決められていた．そし

て，その軌道修正の決定内容に従って，Lockheed-Martin Astronautics 社の Mars Climate Orbiter Spacecraft Team がエンジン噴射推力を計算し，要求元である Mission Navigation Team に返信していた．これらの 2 チームが実装していたソフトウェアはそれぞれ，定義された要件に従って正しく実装されていた．しかし，実際には，両者で使用していた単位系が異なっていた．実際には，Mars Climate Orbiter Spacecraft Team 側は English Units（ヤード・ポンド法）を使用し，Mission Navigation Team 側は Metric Units（メートル法）を使用しており，事故の発生まで，この事に両者は全く気づいていなかった．この単位の相違から生じた計算誤差により，MCO は，火星周囲軌道への突入の際に，予定より大幅に高度が下がってしまい，この事故を招いてしまったと推測されている．さらに，1999 年 12 月には，Mars Polar Lander が火星表面に墜落する事故が発生した．火星探査機は安全に着陸するために，その着陸の際には的確に減速しなければならない．そのためにも，火星の大気圧を考慮して，探査機に備えられた降下用のパラシュートや軟着陸用エンジンをソフトウェアで制御していた．そして，そのソフトウェアは，降着装置に搭載された高感度センサーにより着陸したかどうかを検知していた．しかし，降着装置が展開した時に発生したノイズ（false signals）をこの高感度センサーが検知してしまい，ソフトウェアは探査機が着陸したと認識し的確な減速をすることなく，軟着陸用エンジンを地表のまだ 40 メートル上空で停止させてしまった．その結果，Mars Ploar Lander は火星表面に墜落してしまった．このようなノイズの考慮はソフトウェアの開発の要件にそもそも含まれておらず，検知してしまった事で発生した事故であったと推測されている（JPL Special Review Board Report, 2000）．

JUAS のソフトウェアメトリックス調査 2016 によると，要件定義には開発工程全体のうち 20%の期間が費やされていることや，工程遅延の理由の 50%以上が要件定義の問題であること，さらには予算オーバーや品質不良においても要件定義の問題が原因の多くを占めることが 479 プロジェクトを対象に行ったアンケート調査の結果から指摘されている（日本情報システムユーザー協会（JUAS), 2016）．

以上のように，要件定義工程において，システムの構成要素における要素間の相互作用の関係が原因で，近年のシステムにおける深刻な事故や損失を引き起こす場合が多々発生している．そこで，本論文は，要件定義工程へ効果的に STAMP/STPA を適用することを考える．

1.2 課題と先行研究

STAMP/STPA の開発現場への導入について，内在する主な課題は 3 つ確認できた．第一の課題は，STAMP/STPA の使用者が，どの工程で適用するのかを明確化することである（Fleming, 2015）．第二の課題は，開発プロセスと安全解析プロセスを個々に独立して実施することなく効率的に実施できるようにすることである（Abdulkhaleq, 2017）．第三の課題は，STAMP/STPA のために作成するコントロールストラクチャのメンテナンスに時間をかけず，システムが損失を引き起こす状態に至りうるシナリオ（以下，損失シナリオ）から導出した安全要件（以下，コンポーネント安全要求）をシステム開発にすぐにフィードバックすることである（Abdulkhaleq, 2017; 独立行政法人情報処理推進機（IPA）, 2018 ）．

これらの 3 つの課題に対する先行研究の取り組みを示す．第一の課題に対して，開発の概念設計工程に着目した先行研究が存在する．STAMP/STPA では，解析の方法自体は規定しているが，実際の開発における，現場への適用プロセスについては明言されていない（Leveson, 2012）．これに対し，MIT の Fleming は，開発プロセスにおける，安全／セキュリティとコストとの関係性に着目し（Frola, 1984; Strafaci, 2008），概念設計工程での STAMP モデルをベースとした Systems-Theoretic Early Concept Analysis（STECA)という解析手法を考案した（Fleming, 2015）．この手法は Concept of Operation（ConOps)という運用定義書の利用を前提としているが，ConOps は開発するシステムについて，その運用に焦点を当てていないときや Unified Modeling Language（UML）表記法などを使用しているときには作成しない場合もあるため，適用の幅が限定されている．

第二の課題に対して，開発の設計工程以降のプロセスと STAMP/STPA の実施のプロセスをツールで結びつける先行研究が存在する．現状では，開発プロセスでの成果物である既存の開発文書から，あるいは，解析者が開発者にヒアリングすることにより，安全解析手法 STAMP/STPA 実施のためのシステムのコントロールストラクチャを新規に作成しなければならない．先行研究としては，この事を STAMP/STPA の導入を妨げる要因であると問題視して，開発の詳細設計工程以降での STAMP/STPA の実施をツール化することでサポートする動きがある（Abdulkhaleq, 2017）．しかし，STAMP/STPA 適用を考えた場合，要件定義工程での既存の開発文書では，STAMP/STPA で最も重要な事項である，「システムを構成する構成要素（ハードウェア，ソフトウェア，ヒューマンファクター）とその要素間の関係」が洗い出されて

いない．そのため，要件定義工程においては，既存の開発文書を活用することなく，システムの開発と STAMP/STPA の安全解析を別々のプロセスで実施しなければならない．

第三の課題に対して，コントロールストラクチャのメンテナンスをツールでサポートする先行研究が存在する．STAMP/STPA では，解析をおこなうためにシステムのコントロールストラクチャを作成しなければならない．実際の開発の現場では，開発の上流工程のシステム開発段階までに，STAMP/STPA のために作成したコントロールストラクチャにおけるシステムの構成要素や要素間の相互作用の追加／変更／削除が頻繁に発生する．この追加／変更／削除に対応するため，コントロールストラクチャのメンテナンスに時間がかかり，STAMP/STPA の実施が遅れてしまい，損失シナリオから導出したコンポーネント安全要求をシステム開発になかなかフィードバックできない．この課題に対しても先行研究として，先の課題のツールを開発している事例も含め，そのコントロールストラクチャの作成及び維持をサポートするツールも開発されている（Abdulkhaleq, 2017）．特に，日本の独立行政法人 情報処理推進機構はこの課題を意識して，ダイアグラムエディタとしてユーザビリティの高い，STAMP/STPA 実施のためのサポートツールを開発している（独立行政法人情報処理推進機（IPA）, 2018）．しかし，これらのツールは，あくまで STAMP/STPA で作成する図の作成やメンテナンスを，ツールとしてグラフィカルにサポートしているだけであり，既存の要件定義書を効率的に活用する形でのサポートをしていない．また，STAMP/STPA の損失シナリオから導出したコンポーネント安全要求をシステム開発にすぐにフィードバックするプロセスを提案していない．

さらに第三の課題に関する事項として，STAMP/STPA によるシステムの安全解析では，解析の抜け／漏れがないように，抽出したすべての非安全なコントロールアクションに対して解析を実施する．そして，損失シナリオから導出したコンポーネント安全要求をシステム開発へフィードバックするプロセスを基本としている（Leveson, 2012）．しかし，すべての非安全なコントロールアクションに対して解析を実施するのでは，それらの損失シナリオを特定し，コンポーネント安全要求を導出するのに時間がかかる．その結果，損失シナリオから導出したコンポーネント安全要求をシステム開発へ直ちにフィーバックすることが困難となる．STAMP/STPA での安全解析を効率的に実施できるように，その適用プロセスを Graphical User Interface（GUI）で視覚的に解析者をサポートし，実施にかかる作業の手間や時間を低減するためのツールもいくつか開発されている（Abdulkhaleq, 2017; 独立行政法人情報処理推進機（IPA）, 2018）ことを先に述べた．しかし，これらは，

STAMP/STPA の適用で抽出したすべての非安全なコントロールアクションに対して解析を実施後，損失シナリオから導出したコンポーネント安全要求を開発へフィードバックすることを基本としている． 近年の大規模化／複雑化するシステムにおいて，システムを構成するすべての要素に対して安全解析を実施するのは，有限な開発期間の中で現実的ではないとの主張がある（Cupryk, 2011）．重要なシステムの構成要素について優先的に安全解析することが実用的であり，解析の優先順位を考慮した手法は，優れた手法であるとされている（Robert, 1993）．そこで，Failure Mode and Effect Analysis（FMEA）や Probabilistic Risk Assessment（PRA）などの他の安全解析手法では，安全解析によるシステムの故障モードについての優先順位を考慮した，故障原因を解析する手法が近年，活用されている（Borgovini, 1993; 原子力委員会, 2014）．現状，安全解析手法として様々な産業で使用されている FMEA（US Department of Defense, 1949）では，単一要素の故障モードの発生確率等を使用することにより，システムの故障モードについての優先順位を考慮した手法が提案されている（Lutz, 2005; Borgovini, 1967; Collett, 1984）．また，Hazard and Operability Study （HAZOP）も近年，化学プラントなどの安全解析において広く普及している安全解析手法であるが，要件定義工程のような開発の上流では適用が難しく，また，既存安全対策の失敗確率として発生確率を考慮した手法が考案されている．（HAZOP and Plant Safety Promotion, 2018）．しかし，STAMP/STPA では，発生確率等の統計的な情報を使用することを前提としていない（Leveson, 2012; 兼本, 2018）．そのため，STAMP/STPA では統計的な情報を介在させずに解析の優先順位を考慮する手法が必要となる．

1.3 本論文の目的と新規性

本論文は，要件定義工程へ効果的に STAMP/STPA を適用することを目的とする．そのために，前節で述べた 3 つの課題を解決する必要がある（表 1）．

表　1. STAMP/STPA の開発現場への導入の課題

No.	課題
1	STAMP/STPA の使用者が，どの工程で適用するのかを明確化すること
2	開発プロセスと安全解析プロセスを個々に独立して実施することなく効率的に実施できるようにすること
3	STAMP/STPA のために作成するコントロールストラクチャのメンテナンスに時間をかけず，損失シナリオから導出したコンポーネント安全要求をシステム開発にすぐにフィードバックすること

そこで，本論文は，STAMP/STPA を適用できる，要件定義書へ追記する記載項目及びその記載ルール，解析の優先順位を考慮した手法とそれらの適用プロセスを提案する．本論文で提案した手法を用いることで，開発の上流工程である要件定義工程にて新しい安全解析手法を効果的に適用し，開発の早期でより安全性の高いシステム開発を実現することを目指す．

以上より，本論文の新規性は，以下の 3 つの事項を同時に満たす点となる．

- 適用対象とするシステムを限定せず，開発プロセスの要件定義工程と STPA による安全解析プロセスを統合している
- 部分的に STAMP/STPA を適用し，損失シナリオから導出したコンポーネント安全要求を開発プロセスの早期にフィードバックすることを可能としている
- 損失からハザード，非安全なコントロールアクションへのトレーサビリティを担保し，さらに非安全なコントロールアクションに関連するハザードの影響度に基づいてその優先順位を考慮した，逐次的な安全解析を可能としている

1.4 本論文の構成

本論文は，図 1 のような構成で成り立っている．第 1 章では，本論文の背景，課題と先行研究，目的と新規性を示し，本論文の意義について述べる．第 2 章では，本論文の緒論で言及した内容に関する，本論文で活用あるいは考慮すべき理論や手法について述べる．ここでは特に，安全解析手法と開発プロセスの概略について言及している．第 3 章では，本論文で提案する，要件定義工程へ STPA を適用する手法の構築について述べる．第 4 章では，3 章で提案した要件定義工程へ STPA を適用する手法の適用とその結果について述べる．ここでは，提案した手法を放射線治療装置へ適用する方法とその結果を示す．第 5 章では，本論文で提案した手法とその適用結果についての考察を述べる．なお，ここではこの他にも，本論文で提案した手法に関する，適用の制限事項と，第 2 章で示した従来手法との差異についても言及する．最後に，第 6 章では本論文で設定した課題や目的に対する，本論文の結論及び今後の展望を述べる．

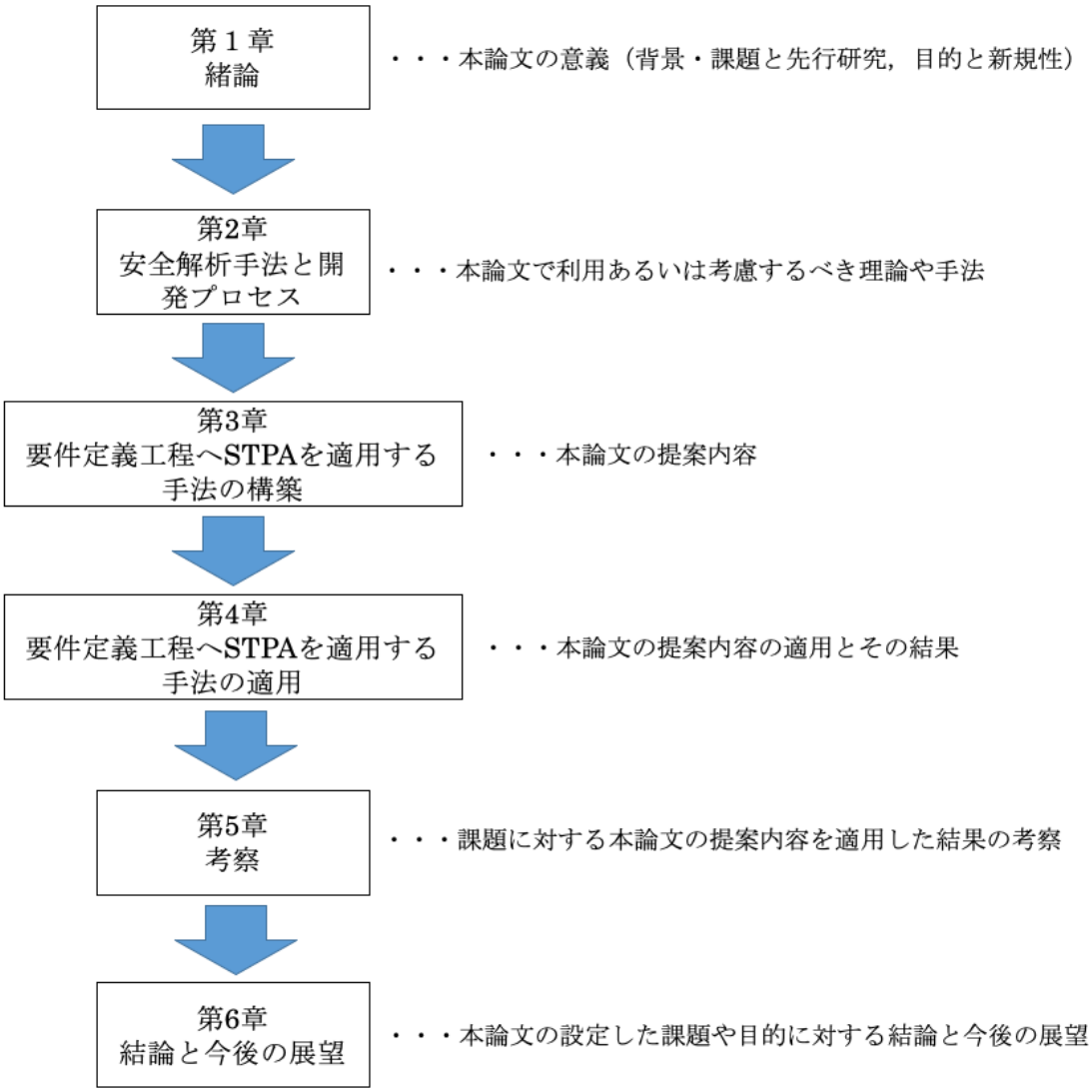


図　1．本論文の構成

図 2 では，第 3 章の本論文の提案内容と第 4 章の適用とその結果についての関係を示す．本論文の提案内容は以下の 3 つであるが，これらは第 4 章の 4.2 節，4.3 節，4.4 節と関係している．

- 3.1 節：要件定義工程でのシステム構成要素とその関係の明確化
- 3.2 節：システム開発プロセスと安全解析プロセスの統合
- 3.3 節：安全解析の優先順位づけ

なお，4.1 節では放射線治療装置への本論文の提案内容の適用についての背景を述べる．また，4.2 節では，提案内容を適用対象とした放射線治療装置（TomoTherapy）について，そのシステムの概略を述べる．

まず，3.1 節の提案内容を 4.3 節の「要件定義工程でのシステム構築要素とその関係を明確化する手法の適用」で放射線治療装置へ適用する方法を具体的に示している．そして，3.3 節の提案内容については，4.4 節の「STPA による安全解析に優先順位をつける手法の適用」において，同システムへの適用の方法を示している．なお，4.3 節と 4.4 節は，共に 3.2 節で示したプロセスに基づいて実施し，その結果を示したものである．

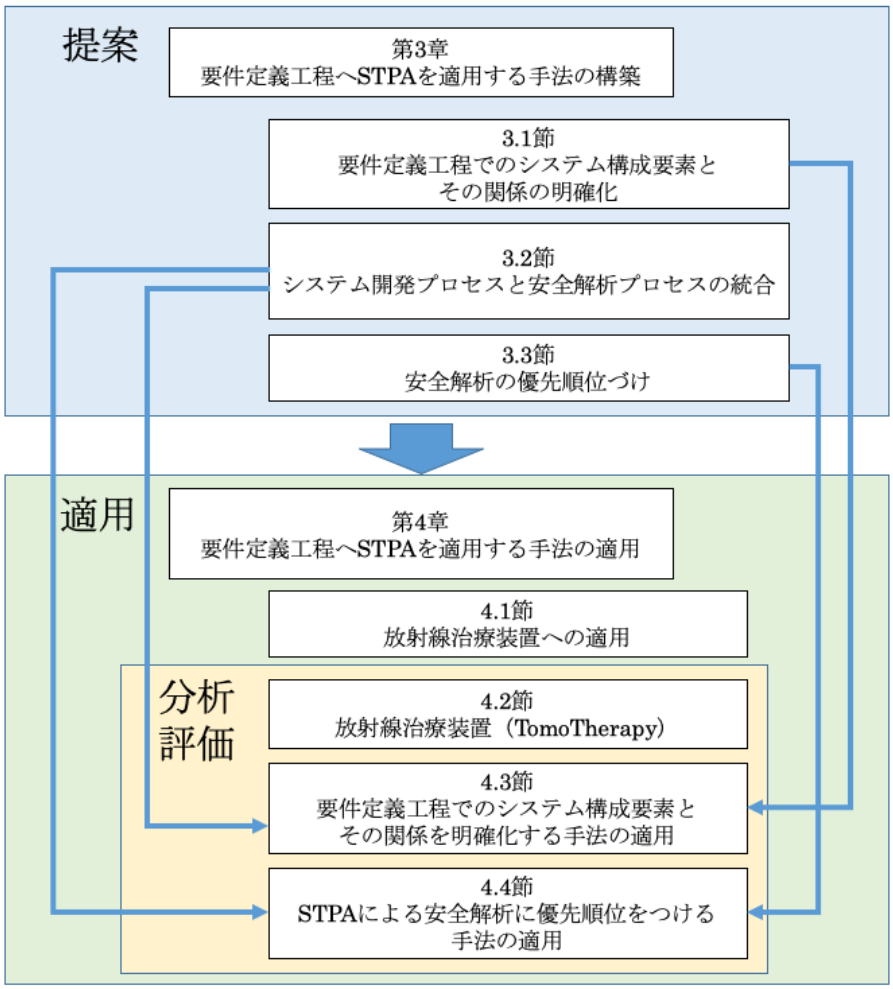


図　2．本論文の 3 章と 4 章の関係

第2章　安全解析手法と開発プロセス

本章では，様々な産業で幅広く使用されている安全解析手法とシステム開発における開発プロセスの概要を述べる．安全解析手法は，アクシデントモデルに基づき，そのモデルを実現するために手法化されている．2.1 節ではアクシデントモデルとそれらのモデルに基づく代表的な安全解析手法の概略について述べる．2.2 節では，本論文における提案内容に関わる開発プロセスと，その中で特に着目した要件定義工程及び要件定義書についての概要を述べる．さらに，開発プロセスと開発コストの関係性についても述べる．

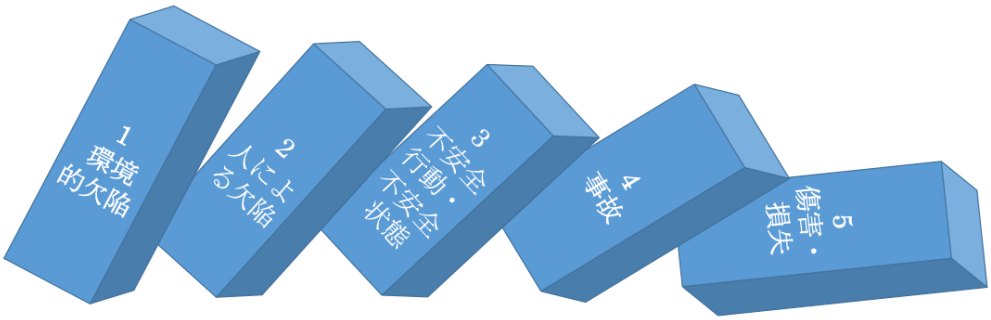
2.1 安全解析手法

2.1.1　　アクシデントモデル

2.1.1.1 Chain of Events モデル

Chain of Events モデルの代表的なものとして，ドミノモデルとスイスチーズモデルがある．従来の安全解析手法の多くは，これらのモデルに基づいた手法である．

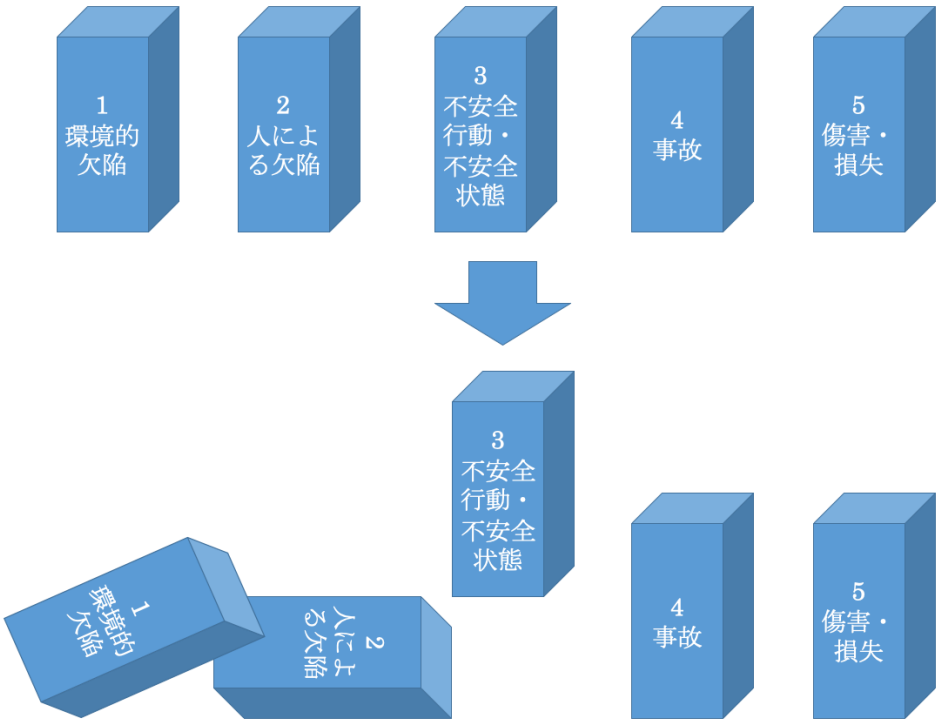
ドミノモデルは，1931 年に Herbert Heinrich により提唱された早期のアクシデントモデルである（Heinrich, 1931）．ハインリッヒのドミノモデルは，図 3 に示すように「1．環境的欠陥（Ancestry and social environment）」，「2．人による欠陥（Carelessness or personal faults）」，「3．不安全行動・不安全状態（Mechanical/physical hazard or unsafe act）」，「4．事故（Accident）」，「5．傷害（Injuries or loss）」の 5 つのドミノから構成される，事故や傷害に至るプロセスを原因と結果の連鎖として説明したモデルである．



参考文献[Heinrich, 1931]を元に著者作成

図　3. ドミノモデル

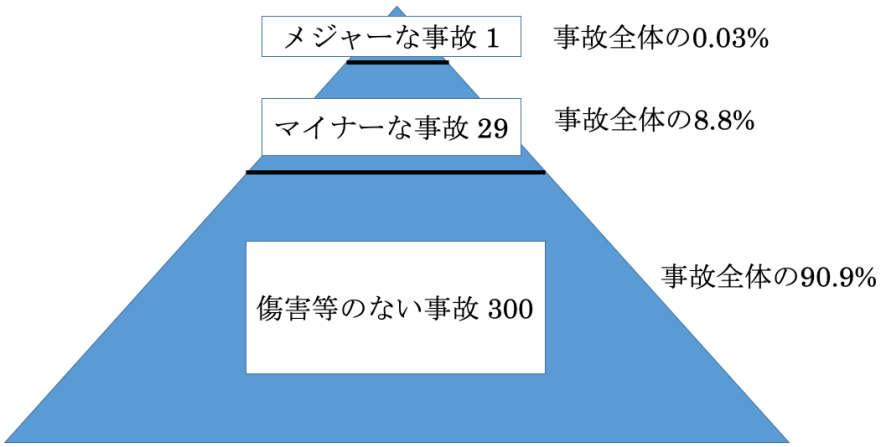
このモデルでは，1つのドミノが倒れることにより，自動的に次のドミノが連鎖的に倒れて行き，最終的に事故や傷害から災害にまで発展することを系統的に表現している．このモデルから，連鎖するドミノのうち，その一つを取り除くことによりドミノが連鎖的に倒れることを止めることができるとしている（図 4）．



参考文献[Heinrich, 1931]を元に著者作成

図　4. ドミノの連鎖を妨げることによる事故の防止

この図でも除去対象として示している通り，ハインリッヒは，5 つのドミノの中で特に除去すべき対象は「3．不安全行動・不安全状態」 であると主張している．このことは，ハインリッヒが 5,000 件以上に及ぶ事故事例を根拠にして導き出した統計的な経験則であるハインリッヒの法則に基づいている．ハインリッヒの法則とは，事故や傷害は偶発的なものではなく，1 つの重大事故（メジャーな事故）の背景には 29 の軽微な事故（マイナーな事故）があり，さらにその背景には 300 の不安全行動や不安全状態（傷害等のない事故）が存在するというものである（図 5）．これは日常的な行動の管理こそ，事故や災害を防止するために最も有効な手段であり，主体的に管理すべきであるとハインリッヒは主張している．

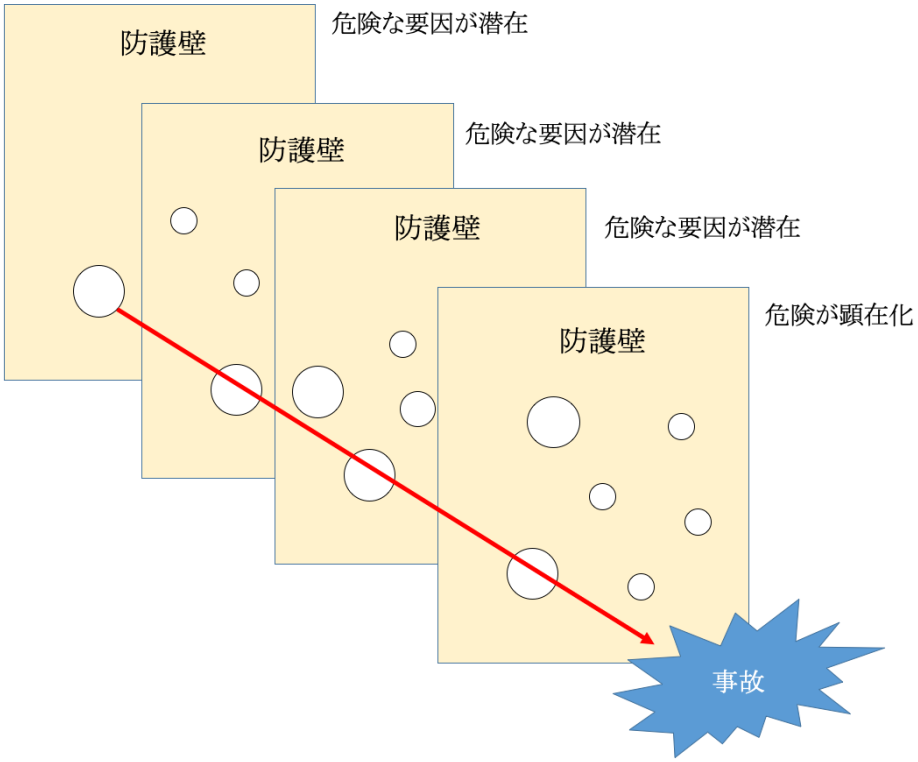


参考文献[Heinrich, 1931]を元に著者作成

図 5．ハインリッヒの法則の概念図

次に，スイスチーズモデルについて述べる．スイスチーズモデルは，英国の心理学者である James Reason が 1990 年に提唱したアクシデントモデルである（Reason, 1990）．このモデルでは，破局的な事故というのは各防護階層に生じた穴が偶然重なりあってしまった状況において，システムが持つ潜在的な危険が顕在化して発生するということを示したものである．Reason は，このことを穴の空いたスイスチーズを幾重にも並べたモデルとして例えた．

本来，防護階層が幾重にも積み重なり，互いに補完しあっている防護を採用していれば，理想的な状態において事故へとつながる可能性は極めて低い．しかし，現実において，防護の各階層にはスイスチーズのように穴（不安全状態）がある．この穴は，ヒューマンエラーや規則違反などの即発的なエラーや，企業文化等の潜在的原因によって生じるとされている（Reason, 2000）．この穴と防護階層は，固定されているように見えるが実際には，それらは揺れ動いている．この防護層は，調整，保守や試験等の間，またはエラーや違反のために，除外されることもある．そして，各層の穴においても，様々な人為的な行為や事情によりその大きさが変化したり，移動や消失したりもする．そして，現実として，その防護の各階層の穴が重なるかのように，エラーが発見の機会を次々とすり抜けていくと，最終的には重大な事故の発生に至る．Reason はこのことをスイスチーズにたとえて可視化した（図 6）．現実の事故を防ぐには穴（不安全状態）の有無を常時監視し，もし穴を発見した場合は，その穴を早急に塞ぐ必要があるとしている．



参考文献[Reason, 2000]を元に著者作成

図　6. スイスチーズモデル

2.1.1.2 STAMP モデル

Systems-Theoretic Accident Model and Processes（STAMP）モデルは，近年の事故調査／予防／アセスメント手順に使用される従来の Chain of events モデルに代わる，新しいアクシデントモデルである．Leplat らによると，最近の事故や損失は，　Chain of events　モデルでの形式ではなく，複雑で動的なプロセスの中で発生していると言われている（Leplat, 1987）. STAMP　は事故や損失を，システムを構成する単一要素の故障の問題として扱うのではなく，構成要素間における制御の問題として扱う．そのため，STAMP　は，複数の構成要素間における構成要素（以下，コンポーネント）の振る舞いや相互作用における制約に着目して事故や損失を防ぐためのモデルである．つまり，STAMP は，ハードウェア，ソフトウェア，組織，マネジメント，人に

よる意思決定，時間経過と共にリスクの高い状態に到達するシステム状態を扱うことを特徴とし，システム理論と制御理論をベースとしている（Leveson, 2004）．特に，システム理論では，以下の考え方を含むことをその特徴としている．

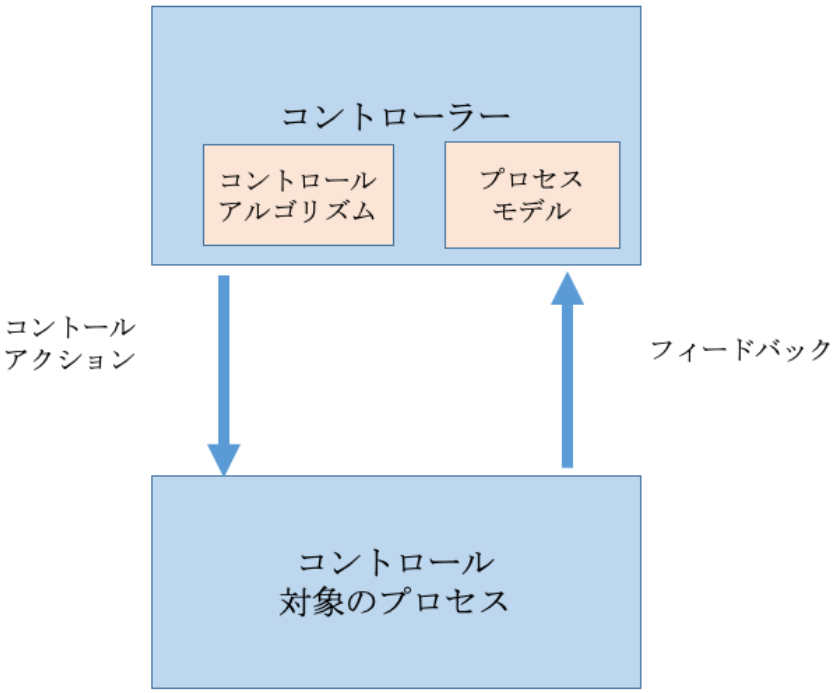
- システムを構成するコンポーネントを部品の集合としてではなく，システム全体として捉える
- システムのコンポーネント同士の相互作用の関係によって生じる創発特性に着目している
- 創発特性は全ての技術的／社会的側面を考慮することによってのみ適切に取り扱うことができ，これをシステムに調和させることができる

上記の創発特性は，コンポーネントから構成された全体が持つ，個々のコンポーネントには見られない特性であり，コンポーネントが相互作用するときに創発するものである．この創発特性が個々のコンポーネントの振る舞いやコンポーネント間の相互作用によって生じる場合，安全性／セキュリティ／保守性や運用性等の創発特性を制御するには，個々のコンポーネントの振る舞いやコンポーネント間の相互作用の制御が必要となる．この考え方に基づき，事故や損失は，システムを構成するコンポーネントの故障によって起きるのではなく，システムの中で安全のための制御を行う要素（コントローラー）と制御される要素（コントロール対象のプロセス）の相互作用が働かないことによって起きるというアクシデントモデルが STAMP モデルである（図 7）．そして，STAMP では，事故や損失を引き起こすハザードに至りうる，非安全なコントロールアクション（Unsafe Control Action（UCA））を以下の 4 つの視点と定義している．

- 与えられないとハザード
- 与えられるとハザード
- 早すぎ，遅すぎ，誤順序
- 早すぎる停止，長すぎる適用

現実の複雑なシステムは複数のレベルを持った多階層の構造として捉えられる．一般的な多層構造のコントロールストラクチャにおいて，システムの様々な階層ではコントローラーとコントロール対象のプロセスに該当するコ

ンポーネントが存在し，それぞれのレベルの構成要素は，その下層のレベルに対して，制約を課すことによって制御している．それらの相互作用が課された制約の上で，適切に働くことによりシステムの安全が実現される．この制約が破られたとき，コントロールアクションが適切に与えられず，事故や損失を引き起こす．不適切なコントロールアクションが与えられる要因として，コントローラー自身が想定するコントロール対象のプロセスの状態が，実際のコントロール対象のプロセスの状態を正しく反映できていないことが主な要因であるとされている．



参考文献[Nancy, 2012]を元に著者作成

図　7. STAMP モデルの概念図

2.1.2 FMEA/FMECA

Failure Modes and Effect Analysis（FMEA）は，設計の不完全や潜在的な欠陥を発見するために構成要素の故障モードとその上位アイテムへの影響を事故へのボトムアップ形式で解析する安全解析手法である．

FMEA は国際電気標準会議（International Electrotechnical Commission（IEC））の国際規格になっている（IEC, 2006）．FMEA は，1949 年にアメリカの軍事開発において初めて導入され（Military, U.S., 1949），1955 年にアメリカの米国海軍航空局に導入された（Dhillon, 2006）．そして，1960 年代に航空宇宙分野で採用され，アポロ計画を含め多くの NASA の開発プログラムでも適用され始めた（Stamatis, 2002; JPL, 1990; JPL, 2010）．さらに，1970 年ごろから民間航空，自動車業界や沖合石油探査にも使用され始めた（Stamatis, 2002; SAE, 1967;, National Research Council, 1981; National Academy of Engineering, 1972）．そして現在，様々な業界で一般的に使われるようになった（Duckworth, 2010）．

FMEA における故障とは機能障害（システムを構成する構成要素の構造的な破壊）を指し，この故障を引き起こした不具合が故障モードである．FMEA で使用する故障モードとは，故障状態の形式（例えば，機器における断線，短絡，折損，摩耗，特性の劣化等）による分類であり，故障そのものではなく故障をもたらす不具合事象の様式分類を示している．例えば，機器において用途も構造も異なる場合でも，電気回路を内蔵している限り，断線するという事象が起こり得る．機器あるいはモデルごとに対して発生し得る故障を全て網羅するのは不可能に近い．しかし，故障を引き起こす故障モードは類型的に分類できる．また，ある機器のモデルがどのような故障を起こすのかを直接予想することは難しいが，故障モードの類型を知ることで，そのような故障が発生する原因や発生の頻度をある程度予想することが可能となる．なお，製造工程についての故障モードの考え方を適用したものが工程 FMEA である．これは，ある工程で実施すべきであると決められていたことに違反することを故障モードとして扱う．例えば，製造工程において，その工程である部品をつけなかったことや，正しい手順でその部品をつけなかった場合が故障モードとなる．

Failure Modes and Effects and Criticality Analysis（FMECA）は，FMEA に故障モードのシステムへの影響を故障等級として定量的に評価する Criticality Analysis (CA)を考慮して拡張した手法である（Rausand, 2004）．システムの構成要素の故障モードについて，システムおよび人の安

全に及ぼす影響を評価し，定量化する．致命度（Criticality）は，構成要素の故障の影響度，故障の発生頻度や確率などの関数で与えられる．そして，得られた値を用いて優先度を推定する．この優先度は，Risk Priority Number（RPN）と呼ばれ，これは故障モードにおいける影響の厳しさ／発生頻度／検出可能性の 3 つの指標の評価点数を全て掛け合わせて算出する．

FMEA も FMECA も Chain of Events モデルに基づく安全解析手法であり，故障モードから事故や損失へのボトムアップ形式となっている．また，その解析にシステムにおける機器の故障モードを列挙することから，詳細なシステム設計書が入力情報として必要となる．そのため，システムの開発プロセスにおいて詳細設計を実施した工程以降にこの手法を用いて解析を実施する場合が多く，実際には FMEA の記載に関して図 8 に示したようなワークシート用いて解析結果を記述する．この例は蒸留脱脂システムにおける天井クレーンの動作部について FMEA を適用した結果の一部である．この FMEA の結果においては，対象としたシステムのコンポーネントごとに解析を行っている．項目としては，対象のコンポーネントについての各部品における，機能，故障モードと原因，その故障が与えるシステムあるいはコンポーネントへの影響，作業や人に与える影響，脅威のレベルが記載されている．なお，この適用はシステムの詳細設計工程で実施されたものであり，この例ではシステムにおける各コンポーネントのパーツごとについて，詳細な設計情報が利用されている（Jeffrey, 2014）．

FMEA ワークシート

プログラム: ボート製造

システム: 天井クレーン
コンポーネント: Tolley & Bridge

施設: メイン製造

日付:
作業者:

ID	製図の部分	部品名	部品の機能	故障モードと原因	システムやコンポーネントへの故障の影響	作業や人員への影響	危険Level
1	XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	巻き上げ機からの宙吊りの荷物の上げ下げのための動力源の供給する	**作動しない:** 動力源の喪失; 回路の欠陥; ベアリングの欠陥	荷物の上げ下げができない. ブレーキが荷物を静止状態にする.	影響なし（修理中のオペレーション遅延を除いて）	3
2	XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	巻き上げ機のモーターの電源が切られたときに，荷物の停止と保持のための摩耗トルクを供給する	**連動に失敗する:**スプリングの故障; ライニングの摩耗	荷物を保持する，モーターブレーキのトルクの喪失. エレクトリックロードブレーキとモーターコントロールを持つ，余剰モーターブレーキが荷物を保持する	影響なし（修理中のオペレーション遅延を除いて）	3
3	XYZ Crane Drawing 04291954-B	Main and Auxiliary Hoist Motors	巻き上げ機のモーターの電源が切られたときに，荷物の停止と保持のための摩耗トルクを供給する	**停止に失敗する:**電力の喪失	荷物の上げ下げができない. ブレーキが荷物を静止状態にする.	影響なし（修理中のオペレーション遅延を除いて）	3
4	XYZ Crane Schematic No. CV34	Main Hoist Gear Reduction Assembly	モーターから巻き上げ機のドラムへのギヤ減速中にモーターとブレーキトルクを移動し，機械的有利を与える	**離す:** ギヤ，小歯車あるいはキー金具の構造的な欠陥	荷物の持ち上げや保持に必要なトルクの喪失. 荷物の落下.	死亡あるいは重大な傷害の可能性; 装置や施設への損害	1

参考文献[Jeffrey, 2014]を元に著者作成

図　8. FMEA ワークシートの記載例

2.1.3　FTA

Fault Tree Analysis（FTA）は，故障木解析とも呼ばれ，「下位アイテム又は外部事象，若しくはこれらの組合せのフォールトモードのいずれが，定められたフォールトモードを発生させ得るのかを決めるための，フォールトの木形式で表された解析」と定義されている（日本工業規格（JIS），2000）．この FTA は，事故からのトップダウン形式で故障の組み合わせを解析するのに有効な解析手法とされている．

FTA は，ベル研究所の H・A・ワトソングループにより，1961 年に開発されたミニットマンミサイルの信頼性評価／安全性解析を目的として考案された（Watson, 1961）．その後，1990 年に IEC 61025 として国際規格になり，原子力プラントなどの工場や交通システムなどに幅広く使用されている（Vesely, 1981）．

FTA は，Chain of events モデルに基づいており，事故や損失をトップイベントとしてツリーストラクチャダイアグラムに配置する．このトップイベントから解析者はトップイベントに寄与する特定のイベントを同定して行き，フォールトツリーを構築する．FTA は，最終的に事故や損失の原因を特定していくことを解析の目標としている．FTA では，トップイベントである，その発生が好ましくない事象についての発生経路，発生原因及び発生確率をフォールトツリーのツリーストラクチャダイアグラムを用いて解析する．つまりは，発生頻度の解析のために，原因の潜在的なフォールト（機器の故障やヒューマンファクターによるエラーなどのイベント）を論理的に辿り，それぞれの発生確率を加算し，基本的な事象が起こりうる確率を算出する．

FTA の強みとして，解析者が故障の組み合わせを考慮しながらトップイベントと関連した故障を解析できることが挙げられる．加えて，FTA は解析結果を木形式（ツリー形式）のグラフィカルなフォーマットであるため，結果に対する理解を促す効果も有している．加えて，解析者はこのフォールトツリーを構築する過程において，対象となるシステムについてより深く理解することができる．

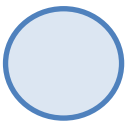
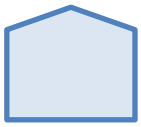
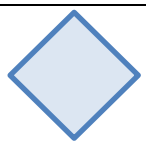
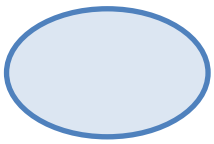
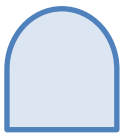
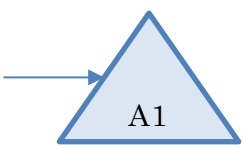
FTA のツリーストラクチャダイアグラムを作成するために表 2 に示したような記号を使用する（Jeffrey, 2014）．

ツリーストラクチャダイアグラムを構成する要素は主に 8 つ存在する．まず，四角形の記号は，事故となるトップイベントまたはそれの要因として展開される個々のイベントや調査を必要とするシステムの状態を表す．次に円の記号は，基本的なフォールトイベントを表しており，これ以上の展開を要

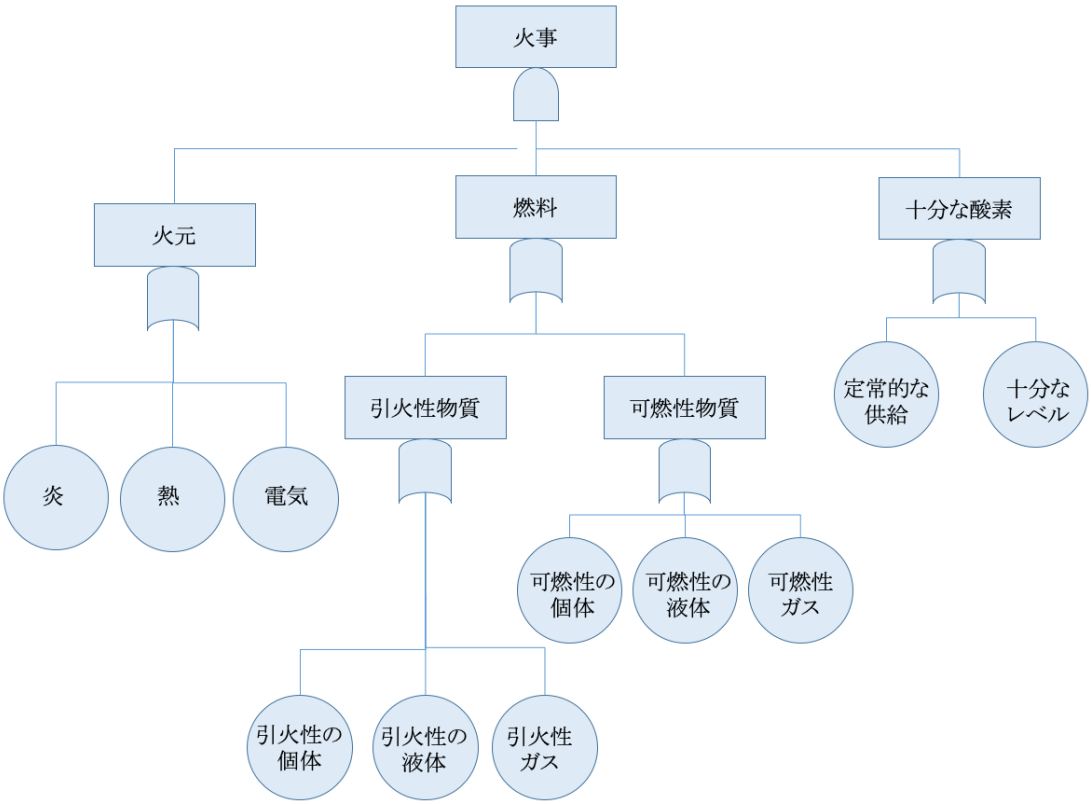
求されないあるいは，する必要がない基本的なイベントを表している．なお，重大な要因であると判断される場合，具体的な対策が必要となる．ハウスの記号は，フォールトイベントではなく，通常のオペレーションの下で起こることが期待されるイベントについてこの記号を使用する．菱形の記号は，情報が不足しているあるいは技術的な内容が不明であるため，これ以上展開されていないイベントを表す．なお，それ以後に詳細な解析ができるようになった場合には，展開されるべきである．楕円の記号は，フォールトの並びにおいて，条件となるようなイベントを表している．つまり，入力事象について，このゲートで示す条件が満たされる場合のみ出力イベントが発生する場合に使用する．AND ゲートは，全ての入力となるイベントが同時に発生するとき，出力となる事象が発生する場合に用いる記号となる．OR ゲートは，入力イベントのうち，少なくとも 1 つ以上のイベントが発生するときに出力事象が発生する場合に使用する記号である．最後に，移行ゲートは，ツリーストラクチャダイアグラム上の関連する部分への移行，または連結を表す記号である．これは，ダイアグラム上の重複した記載を避けるために用いられる．

安全解析手法の使用例としてこれらの記号を用いたフォールトツリーには Positive 型のフォールトツリーと Negative 型のフォールトツリーが存在する．Positive 型は，トップイベントとして事故や損失がない場合の FTA のフォールトツリーであり，一方，Negative 型は，トップイベントとして事故や損失という望ましくない事象をトップイベントとした場合である．（Jeffrey, 2014）．このうち，図 9 に Negative 型のフォールトツリーの作成例を示す．この例では，トップイベントに「火事」というイベントが配置され，それを展開するイベントとして，より調査が必要なイベントとして火元，火事となった燃料や酸素供給をツリーに配置している．そして最下層にこれ以上の展開を要求されない，あるいは，する必要がない基本的なフォールトイベントを配置している．

表　2. FTA の表記に使用される記号

記号	名前	説明
	四角	事象を示す．トップイベント（頂上事象）では，解決したい問題を定義する．中間事象では，要因を記載して，因果関係を明記する．
	円	基本事象を示す．フォールトツリーの最下部の事象で，これ以上展開しない事象を示す．重大な要因であると判断される場合，具体的な対策が必要となる．
	ハウス	通常のオペレーションのもと，発生が期待される事象を示す（フォールトイベントではない）．
	菱形	否展開事象と呼ばれる，これ以上あえて展開しないとした事象を示す．
	楕円	条件付き事象と呼ばる，上位の事象（結果）が発生するために両方の事象が発生しなければならない場合，別の事象の発生が条件となる事象を示す．
	AND ゲート	下位の事象（原因）の全てが発生すれば，上位の事象（結果）が発生する．
	OR ゲート	下位の事象（原因）の内，いずれかが発生すれば上位の事象（結果）が発生する．
	移行 ゲート	システムの別の部分で展開しており，フォールトツリーの別の箇所で示す．なお，リファレンスはアルファベットのコードにより作成される．

参考文献[Jeffrey, 2014]を元に著者作成



参考文献[Jeffrey, 2014]を元に著者作成

図　9. Negative 型のフォールトツリーのサンプル

2.1.4　　HAZOP

Hazard and Operability Study（HAZOP）は，設計パラメータや操作にガイドワードを組み合わせることで，意図した正常な振る舞いから逸脱したシステムのハザードとそのハザードをもたらす原因を抽出する安全解析手法である（Crawley, 2008）．HAZOP は，1960 年代に英国の ICI 社が新規科学プロセスを開発する際に安全を確保する手法として考案され，1974 年に公開された（Kletz, 2006; Lawley, 1974）．化学プラントの安全性を確保する上で重要なのは，如何に設備やシステムの潜在危険性や運転上の阻害要因を漏れなく特定することである．特定されなかった潜在危険性は，何ら対策がなされないまま放置され，いつしか事故として顕在化する恐れがある．この潜在危険性及び運転阻害要因の洗い出しを漏れなく行うため，HAZOP は化学プラ

ントの運転状態の設計意図からのずれ（プロセス異常）に着目するという考え方に基づいた手法である（Crawley, 2008; Dunjó,2010; Fields, 1988; Burns, 1993; Chudleigh, 1993; Cagno, 2002）．これは，適切に開発されたプラントは，設計意図通りの状態を維持しながら運転する限り安全であり，危険な状態や事故は，プラントに設計意図とは異なる状態となるずれ（プロセス異常）が発生した時に起こると考えられている．そのため，考えられるすべての設計意図からのずれを事前に把握し，そのずれの発生自体を防止あるいは，ずれからの危険な状態や事故への発展を防げれば，プラントは安全に維持できるものとしている．HAZAOP は，現在，他の分野においてもその有効性が認められ，電子／電気，機械，輸送システム等に対する適用ガイドラインが IEC 標準として発行されているほか，医療分野においても幅広く使用されている．また，事故や損失からのトップダウン形式あるいは，故障からのボトムアップ形式のどちらにも対応できる手法であることも幅広く使用されている要因のひとつである（Cagno, 2002; Jeffrey, 2014）．

HAZOP では，無（no）逆（reverse）他（other than）大（more）小（less）類（as well as）部（part of）早（early）遅（late）前（before）後（after）といった 11 個の標準ガイドワード（誘導語）をすべての使用について順に適用していくことを特徴としている．それにより，効果的に想定外の事象を洗い出すことが可能とされ，化学以外の様々な分野でもその適用が進んでいる．1994 年に，以下の 4 つが主要目的として言及されている（Jeffrey, 2014）．

1. 意図した機能の設計から逸脱した，すべてのシステム上の変化の原因を同定するため
2. 同定された逸脱と関連を持つ，すべての重要なハザードあるいはシステム操作上の問題特定するため
3. 行動がハザードあるいはシステム操作上の問題を制御するのに要求すべきかを決定するため
4. 上記で決定された行動が実施され，文書化されているかを確認するため

実際には HAZOP の記載に関して，図 10 に示したようなワークシート用いて解析結果を記述する．なお，HAZOP は，物に対する異常状態（故障）から安全解析を行い，ガイドワードにより導かれた異常状態に対して，要求するアクションまで詳細に解析する手法である．

この例は蒸気脱脂システムに対して HAZOP を適用した結果の一部である．この HAZOP の結果においては，対象としたシステムにおいて，その装置あるいは動作プロセスごとに解析を行っている．項目としては，ガイドワード，装置あるいは動作プロセスの逸脱状態，その状態の考えられる原因，その状態により続いて起こると考えられる結果，その防止策，Risk Assessment Code（RAC），及び推奨される防止のためのアクションが記載されている．RAC は，リスクの重要度を 1 から 4 の 4 段階（Catastrophic, Critical, Significant, Minor）とし，発生頻度も 4 段階（Frequent, Likely, Occasional, Rarely）としてマトリックスとして表現し，そのマトリックス上のどこに位置づけられるかでリスクのレベルを定義したものである（Franklin, 2015; U.S. Department of Interior, 2012; Beitia, T., 2012）．

なお，この適用においては，対象となるシステムにおける，その装置あるいは動作プロセスについての詳細なシステム逸脱状態あるいは状況が把握できる入力情報が必要となる．

HAZOP ワークシート

エリア: 蒸気脱脂

装置/プロセス: Freon 113 Transfer

日付:
チーム名:

ID	ガイドワード	逸脱	考えられる原因	考えられる結果	セーフ・ガード	RAC	推奨する対応	備考
1	フロー	フローなし	バルブ（閉）	ポンプが機能しない	エンジニアリング・デザイン; バイパス	4D	なし	なし
			ポンプ（失敗）	なし	バックアップ用のポンプ	4D	なし	なし
			ポンプ（off）	なし	バックアップ用のポンプ	4E	なし	なし
			電源（失敗）	なし	予備電源	4E	バックアップが機能していることを確認	なし
			ライン（断線・破れ）	化学物質の漏洩	手順の制御; ラインの定期点検; オペレーションの監視	3C	なし	なし
2	フロー	低フロー	ポンプ（逆流）	不十分な転送; タンクバキュームが機能しない	手順をローテションでチェックする必要性・穴と線端を適切に	3C	オペレーターのトレーニングが十分であることを確認	なし
			システム閉塞	不十分な転送; 汚染	手順をローテションでチェックする必要性・穴と線端を適切に	3B	なし	なし
3	プレッシャー	高プレッシャー	バルブ（閉）	ポンプが機能しない	手順; トレーニング	3C	なし	なし
			システム閉塞	不十分な転送; 汚染	手順をローテションでチェックする必要性・穴と線端を適切に	3B	なし	なし

参考文献[Jeffrey, 2014]を元に著者作成

図　10. HAZOP ワークシートの記載例

2.1.5　PRA

Probabilistic Risk Assessment（PRA）とは，確率論を考慮したリスク評価手法の一つである（U.S.NRC, 2018）．この手法は，システムにおける設備故障などが重なったときに発生する可能性のある事故を対象として，その発生頻度と影響度を評価して，総合的な安全性の度合を定量的に解析する手法である．近年，航空分野，海洋分野，化学プラントなど，様々な分野において使用されている（原子力委員会, 2014; 株式会社テプコシステムズ, 2019）．

PRA は，1960 年代から原子力発電所を対象とし，米国にて開発され始めた手法である．そして，1975 年 10 月に U.S.NRC にて，手法としての確立が公表された．当時公表した事故シナリオは，その発生頻度が高いものとして公表されたが当時は実際には起こりえないと考えられ，あまり注目されるに至らなかった（U.S.NRC, 1975）．しかし，1979 年に発生したスリーマイル島事故の発生したシナリオが，この過去に公表されたシナリオと類似していた．そのため，注目されるようになり，それ以後，世界各国の原子力発電所の安全研究で欠かせない技術として研究開発が進められるようになった．なお，いくつかの国では許認可上の必須項目とされている．また，米国の NASA においても 1986 年 1 月に発生したチャレンジャー号の事故を受けて，宇宙分野における PRA の手法開発が進められるようになった．そして，1989 年にガリレオ・ミッションの評価（NASA, 1989），1995 年にはスペースシャトルの評価が実施されるようになり（Fragola, 1995），NASA の国際宇宙ステーションの安全性評価においても PRA が重要な役割を果たすようになっている（NASA, 2000; NASA, 2012; Stewart, 2015）．

PRA では，重大な事故（例えば，原子力発電所においては炉心損傷など）などでその事故のきっかけとなりうる出来事（起因事象）の確率論的な発生頻度に，各種安全装置が故障などの障害により機能しなくなる確率を掛け合わせることで，事故に至る頻度の最終表を行う手法である．なお，Probabilistic Safety Assessment（PSA）と呼ばれることもある．PRA では，FTA のように，事故の防止策の成否による，事故に至るまでの進展をイベントツリーで表現する．この他にも，Event Tree Analysis（ETA）等の信頼性工学の技術を単独もしくは複数組み合わせることで，大規模なシステムの信頼性，安全性やリスクを評価するのに使用される．これをフォーマットで表現すると図 11 のようになる．

起因事象	事故防止策				
事象１	防止策１	防止策２	ケースNo.	状態	発生頻度
	→成功		1	発生せず	AA
	0.XX		2	発生せず	BB
	↓失敗	0.YY	3	発生	CC
				事故の発生頻度	CC

参考文献[株式会社テプコシステムズ, 2001]を元に著者作成

図　11. PRA フォーマットの記載例

図 11 では，イベントツリーの左端に起因事象を配置し，その右隣に防止策を配置する．そして，下へ進むごとに，各防止策を実施するようにツリーが進んで行く．各防止策の下には，その防止策の失敗確立を示す．そして，ケース No.に示された各行を 1 ケースとして，それぞれの状態とその発生頻度を記載し，最後の行にて事故の最終的な頻度を記載する．PRA によるリスク評の手順の概略を以下に示す（後藤, 2014）．

① 大規模システムの事故状態を定義する（事故の定義）
② 事故の発端を定義する（起因事象の定義）
③ 起因事象発生時の事故対策を抽出する（安全対策の抽出）
④ 起因事象発生後に大規模システムが事故状況に至るまでに実施した安全対策の成功／失敗の組合せを検討する（事故シナリオの設定）
⑤ 事故シナリオの起因事象の発生頻度と安全対策の失敗確率を積算して事故シナリオの発生頻度を算定する
⑥ 全ての事故シナリオの発生頻度を加算して大規模システム全体の事故発生頻度（事故発生リスク）を評価する

なお，実際の解析においては，ひとつの大規模システムに対し，数十種類もの安全対策を摘出する．そして，各安全対策をその構成機器の故障や人間の操作失敗という，数百から数千個の要因に分割して，それらの確率に基づいて数百の事故シナリオを定量化する．PRA ではこのような詳細化されたモデル作成のため，事故発生のリスクに対する個々の要因の寄与率の評価（重要度評価），個々の要因の発生確率分布を考慮した事故の発生頻度分布の評価

（不確実性評価），というより詳細な事故発生リスクの要因解析や結果の信頼性評価等を比較的容易に実施できることが PRA の大きな特徴であり，その利点とされている（後藤, 2014）．

2.1.6 STPA

System Theoretic Process Analysis（STPA）は，アクシデントモデルである，STAMP モデルに基づいた安全解析手法である．なお，図 12 に示したように，STAMP モデルをベースにいくつかの手法が構築されている．その代表的なものの一つとして Causal Analysis using System Theory（CAST）という，すでに発生した事故（損失）に対する，STAMP モデルの考えに基づいた事故解析手法がある（Leveson, 2012）．

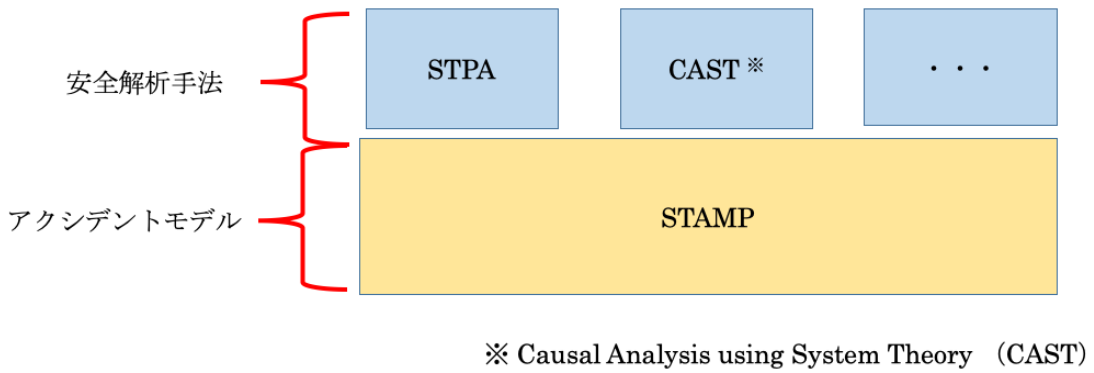


図　12. STAMP と STPA の関係

以下において，STPA の実施手順の概略を述べる（Leveson and Thomas, 2018; Leveson, 2012）．なお，本論文では，STAMP/STPA で用いられるプロセス／用語については STPA Handbook（Leveson and Thomas, 2018）に準拠している．STPA は大きく以下の 4 つの Step で構成される（図 13）．

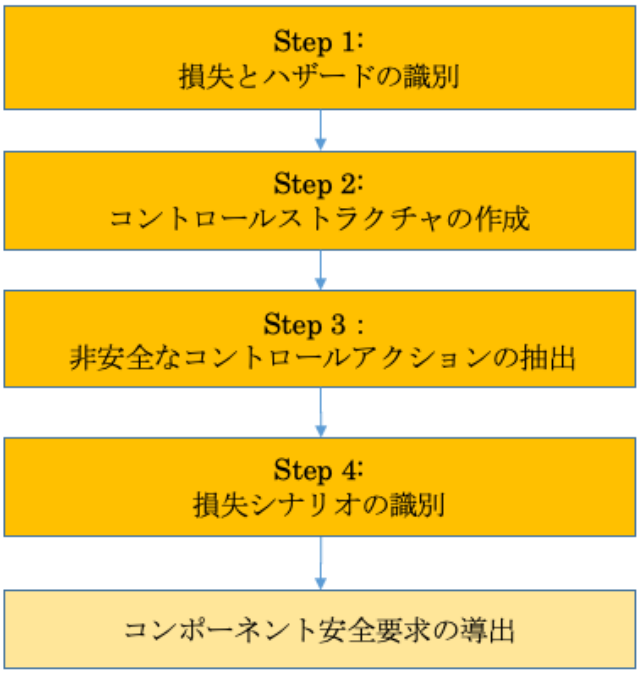


図　13. STPA による安全解析の基本ステップ

（1）Step1：解析目的の定義（損失とハザードの識別）

安全解析の対象とするシステムにおいて想定される，損失及びハザード（損失を引き起こしうるシステムの状態）を識別する．また，システムレベルの安全制約を導出する．システムレベルの安全制約とは，システムを安全に保つことを目的とした，ハザードをコントロールするために導いたシステム上の要件もしくは制約である．システムをトップダウンからモデリングしていくとまず，高レベルの安全制約が導かれる．このような高レベルの安全制約（システムレベルの安全制約）はこの段階において，全て確定するとは限らず，その後の STPA の実施によっても導出，あるいは修正されることもある．システムレベルの安全制約としては，本論文の提案内容を適用する対象とした，放射線治療装置の例を以下に挙げておく．

例）放射線治療装置での治療において，患者の治療対象となる患部は，
正しい線量の放射線が照射されていなければならない

（2）Step2：コントロールストラクチャの作成

システムにおいて，安全制約の実現に関係する構成要素（サブシステム，ソフトウェア，ハードウェア，人，組織など）及び，構成要素間の相互作用（コントロールアクション，フィードバックデータ）を解析し，コントロールストラクチャをモデル化し，作成する．図 14 に放射線治療装置における，簡略化したコントロールストラクチャの一例を示す．ここでは，コントローラーとしてオペレーターと放射線治療装置，コントロール対象のプロセスとして放射線治療装置と患者がある．これらの要素間において，コントロールアクションとフィードバックである要素間の相互作用の関係を明示して，システムにおける構成要素間のコントロールループが形成される．

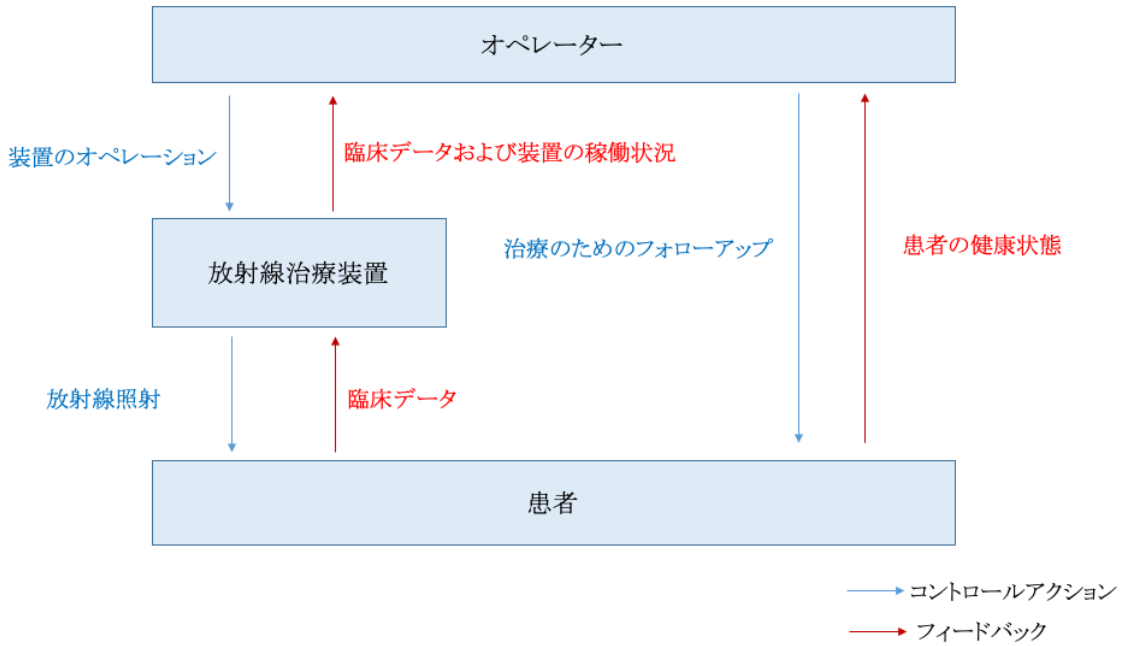


図　14. 簡略化したコントールストラクチャの一例

（3）Step3：非安全なコントロールアクション（Unsafe Control Action．以下，UCA）の抽出

コントロールアクションから，ハザードに至りうる UCA を抽出し，コントローラー制約（Controller Constraints．以下，CC）を導出する．損失を引き起こしうるシステムの状態は，UCA による結果である．STAMP モデルで定義されるように，それらは以下の 4 つの視点で起こりうる．

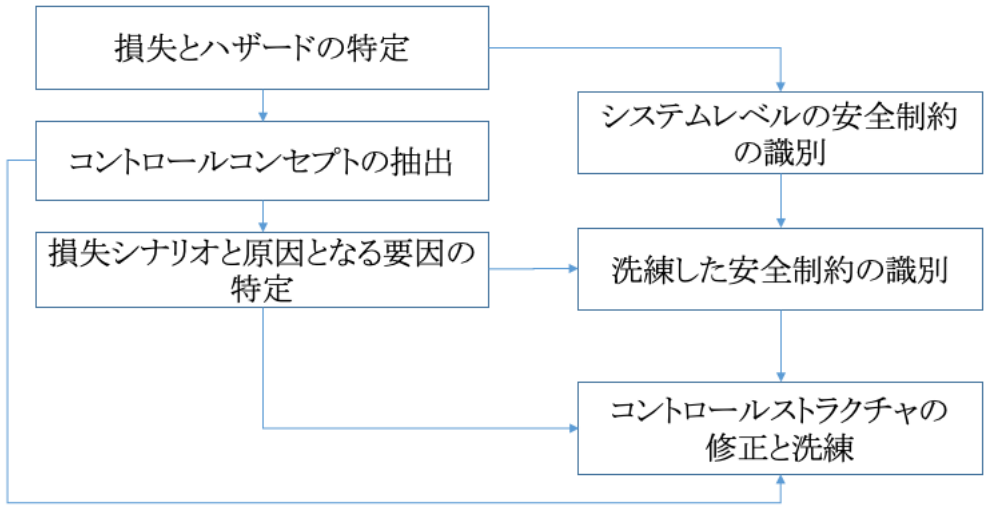
- 与えられないとハザード
- 与えられるとハザード
- 早すぎ，遅すぎ，誤順序
- 早すぎる停止，長すぎる適用

（4）Step4：損失シナリオの識別

Step3 で抽出した UCA 毎に，関係するシステムの中で安全のための制御を行うシステム構成要素（コントローラー）と制御される要素（コントロール対象のプロセス）を識別して，コントローラーとコントロール対象のプロセ

ス，コントロールループ（コントロールアクション，フィードバックから成る循環関係）に着目し，そのループを阻害するシナリオ（損失シナリオ）を識別する．そして，識別した損失シナリオの発生を防ぐための非機能要件に分類される安全要件をコンポーネント安全要求として導出する（Leveson and Thomas, 2018）．なお，システムにおける要件は，システムに実装する機能である機能要件と実装する機能以外の非機能要件として区別される．

STAMP/STPA では，解析方法自体は規定しているが，実際の開発における，現場への適用プロセスについては明言されていない（Leveson, 2012）．これに対し，MIT の Fleming は，システムの開発プロセスにおける，安全／セキュリティとコストとの関係性に着目し（Frola, 1984; Strafaci, 2008），概念設計工程での STAMP モデルをベースとした Systems-Theoretic Early Concept Analysis（STECA)という解析手法を考案した（Fleming, 2015）．図 15 に STECA による解析の流れを示す．この中で STPA と異なり，STECA の Step で特徴的なのは「コントロールコンセプトの抽出」である．この Step では，システムの概念設計で Concept of Operation（ConOps)という運用定義書の利用を前提としている．ConOps で作成された運用定義書から，必要な安全要件を自動生成することで，システム設計における潜在的なハザードと改善案の識別が可能となると主張している．また，STECA を使うことで運用定義書との安全要件に必要な情報の欠落，不一致，矛盾，脆弱性やリスクなどの識別が可能となるとしている．しかし，ConOps は開発するシステムについて，その運用に焦点を当てていないときやソフトウェア開発で UML 表記法などを使用しているときには作成しない場合もあるため，適用の幅がかなり限定されている．



参考文献[Fleming, 2015]を元に著者作成

図　15. STECA による解析の手順

STPA による解析を効率的に実施するためのサポートツールも既にいくつか開発されている．例えば，eXtensible STAMP Platform（XSTAMPP）は，ドイツの Stuttgart 大学で開発され公開されている，アプリケーションソフトウェアである（Abdulkhaleq, 2017）．このツールは Automated tool support for STPA（A-STPA）と呼ばれていたものを発展拡張させたものである．

XSTAMPP は，Eclipse の Plugin Development Environment（PDE）と Rich Client Platform（RCP）に基づいて Java で開発されており，以下の 5 つの Plugin を有している．

- Automated tool support for STPA（A-STPA）
- Automated tool support for CAST（A-CAST）
- Extended Approach to STPA（XSTPA）
- STPA Verifier
- STPA Test Cases Generator Plugin

このツールでは，STPA での安全解析を支援する基本的な機能を有しており，事故及び損失とハザードの関連付け，コントロールストラクチャとコントロールアクションの関連付け，コントロールアクション解析のための表のテンプレートの生成，コントロールストラクチャへのコントローラー及びコントロール対象のプロセスの追加等の，STPA の実施における各 Step の解析

作業をサポートしている．また，各 Step 間における成果物の変更内容の整合性をとるようなサポートも STPA Verifier などで実現し，STPA による安全解析の作業を解析者が効率的に行えるようにしている．さらに，STPA を実施した結果から，実際のテストケースを自動生成し，開発のテスト工程を支援する機能も提供している．

次に，独立行政法人情報処理推進機（IPA）は，STAMP 導入を容易にするモデリングツールとして STAMP Workbench を公開している（独立行政法人情報処理推進機（IPA）, 2018）．STAMP Workbench は，解析結果を清書する機能，解析手順のガイド機能，解析者が解析に注力できるように支援する機能を提供することで，STAMP 自体を研究する研究者向けのツールではなく，産業界で広く活用されることを目的として開発されたツールである．特に，STAMP Workbench は，解析結果を清書する機能を重視するのではなく，解析者にとって反復しながら解析を進める際に発生する手間（図表変更とその変更が引き起こす修正作業等）を問題視しており，そのような STAMP の導入を妨げる要因を排除することを目指している．このツールの特徴として，まず，はじめに，STAMP 専用の作業手順や用語，表記法を知らなくても安全解析を実施できることが挙げられる．初学者でも，このツールが提供する解析手順のガイド機能に従って作業をしていけば，STAMP に基づく安全解析を実施できる機能を提供している．次に，定型的な単純作業を可能な限りツールで自動化する機能を提供していることが挙げられる．STAMP の安全解析の作業では，特に STPA の実施においては，作画ツールで解析に必要なコントロールストラクチャを作成した後，そのコントロールストラクチャを参照しながら表作成ツールで何枚もの UCA 作成のための表を作成する必要がある．そのため，コントロールストラクチャを変更したり，解析の視点を変更したりすると，変更に対応するコントロールストラクチャや UCA の表などの変更箇所をすべて矛盾なく修正する必要があり，膨大な作業で解析者が疲弊してしまうという問題があった（独立行政法人情報処理推進機（IPA），2018）．そのため，STAMP Workbench では，手間と時間がかかり，ミスをしやすい，STAMP で作成する図表の修正作業を自動化した．これにより，解析者は手間のかかる作業から解放され，安全解析自体に集中できる機能を提供している．

2.2 開発プロセス

2.2.1 V-Model

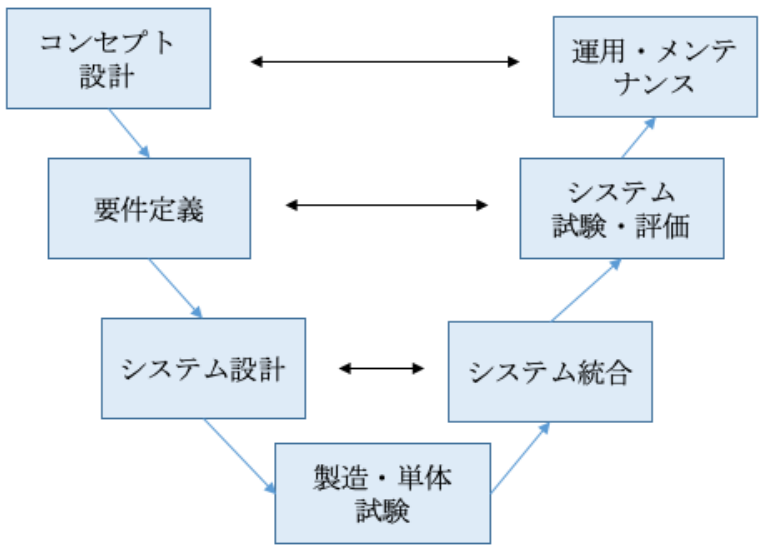
V-Model は，ドイツ政府関連のシステム開発工程を規定するために開発されたプロセスモデルである．V-Model では，システム開発において行うべき活動とその成果物を規定しており，開発のライフサイクルを表現している．図 16 に，標準的なシステムズエンジニアリングの開発プロセスである V-Model を簡略化した図を示す（Kevin, 1991; de Weck, 2011）．V-Model の左側は，システムデザインと言われる，システムの基本的な設計工程を表している．V-Model では，まず，システムの概念設計を行う．ここでは，システムの基本的な目標と制約が定義される．そして，開発初期の段階において，手戻り防止のための様々な実現可能性を検討したり，その他の解析を実施する．次の要件定義工程では，事前に合意された基本的な目標と制約を考慮して，システムに対する詳細な要求を定義する．次工程のシステムアーキテクチャ開発では，詳細な設計と開発を行う前段階として，システムの基本アーキテクチャまたは上位レベルの設計を行い，製造／試験プロセスへ進む．

一方，V-Model の右側は，開発の下流工程を示しており，システムの統合，その評価／保証と運用を実現する事を表している．V-Model では，右側と左型のレベルを合わせてあり，V-Model の左側での設計に対応した試験が，V-Model の右側で実施される．また，右側で実施される試験の事を考えて左側で設計を実施する．V-Model は，現実の開発プロセスを意図的に簡略して，その概念を示したモデルである．実際には工程間において常に多くの行き来があり，時系列として 1 つの直線となるプロセスを示すものではない．例えば，設計プロセスにおいて，その設計作業を進めていく中で発生する問題を解決していくと，元の要件を追加あるいは変更する場合が生じる．要件は当初から完全には特定されていないこととなる．

このモデルにおいて，本論文にも関わる重要な概念としてトレーサビリティ（追跡可能性）の考え方がある．非常に大規模かつ複雑なシステムは，完成するまでに膨大な文書量の詳細な仕様が記述される場合もある． V-Model の一つの側面としてドキュメント駆動の考え方があり，複雑なシステムを実現する設計作業の入力情報として，その仕様の策定は重要である．通常，そのようなシステムには多くの開発要員が費やされ，非常に長い時間をかけてその開発や運用が行われる．開発した成果物がユーザーの要求を満たし，そのシステム設計に関する意思決定が，要員間におけるコミュニケーション上の

問題が原因で混乱に陥っていないことを保証するために，誤解のない仕様の策定が必要となる．そのためにも，システムの開発／運用において，システムで開発する要素と，その要素の具体的な内容を決定するために依拠した開発工程の前提やその前工程の結果との関係性を示すことが求められる．

本論文で扱っているシステムの安全性に関して多くの場合，V-Model のような開発プロセスから独立して扱われることがある．特に，安全性に関しては開発プロセスにおける事後の保証活動として扱われることがある．安全性を事後に扱ってしまうと，安全に関する開発の上流工程における欠陥は，いつも後工程で発見され是正することができない事態となり得る．その結果，欠陥を是正する必要がないことの根拠を見つけ出すことに労力が割かれ，さらにその論拠が破綻し始めるとシステムに冗長性を持たせる，あるいはオペレーターに好ましくない運用手順でシステム上の欠陥の検知と回避をさせるような，高コスト且つ非効率な解決策へ労力が費やされる事態となる（Leveson and Thomas, 2018）．



参考文献[Kevin, 1991; de Weck, 2011]を元に著者作成

図　16. 単純化した V-Model

2.2.2 ESPR

Embedded System development Process Reference（ESPR）とは，組込みソフトウェア向けの開発プロセスガイドである（独立行政法人情報処理機構（IPA），2007）．このガイドでは，組込みソフトウェアの開発を円滑に進めるための標準的な作業やベストプラクティスを V-Model をベースとして示している．

この中で，Safety Engineering Process（SAP）として，製品として想定されるあらゆる使用形態を考慮してその状況下で製品に求められる安全性を定義し，それが確実に実現されていることを確認する作業についてのガイドがある．その SAP の中で特に，SAP1（安全性要求定義）の SAP1.1（安全要求仕様書の作成）と SAP1.2（安全要求仕様の確認）では，開発プロセスの上流工程において，安全要求の策定とその確認について言及している．

まず，SAP1.1 の SAP1.1.3（安全性実現のための要件検討）では，製品やシステムに求められる安全性の実現のために必要となる要件（安全機能）を検討し，機能ごとに安全度水準を決めるための実施内容を以下のように示している．

[実施内容]

① 製品企画書，製品仕様書，想定システム障害リストをもとに，製品に求められる安全性を考慮して，製品の安全性を実現するためにシステムに求められる安全機能の要求を洗い出す

② 安全機能はソフトウェア単独ではなく，関連するハードウェア動作なども考慮してシステム全体としての安全が保たれるように考える．特に，
   - ソフトウェアの自己監視機能
   - ハードウェアやセンサー，アクチュエータの監視機能

   などには注意を払って，システムやソフトウェアのアーキテクチャに対する安全要求を整理する

③ システムの動作モード（始動，自動，手動，半自動，定常／非定常など）に対応した安全機能を洗い出し整理する

④ システムの安全メカニズムとしてロジックの二重化やフェールセーフ，フールプルーフなどの機構の実現も検討する

⑤ システムに対する外乱や入力データの誤差，あるいは，ユーザーの操作ミスなどの可能性も含めて，これらの影響を最小化し，システムの安全性を維持するためのメカニズムを検討する

⑥ システム安全要求については，単純にシステムとして実装する安全機能以外にも，システムの使用や運用の際の方式面（システム異常時のシステム管理者やユーザーの対応など）での安全性確保などについても検討しておく
⑦ 安全な製品／システムを開発するために，使用する開発手法やツールなどについても合わせて整理しておく．特に高度な安全性が求められる場合には，開発で使用するコンパイラやツールなどを明らかにしておく
⑧ 不具合やトラブルの発生頻度とそれらによる影響度合いを考慮して，安全機能がどの程度機能することを保証するか検討し，安全機能ごとに安全性の水準（安全度水準）を決定する

また注意事項として，以下を列挙している．

[注意事項]

- システムに求められる安全性が達成され得るように，必要な安全機能については十分に詳細にその仕様を検討し整理する
- 安全機能に関する要求事項は明確かつ厳密に定義し，機能安全評価や安全性テストの局面で，検証や試験が可能であるように配慮しておく
- ソフトウェア，ハードウェア間の安全に関する制約なども全てリストアップしておく
- 開発で使用するコンパイラやツールを検討する際には，信頼性や実績を考慮する
- システムの安全度の度合い（レベル）については，IEC61508 などで提唱されている安全度水準の考え方なども参考にする

次に，SAP1.1 の SAP1.1.4（安全要求仕様書の作成）では，製品やシステムの安全性に関する要求事項を整理し，安全要求仕様書を作成することに関する注意事項を以下のように示している．

[実施内容]

① 安全要求仕様書を作成する
    - 上記検討の段階で幾つかの代替案を並行して検討してきた場合には，最終案を選択決定する必要がある
    - システムの安全設計指針やシステム使用／運用時の安全性担保の方針も合わせて整理する

- 安全要求仕様書にはソフトウェア安全機能に関する要求を含めて製品に求められる安全特性（安全機能と安全度水準）を明示しておく

また注意事項として，以下を列挙している．

[注意事項]

- 安全要求仕様書では
  - システムのトラブルなどによって安全性が損なわれた場合の影響
  - これらを未然に防ぐためのシステムとしてメカニズム
  - システム運用や使用の際に安全性を担保するための仕組み
  - システムに求められる安全度の水準

  なども明確になっていることが望ましい
- 必要に応じてユースケース分析の結果（ユースケース図，ユースシナリオなど）も加えておくと良い
- システムの安全設計指針としては，
  - 設計に関する安全性の面からの制約条件
  - 安全な設計を行うための設計手法
  - システムの安全を確実なものとするためのシステムの動作プラットフォーム
  - 既存システムの再利用による安全性の担保

  なども記載しておくとよい
- 安全要求仕様書の段階で，未確定要因がある場合には，それを明記しておく
- 文書化での留意点
  - 変更履歴を添付し，変更箇所なども明示する
  - 作成文書に関しての責任所在を明示する
  - 作成文書は構成管理および変更管理にて確実に管理する

そして，SAP1.2 では，定義したシステム安全要求事項が製品としての安全性要求を満たしているかを確認するための実施内容を以下のように示している．

[実施内容]

① 下記の視点で，安全要求仕様書の内部確認を行う

- 当該製品やシステムに関して不具合やトラブルが発生した場合に，どのような影響がユーザーやその周囲に及ぶか，その影響度合いを検討しているか
- 不具合やトラブルの発生頻度と，影響度合いを考慮して，システムに求められる安全性の水準（安全度水準）を決定しているか
- システムに対する外乱や入力データの誤差，あるいは，ユーザーの操作ミスなどの可能性も含めて，これらの影響を最小化し，システムの安全性を維持するためのメカニズムを検討しているか
- システム安全要求について，単純にシステムとして実装する安全機能以外にも，システムの使用や運用の際の方式面（システム異常時のシステム管理者やユーザーの対応など）での安全性確保などが検討されているか
- 上記を踏まえてシステムで実現すべき安全面の機能要求事項が明確になっているか

② 確認結果は内部確認レポートとして整理し，確認作業で指摘された問題およびその対応元を明記した上で，関係者に配布する．

また注意事項として，以下を列挙している．

[注意事項]

- 安全要求仕様書の確認に際しては，
  - システム開発に関係する開発者／技術者
  - 当該システムの製品仕様書，製品企画書の検討に関わったメンバー
  - 過去に類似のシステム開発に携わった技術者

  なども交えて確認を行うことが望ましい
- システムのアーキテクチャ，ハードウェア，安全性，性能効率，使用性などの視点から安全要求仕様書を確認する
- システムの安全面に関するトレーサビリティに配慮する
- 管理者は内部確認において指摘された問題事項については，解決策やその対応のためのアクションなどもあわせて記載しておくことが望ましい

2.2.3　要件定義工程と要件定義書

要件定義工程は，システム開発において，事前に合意された基本的な目標と制約を考慮して，システムに対する詳細な要件を開発する工程である．要件定義工程での活動は以下を目的としている（Project Management Institute, 2018）．

- 開発対象の複雑さとスコープを判断するために，使用環境及びシステムを解析し，システム的な観点から開発対象に対する要件を洗い出す
- 開発に必要なコスト／スケジュール／リスクを特定できるレベルまで，システムにおけるソフトウェアとハードウェアの境界を明らかにし，ソフトウェア要件及びハードウェア要件を定義し，アーキテクチャの概要を作成する

これらの目的を達成するために要件定義工程で行われる活動には以下のような活動項目がある．

- 要件定義工程の立ち上げ
- 開発対象とするシステムの解析
- 開発要件の定義
- アーキテクチャの検討
- 影響評価
- レビュー計画の策定と実施
- 要件定義結果のまとめ及びその確認

以上の活動項目の中で，要件定義書は，「開発対象とするシステムの解析」と「開発要件の定義」の活動の中で作成される．これらの活動では，開発予定のシステムに対する要求をステークホルダー毎に洗い出し，具体化する．その要求を元として，機能要件と非機能要件を洗い出す．機能要件は，システムに実装する機能であり，非機能要件は，パフォーマンス，スケーラビリティ，可用性，保守容易性，安全性，セキュリティ，管理容易性，環境面，ユーザビリティ，アクセサビリティー，データ保全性などを示す．そして，

これらの機能要件と非機能要件を記載した文書が，要件定義工程での主要な成果物でもある，要件定義書となる．

Universal Specification Describing Manner（USDM）（清水, 2010）が抜け漏れしにくい仕様書の表記法として使用されており，この記載例を図 17 に示す．USDM では各要件（例においては要求と記載されている）の理由を明記することで，仕様に対する理解を深め，要件番号と設計書の仕様番号を付与することで開発プロセスにおける各工程の成果物間のトレーサビリティを確保していることを特徴としている．

この例は，パターン 1 は要件が 1 階層として商品の在庫を管理するシステムの例を示しており，要件と理由が明確化され，ID は，要件定義後の設計仕様におけるトレーサビリティ確保のためなどのプロジェクト管理のために利用される．パターン 2 は，電子メール送受信用クライアントアプリケーションについての要件の一部を示している．これは，要件がもう一段階層化される場合を示しており，これ以上の階層化は避けた方が良いとされている（清水, 2010）．

パターン１： 要求が１階層

要求	SAL01	商品ごとに設定されている当日の売り上げ数量の予測に対して，実売データとその間に大きな開きがあるときは警告メッセージをマネージャーのPC画面に出す
	理由	すぐに原因を調べて，陳列方法の変更など適切な対応策を講じる必要がある

パターン２:要求が多階層

要求	MAL01	事前に指定された受信および送した電子メールをキーワードで検索してメーラー上で再利用したい	
	理由	メールが多くて，関連するメールを探せない	
	要求	MAL01-01	検索グループを指定する
		理由	検索グループが複数あるため
	要求	MAL01-02	いくつかのキーワードを組み合わせて検索できる
		理由	可能性のあるキーワードで探したい
		MAL01-02-1	検索したいキーワードを入力できる
		MAL01-02-2	複数のキーワードを「AND」と「OR」でつなぐことができる
		MAL01-02-3	キーワードは最大８個まで指定できる

参考文献[清水, 2012]を元に著者作成

図　17. USDM フォーマットの記載例

また，前節で示した ESPR においても，要求仕様書のフォーマットが提示されている．このフォーマットには，ソフトウェア要求定義の作業で検討した，ソフトウェアとして実現が求められる機能要求事項，非機能要求事項や制約条件などを記載する．この記載例を図 18 に示す．

文書名：要求仕様書

発行日：
作成者：
承認者：

1．概要

＜記載例＞
・本書の目的
・本書の位置づけ
・対象ユーザー
・記載範囲，記載内容など
・定義（用語，略語など）

2．システム構成

＜記載例＞
・システム全体構成
　- システム構成要素の名称／基本機能
　- ソフトウェアに求められる要求仕様

3．機能概要

＜記載例＞
・システムとして実現・提供する機能のうち，ソフトウェアで実現する機能のリストと概要

4．制約条件

＜記載例＞
・ハードウェア構成とその制約
・利用するOS，ミドルウェアなどの制約

5．ユースケースとユースケースシナリオ

＜記載例＞
・製品の利用シーンや利用コンテキストをもとにしたユースケースとユースケースシナリオ

6．機能詳細

＜記載例＞
・５項で整理したユースケースを実現する機能の詳細

7．インターフェース詳細

＜記載例＞
・製品が連動動作する周辺のソフトウェア，システムやハードウェアなどとのインターフェース

8．性能・品質等非機能要求詳細

＜記載例＞
・信頼性要求
　- システムの異常処理方式
　- システムの異常動作モードからの復帰手順や復帰方式
・使用性要求
　- ソフトウェアで実現する部分の操作性
　- ハードウェアで実現する部分との接点
・効率性要求の検討例
　- システムの実行性能（例：処理速度，起動時間，応答時間など）
　- リソース効率（例：メモリ容量，データサイズ）
・保守性要求
　- リモートメンテナンスなど保守の形式とその実現方法
・移植性要求
　- ソフトウェアユニットの独立性
・セキュリティ要求の検討例
　- 例：データ暗号化，ユーザー認証，ウィルス対策など

9．その他

＜記載例＞
・セキュリティ要求（例：データ暗号化，ユーザー認証，ウィルス対策など）
・相互運用性（例：通信プロトコルなど）
・外部インターフェース要求
　（例：連携ソフトウェアとの関数インターフェース，通信プロトコル，ユーザーインターフェースなど）

参考文献[独立行政法人情報処理機構（IPA），2007]を元に著者作成

図　18. ESPR の要求仕様書のテンプレート

この記載例示されている各項目に書くべき内容を以下に説明する．

1. 概要：文書の目的，位置づけ，記載内容などの文書の概要及び参照している文書名を記載．
2. システム構成：ハードウェアを含めたシステム全体の構成とソフトウェアの位置づけ，およびソフトウェアを取り巻く関係／条件を記載．また，システム要求仕様書やハードウェア仕様書等の関連資料から要求，条件などを整理して記載．
3. 機能概要：機能概要を箇条書きでまとめる．
4. 制約条件：制約となる条件を漏れなく記載．
5. ユースケースとユースケースシナリオ：システムを構成する機能ブロックごとにユーザーとソフトウェアとしてのやり取りを考慮し，時系列的にその流れを整理して記載．
6. 機能詳細：各機能の詳細を機能ごとに記載．
7. インターフェース詳細：インターフェース対象ごとにインターフェースの詳細を記載．
8. 性能／製品等非機能要求の詳細：機能で表現できない，性能／品質的な事項を記載．
9. その他：その他特記しておくべき事項がある場合にその内容を記載．

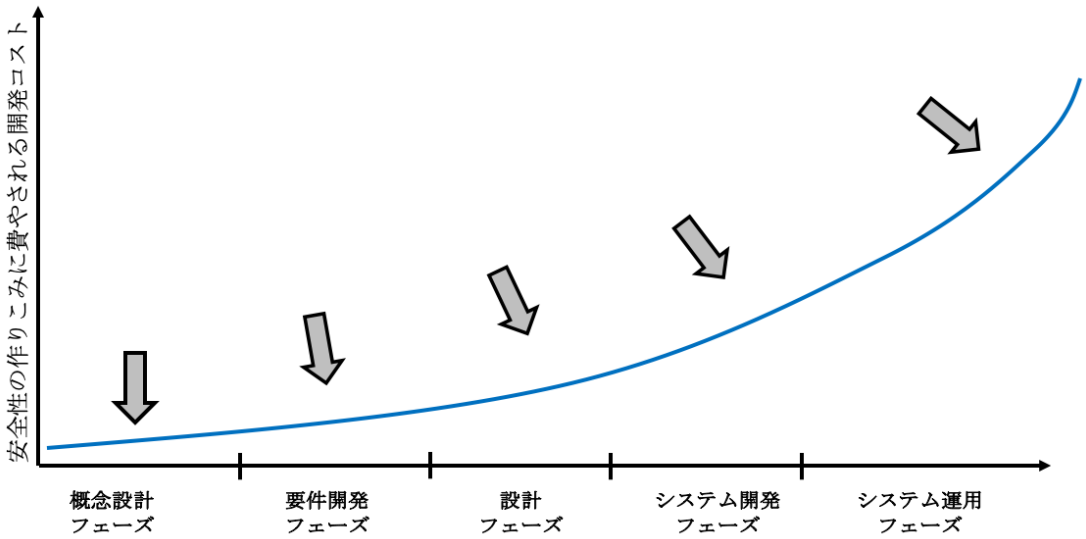
要件定義工程は，上記のようにシステム開発の根幹となる成果物を開発する工程である．それにも関わらず，1.1 節で述べたとおり，近年の深刻な事故やシステム損失は，特に，この要件定義工程に起因したものが増加している現状がある（JPL Special Review Board Report, 2000; 日本情報システムユーザー協会（JUAS), 2014）．また，JUAS のソフトウェアメトリックス調査 2016 によると，要件定義には開発工程全体のうち 20%の期間が費やされていることや，工程遅延の理由の 50%以上が要件定義の問題であること，さらには予算オーバーや品質不良においても要件定義の問題が原因の多くを占めることが 479 プロジェクトを対象に行ったアンケート調査の結果から指摘されている（日本情報システムユーザー協会（JUAS), 2016）．

2.2.4　開発プロセスと開発コストの関係

V-Model のような開発プロセスと開発コストの間には密接な関係が存在する．MIT の Young らによると，開発の早期工程で安全要件をシステム開発に取り込むことは，開発プロセス全体を通してのシステムの開発コストの削減に寄与できると主張されている（Young, 2017; Leveson, 2018）．安全やセキュリティに関しては，V-Model における開発の上流工程で検討され，その結果は安全／セキュリティ要件としてシステム全体あるいはコンポーネント群のために生成されるべきであるとされている．開発の初期段階である概念設計工程や要件定義工程では，通常，開発するシステムに関する利害関係者や使用者のニーズ解析，顧客要求の同定，規制要求の審査，実現可能性の検討，前提条件や制約条件の同定及び設計を決めるための評価基準の確立，そして要件定義の開発等の活動を実施する．また，運用コンセプトを検討する場合もある．概念設計工程や要件定義工程での開発が不十分であると，開発した成果物が顧客の要求を満たさず使い物にならなかったり，部分的にしか利害関係者のニーズを満たせなかったり，あるいは保証／保守／運用も困難なシステムを開発してしまう可能性がある．初期段階の検討不足を補うために，後工程で変更を行うが，後工程での変更はより開発コストが多くかかる結果となり，プロジェクトの失敗を招く可能性がある．特に，安全性やセキュリティについては，上流工程における検討が不十分な場合が多々ある．多くの場合は，システムの運用中に損失が発生した後の対応に重点が置かれている．また，大半の設計がすでに行われた後に安全性やセキュリティに関する追加事項へ対応することに注力されている現状がある（Leveson and Thomas, 2018）．このような後工程における変更は，開発の初期工程からシステムの安全性とセキュリティを作り込んでいた場合に比べ，より多くの開発コストが費やされる結果となる．

Frola（1984）によると，安全性に関する 70~90%の設計内容への決定はシステムの早期工程についてなされ，この決定や要件に対する変更が遅れるほど実現可能性が低くなり，また，変更対応への費用が莫大になると主張している（Frola, 1984）．このことはセキュリティでも同じであるとされている．なお，本論文においては，安全性に関するこの考え方を踏襲している．開発プロセスと開発コストの関係は図 19 のようになり，要件定義工程までにシステムについての安全性やセキュリティの要件を開発することは，システ

ム開発全体での開発費用の削減に寄与することを示している（Leveson and Thomas, 2018）.



参考文献[Young, 2017; Leveson, 2018]を元に著者作成

図　19. システム開発プロセスと安全性への対応コストの関係

第3章　要件定義工程へ STPA を適用する手法の構築

本論文では，第 1 章の 1.1 節で述べたように，システムの安全解析を開発の現場で効果的に実施するため，要件定義工程での適用が重要であると考えた．なぜなら，第 2 章の 2.2.4 節から，MIT の Young らによって，開発プロセスの要件定義工程において安全要件をシステム開発に取り込むことは，コスト面から効果的であることが示されているからである．このことは，安全要件は，開発工程が進めば進むほど，それらの要件をシステム開発に組込むコストは要件定義工程以降，より高くなっていく事を示している（Young, 2017; Leveson, 2018）．

そこで，この工程で効果的に開発現場へ STPA を適用するための，次の 3 つの事項を提案する．まず 1 つ目として，3.1 節において，システムの構成要素と構成要素間の相互作用の関係を提案するルールによって明確化できる，既存の要件定義書へ追記する記載項目及び，その記載ルールを提案する．次に 2 つ目として，3.2 節において，実際の現場適用を考慮したプロセスフローを提案する．このプロセスフローは，開発プロセスと STPA の安全解析プロセスを統合している．さらに 3 つ目として，3.3 節において，STPA を部分的に実施して導出したコンポーネント安全要求をシステム開発へすぐにフィーバックできるように，STAMP/STPA での解析対象となるコントロールアクションに優先順位をつけて解析を実施する手法とそのプロセスも提案する．以上の 3 つの提案により，緒論で述べた 3 つの課題が解決できると考える．

3.1 要件定義工程でのシステム構成要素とその関係の明確化

本節では，システムの構成要素と構成要素間の相互作用の関係を提案するルールによって明確化できる，既存の要件定義書へ追記する記載項目及びその記載ルールを示す（山口, 2018）．

まず，はじめに，STPA 適用のための要件定義書へ追加する記載項目を表 3 のように定義する．

この表において，まず一意な「ID」を持つことが管理項目の 1 つ目となる．この一意な ID は，システム開発においてシステムにおける要求／要件，設計書，テスト等とのシステム評価やシステム検証を確認するために使用される．そして，STPA においてこのような一意な ID は，STPA の Step2 で作成するコントロールストラクチャにおけるコントロールアクションを識別するために活用する．

次に「分類」は，システム要件やコントロールアクションが属する分類を示す．この分類は，大きく機能要件と非機能要件の 2 つとなり，要件やコントロールアクションはこの 2 つのどちらかに分類される．機能要件とはシステムを実現する上で実装すべき機能となる要件である．一方，非機能要件は，システムに対するパフォーマンス，セキュリティや安全性に関することなどの要件である．STPA で導出するシステムレベルの安全制約や損失から導出したコンポーネント安全要求は安全要件として，非機能要件に分類される．

「アクター」には，この表では「アクター（From）」と「アクター（to）」の 2 つが存在する．このアクター（From）というのは，コントロールアクションの主語となるものであり，STPA ではコントローラーに相当する．一方，アクター（to）は，コントロールアクションの対象となるもので，STPA のコントロール対象のプロセスに相当する．

「アクター分類（From）」と「アクター分類（to）」は，アクター（From）とアクター（to）がそれぞれ，ヒューマンコンローラーかメカニカルコントローラーかを識別するものである．STPA では，コントローラーあるいはコントロール対象プロセスが，ヒューマンコントローラーであるか，メカニカルコントローラーであるかによって，STPA の Step4 の損失シナリオの導出における，そのシナリオ導出の観点が異なる．

「コントロールアクション」は，STPA において，STAMP モデルの相互作用の関係性におけるその相互作用を明確化する．このコントロールアクションの表現にはコントローラーが行う動詞が含まれることとなる．このコントロールアクションはシステムに対する要件そのものに相当する．

最後に「アクターの責任（From）」をこの表に含めている．安全解析において，システムにおけるコンポーネント，つまり STPA におけるコントールストラクチャのコントローラーの安全責任を明確化することは重要な役割を果たす．実際に事故や損失が起こってしまった場合や，その安全解析を行う場合，各コントローラーがどこまでの安全性責任を持って，システム中に位置付けられているのかを明確化する．その責任の範囲に応じて，損失シナリオが導出され，その損失シナリオから導出したコンポーネント安全要求の内容を決めることになる．

実際の開発における要件定義書に記載する項目として，表 3 に示したもの以外には，「内容説明（ステークホルダー間での誤解を回避するため，要件の内容の詳細を記載）」，「状態（要件の検討状態を示し，未確定／確定／中止から選択）」，「新規追加／拡張／変更（当該要件が，新規追加なのか，既存の要件を拡張／変更したものかを選択）」，「確定日（要件をシステムとして実現することをステークホルダーと合意した確定日を明記）」，「備考（当該要件をシステムにて実現する上で，前提条件／制約事項や，補足事項などがあれば記載）」などが考えられる．これらは，システムを開発する上で，一般的に要件定義書の管理項目として記載される項目である．

表 3. 要件定義書における STPA 実施のための管理項目

管理項目	説明
ID	システム開発におけるトレーサビリティ確保のため，要件に一意のIDを与える．また，このIDはコントロールストラクチャにおけるコントロールアクションの番号を与えるためにも使用される．
分類	要件についての分類を示す．この分類は，機能要件か非機能要件（パフォーマンス，安全，外部インターフェース等）のどちらかとなる．通常，安全要件は非機能要件に分類される．
アクター（From）	コントロールアクションの主語となる，アクターを示す．このアクターは，STPA でのコントローラーに相当する．
アクター分類（From）	アクター（コントローラー）がヒューマンコントローラーかメカニカルコントローラーかを示す．
コントロールアクション	目的語と述語を明確化して，コントールアクションを示す．これはシステムの要件に相当する．
アクターの責任（From）	システムにおけるアクターの安全責任を明確化する．
アクター（To）	アクター（From）のコントロールアクションにおける動詞の対象となるアクターを示す．このアクターは，STPA でのコントロール対象のプロセスに相当する．
アクター分類（To）	アクター（コントロール対象のプロセス）がヒューマンコントローラーかメカニカルコントローラーかを示す．

これらの追加項目の中で最も重要なのは，要件定義工程における STPA の実施に必要な，コントローラーとコントロール対象のプロセス及び，その関係（コントロールアクション）を明確化していることである．なぜなら，STPA は，システムにおける複数要素間の相互作用に着目した手法であるからである．現状，2.2.3 節で示したようなシステム開発の現場で使われている要件定義工程における要件定義書では，STPA を実施するために必要な，複数要素間の相互作用の関係が明確に抽出されていない．したがって，この関係を要件定義工程で明らかにしなければ，本来，近年の複雑化するシステムの事故を

防ぐための安全解析である STPA を実施することができない．また既存の要件定義書に表 3 で示した項目を追加しない場合は，要件の定義作業とは独立して，STPA を実施するためだけに，コントローラーやコントロール対象のプロセスを洗い出し，コントロールストラクチャを新しく作成することになる．そのため，開発と安全解析が全く個別のプロセスとなり，その作成のコストや安全要件を考慮してシステムを開発するための要件を作成し直すメンテナンスコストも必要となる．上記を考慮するために，STPA による安全解析のための表 3 に示した要件定義書への追加項目と，先に述べた，開発において要件定義書で一般的に記載される項目を同一の要件定義書内で管理することを提案した．

次に，STPA 実施のために表 3 に示した要件定義書への追加項目を含めた場合の要件定義書への，要件の記載ルールを説明する．まず，要件定義書に追加する 1 つの要件が，STPA のコントロールアクションとなる．そのコントロールアクションに対して，コントローラーとコントロール対象のプロセスを明記する．この記載ルールを図 20 に示す．この表記では，システムの要件に対して，その主語であるコントローラー，目的語となるコントロール対象のプロセスと具体的な述語を含むコントロールアクションを記載するように明記する．このコントロールアクションを明確化することでシステム理論に基づく，システムの複数要素間の相互作用を考慮した安全解析である STPA の実施が可能となる．なお，このような表記は古典的なフィードバック制御系の一般モデルである（杉田, 1991）．

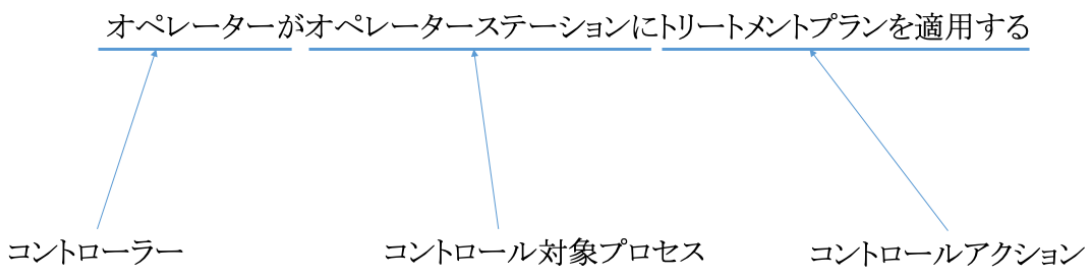


図　20. STPA 実施のための要件の記載ルール

3.2 システム開発プロセスと安全解析プロセスの統合

安全解析手法の STPA を要件定義工程に適用することを考慮し，システムの開発プロセスと本提案の要件定義書を活用するプロセスを図 21 に示した通り提案する（山口, 2018）．

図 21 の右側においては開発プロセスを示している．ここで示している開発プロセスは，V-Model としている．V-Model の上流は，基本的な設計工程を表している．この開発プロセスでは，まず，システムの概念設計を開発する．ここでは，システムの基本的な目標と制約が定義される．次の要件定義工程では，事前に合意された基本的な目標と制約を考慮して，システムに対する詳細な要求が開発される．次工程のシステムアーキテクチャ開発では，詳細な設計と開発を行う前段階として，システムの基本アーキテクチャまたは上位レベルの設計を行う． そして，システムの詳細設計と実装開発を経て，開発の下流工程へ進む．そこでは，システム統合，その評価／保証と運用を行うプロセスとなる．前述の通り，V-Model は，乱雑さを減らすために意図的に簡略化してその概念を示したモデルである．そのため，実際には工程（プロセス）間において常に多くの行き来があり，時系列として 1 つの直線となるプロセスを示すものではない．図 21 では，この V-Model の要件定義工程と，図 21 の左側に示した STPA の実施プロセス結合させている．
STPA の安全解析プロセスでは，Step1 でシステムの損失とハザードを識別する．ここで，システムレベルの安全制約が導出されるので，これらを開発プロセスの要件定義工程への入力情報としてフィードバックする．

そして，この要件定義工程において要件定義書に格納されたシステム開発に対する要件を入力情報からコントロールアクションの情報をメインとして，コントローラー，コントロール対象プロセス，コントローラーの安全責任を入力情報として，STPA の Step2 であるコントロールストラクチャの作成を実施する．そして，UCA を抽出する Step3 を実施して，コントローラー制約（CC）を識別する．その識別した CC も要件定義工程にフィードバックする．STPA の Step4 では，損失シナリオを識別する．そして，識別した損失シナリオの発生を防ぐためのコンポーネント安全要求を導出してこれらも要件定義工程にフィードバックする．以上より，本プロセスフローでの重要な点は，要件定義工程で STPA を実施し，設計工程前までに開発プロセスへ，

システムレベルの安全制約，CC と損失シナリオから導出したコンポーネント安全要求を安全解析の結果としてフィードバックすることである．

図 22 では，要件定義書から STPA を実施するプロセスの詳細（STPA の Step2 以降のプロセス）と V-Model との関係を示す．この図の左側では，要件定義工程から取得した要件定義書の情報を入力情報として，STPA を実施する以降のプロセスを詳細化したプロセスとなる．システム仕様である要件定義書の情報には，表 3 で示した管理項目が含まれており，その情報を元としてコントロールストラクチャを作成する．作成したコントロールストラクチャのコントロールアクションから，「与えられないとハザード」，「与えられるとハザード」，「早すぎ，遅すぎ，誤順序」と「早すぎる停止，長すぎる適用」の 4 つの視点より UCA を抽出する．抽出した UCA からは，コントローラー制約（CC）を識別し，要件定義工程へとフィードバックする．抽出した UCA 毎に，コントローラーとコントロール対象のプロセス間で形成されたコントロールループを阻害する，損失シナリオを識別する．そして，識別した損失シナリオの発生を防ぐための非機能要件に分類される安全要件をコンポーネント安全要求として導出し，システム開発プロセスにおけるシステム設計への入力情報とするために，それらを要件定義書に追加する．

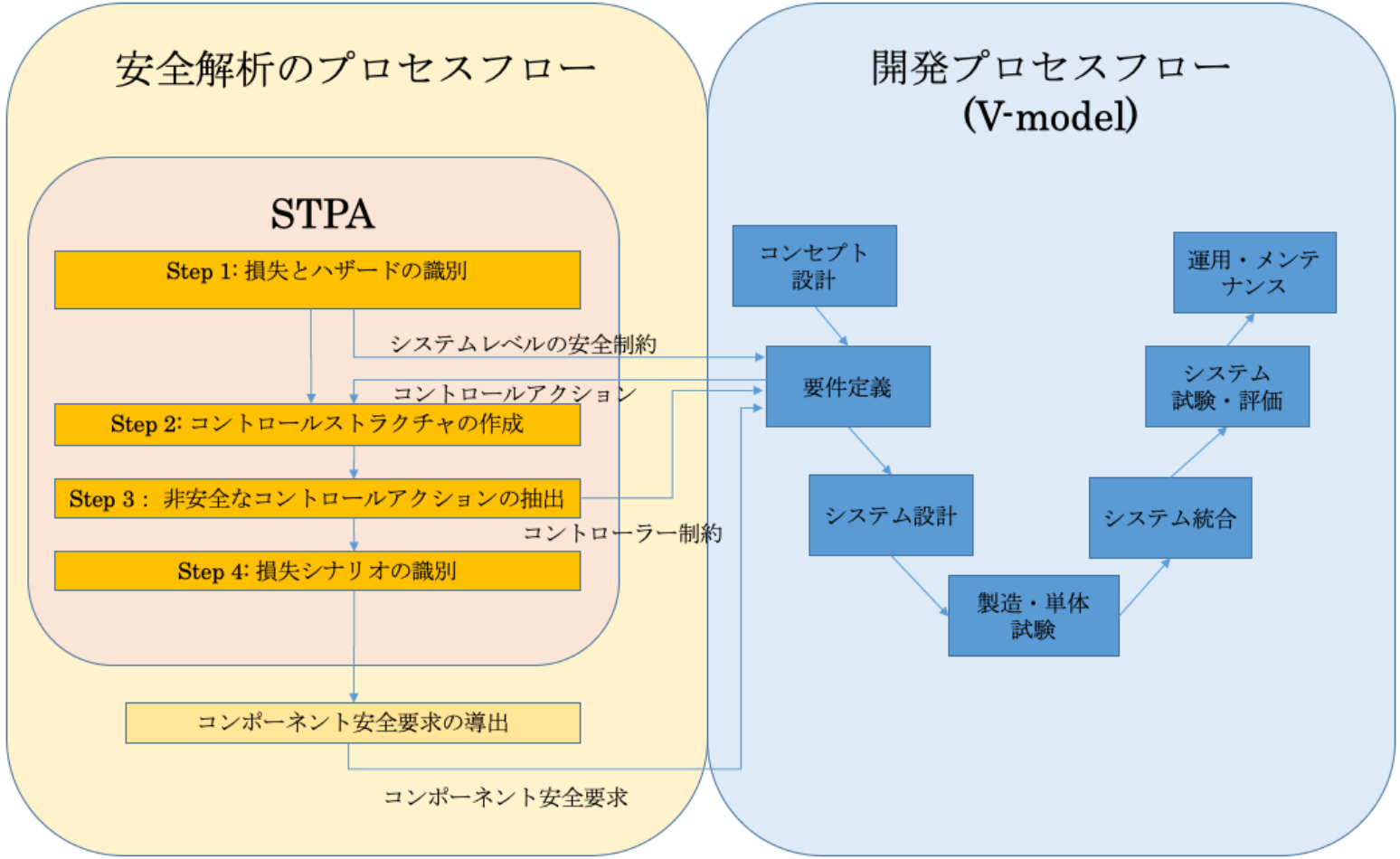


図　21. 開発プロセスフローと STPA による安全解析のプロセスフローの関係

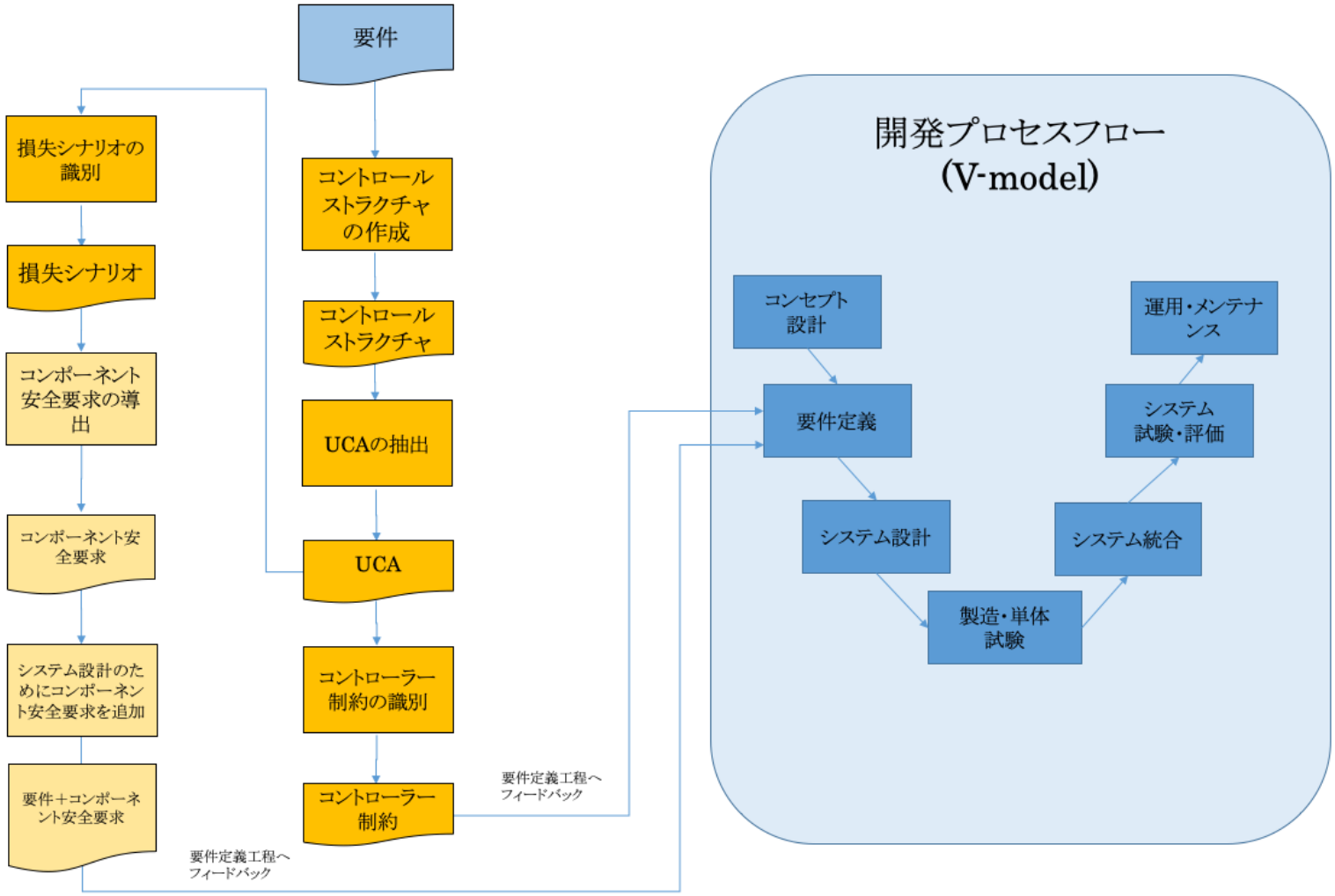


図　22. STPA による安全解析のための詳細な実施フロー

STPA で提唱されている Step をそのまま行うと，コントロールストラクチャの作成から UCA と損失シナリオの特定を全て実施することになり，多大な時間と労力を有する．それにより，STPA の損失シナリオから導出したコンポーネント安全要求のシステム開発へのフィードバックが遅れてしまう．コストや未然防止の観点からもできる限り早い段階で，部分的にでも STPA を行い，損失シナリオから導出したコンポーネント安全要求をシステム開発に早急にフィードバックすることは，開発プロセスでの安全要件をシステム開発に取り込むというコスト面における要件対応の開発効率性の観点からも有効である（Young, 2017; Leveson, 2018）．重大なシステムの事故はコントローラーとコントロール対象のプロセス間のコントロールループが停止したときに起こるので（Leveson, 2004），このコントロールループを阻害するコントロールアクションに関して開発の早期から安全解析を実施することが効果的である．本提案では，実際のシステム開発プロジェクトでの現場適用を考慮し，新しく追加された要件や変更された要件あるいは早急に安全解析における解析の優先順位の高い要件を対象として，表 3 で示した追加項目が記載された単一の要件（コントロールアクション）毎に STPA の Step3 と Step4 を実施するプロセスも提案する．コントロールストラクチャ上の特定のコントールアクションに対して STPA を実施する事により，早期開発工程において，損失シナリオから導出したコンポーネント安全要求を，システム開発における安全要件として開発へフィードバックすることが可能となる．これを示したプロセスフローと V-Model との関係が図 23 のようになる．

この図の左側において，まず，変更あるいは追加された要件を入力情報として，その入力情報が影響を与えるコントロールストラクチャ上のコントローラー，コントロールアクション，コントロール対象のプロセスおよびフィードバックの箇所を変更あるいは追加する．そして，システム全体としての整合性の観点から，更新したコントロールストラクチャの構造を確認する．それ以後のプロセスは，図 22 で示したプロセスと同じである．なお，この図の中の「コントロールストラクチャの更新」から「システム全体における整合性のチェック」までのプロセスは，早期開発プロセスへの，コンポーネント安全要求のフィードバックを目指すため，開発におけるシステムの納期や人的リソース等の状況に応じて後から実施できるものとする．

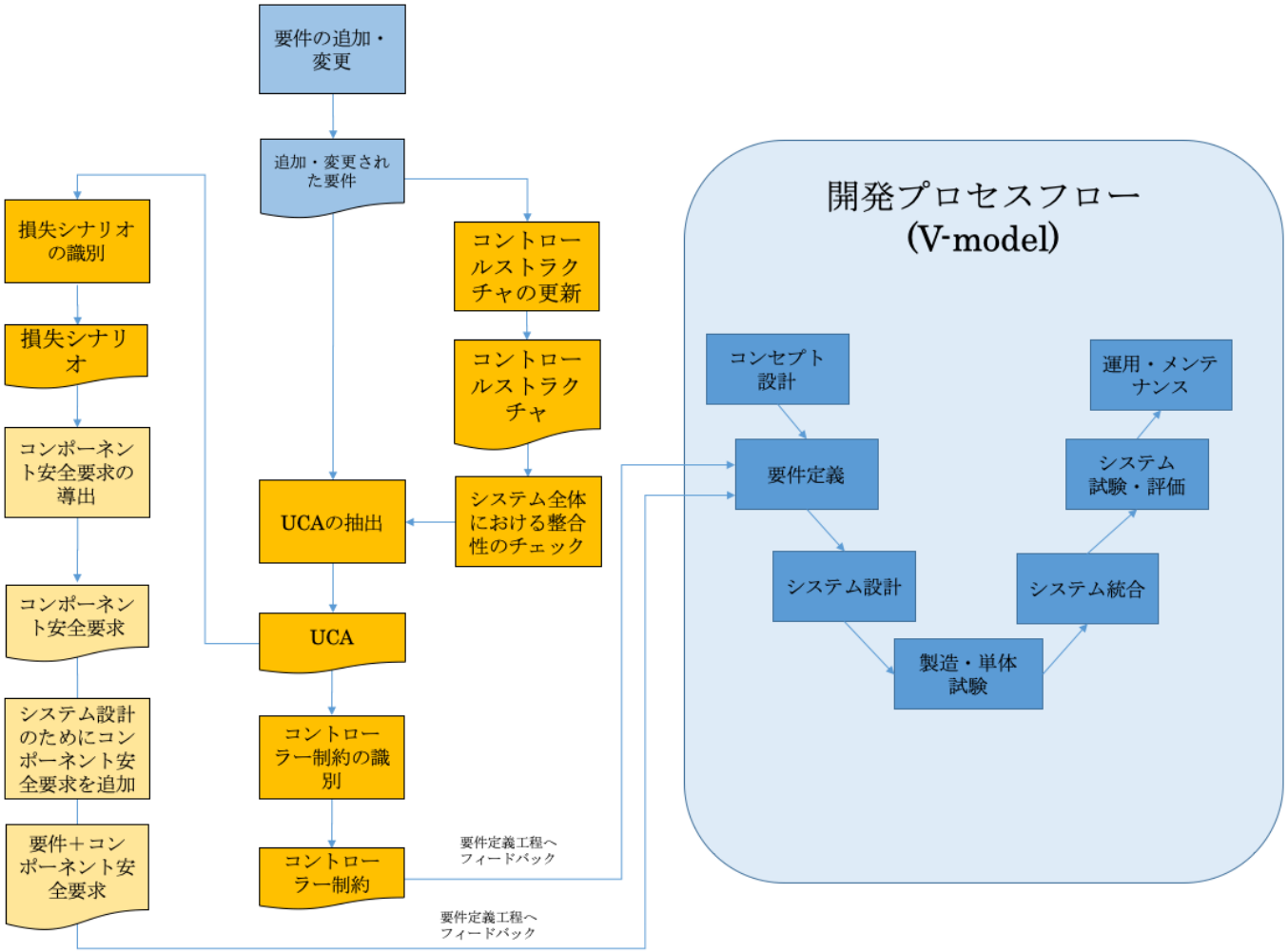


図　23. STPA による安全解析のための詳細な実施フロー（要件の追加／変更に対応）

3.3 安全解析の優先順位づけ

本節では，システム全体を構成する各要素に対して，STAMP/STPA を優先順位の高い UCA から順次解析し，損失シナリオから導出したコンポーネント安全要求を要件定義工程へ逐次的にフィードバックする手法を示す（山口，2019）．これは，STPA の Step3 で識別した UCA に対し，解析の優先順位をつけ，Step4 を逐次的に実施する．

3.2 節では，STPA を要件定義工程に適用するための，システムの開発プロセスと安全解析プロセスを統合したプロセス及び，要件定義書から STPA を実施するプロセスの詳細を示した．この詳細プロセスを基に，Step3 で識別した UCA に優先順位をつけて，Step4 を逐次的に実施するプロセスを本節では提案する．

本提案では，UCA に関連づくハザードの影響度により，各 UCA の優先順位を判断する．STPA の Step1 では，対象とするシステムで想定される，損失とハザードを定義する．そのとき，両者の関連をハザード側に明記する．そして，Step3 では，各 UCA には，Step1 で定義したどのハザードに至りうるのかを明記する．つまり，各 UCA では，Step1 で定義したどのハザードに至るのかがわかり，その損失，ハザードと UCA 間のトレーサビリティを活用して，どの損失と関連づくのかを識別できる．そこで，本手法では安全解析の優先順位の判断において，UCA と関連づくハザードの損失への影響度を使用する．図 24 に本提案内容の手順をフローチャートで示す．

なお，ハザードの影響度については，以下の影響度の評価点数（松岡，2005）を利用する．本論文ではこの評価点数を便宜的に用いるが，産業によってハザードの影響度を数値化し，汎用的に利用されている評価点数があれば，それを利用する．なお，本適用例の場合，放射線治療装置の場合は放射線の線量を考慮した誤照射事故のクラス分類に関する考え方が American Association of Physicists in Medicine（AAPM）や International Commission on Radiological Protection（ICRP）から提案されているため（AAPM Radiation Therapy Committee Task Group 35, 1993; ICRP, 2001），これを利用することもできる．ただし，本論文での提案内容は，ハザード 1 つ 1 つの点数づけに特徴があるのではなく，損失から UCA へのトレーサビリィティを利用し，UCA に総合的な点数を算出した結果から，抽出した UCA に対して優先順位をつけているところを特徴としている．

この指標を用いて，UCA に関連づくハザードの内容を確認しながら，UCA が発生する状況で関連するハザードの影響度の点数付けを行う．

[影響度の評価点数]

10：致命的，死傷，破壊
 8：重大，機能喪失，後遺症
 6：機能低下，怪我
 4：軽微，軽傷
 2：極小，無視できる

また本提案における，各 UCA の優先順位をつけるための点数の計算式を以下に示す．ここでの n は UCA が関連するハザードの数を表す．

$$Priority\ \ of\ \ UCA = \ \sum_{i=1}^{n} Severity\ \ of\ \ Related\ \ Hazard_{\mathrm{i}}$$

まず，表 3 の管理項目が記載された要件定義書からコントロールストラクチャを作成する．次に，コントロールストラクチャから，Step3 で示した 4 つの視点で UCA 及び CC を識別する．ここで識別した UCA には，Step1 で識別したハザードの ID を明記するので，損失とのトレーサビリティを確保できている．なお，図 23 の通り，著者らの先行研究（山口, 2018）では，UCA の一部についても適宜，STPA を実施していくことで，損失シナリオから導出したコンポーネント安全要求を直ちにシステム開発へフィードバックすることを意識したプロセスも示している．システム開発ではその開発中，頻繁に機能要件の追加や変更が発生し，それに伴いコントロールアクションの追加や変更が発生する．その追加／変更されたコントロールアクションに対しても部分的に Step3 以降の手順を実施する．この内容に追従したプロセスを図 24 の右側における，追加／変更した要件があると判断した場合以降のフローに示す．そして，その箇所で記載している，コントロールストラクチャにおけるシステム全体を俯瞰した，全体の整合性を確認するプロセスは，開発におけるシステムの納期や人的リソース等の状況に応じて後から実施できるものとする．

続いて，Step3 で識別した UCA に優先順位をつけ，損失シナリオを識別し，コンポーネント安全要求を導出する．そして，前述のハザードの影響度の評価点数と上記の計算式を用いて，各 UCA の点数を算出する．この点数の高いものを優先的に解析する．

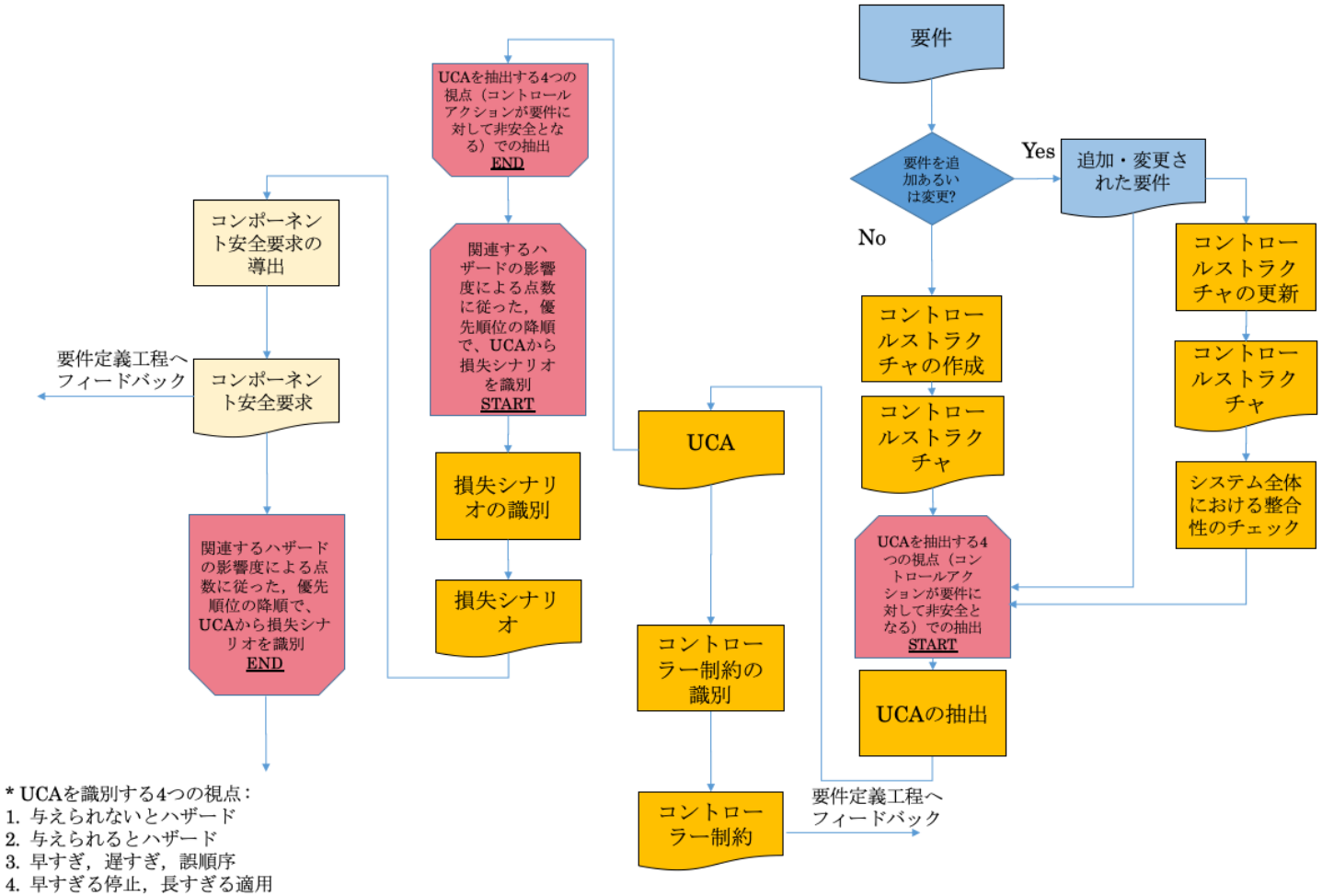


図　24. UCA の優先順位を考慮した STPA による安全解析の詳細な実施フロー

第4章　要件定義工程へ STPA を適用する手法の適用

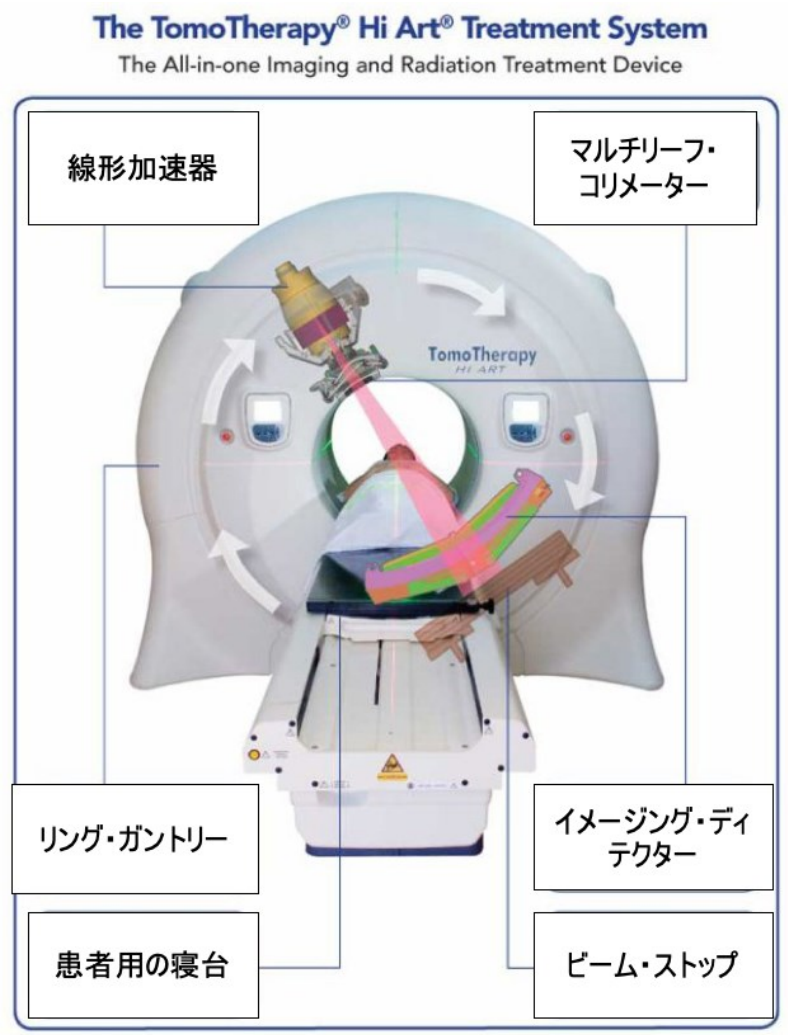
4.1 放射線治療装置への適用

医療機器分野においても，アメリカの FDA による調査によると，製品に関わるステークホルダー（患者，オペレーター，医師等）の安全確保のため，医療機製品のリコール数は近年，増加していることが示されている（Johnson, 2016; the New York Times, 2019）．その中で，放射線治療装置の放射線量の患者への誤照射による事故があったことが 2017 年に報告された（SC Times, 2017）．この報告によると，CentraCare Health Coborn Cancer Center で治療を受けていた数名の患者が過剰照射あるいは過少照射を受けたとしてヘルスケア会社，病院と担当医師が起訴された．この医療事故は，放射線治療装置が原因ではなく，患者のトリートメントプランにおける病院側のヒューマンエラーが原因の事故として報告されている（the ST. Cloud Times, 2016; Meshbesher&Spence, 2015; South Florida Times, 2015）．

そこで今回，近年の市場シェアが増加傾向にある放射線治療装置の TomoTherapy（Accuray Incorporated, 2018）を対象とし，本論文の 3 章にて提案した内容に基づき，STPA を適用した．本適用には，解析対象となるシステム情報が必要となるが，開発元の Accuray Incorporated から提供されている，システム要件が包含されているシステム情報文書を利用した（Accuray Incorporated, 2014）．

4.2 放射線治療装置（TomoTherapy）

本節では，本論文の提案内容に基づいた STPA の適用対象とした，放射線治療装置である TomoTherapy の，システムとしての概略を述べる．
TomoTherapy はアメリカの Accuray 社によって開発された，X 線を用いた放射線治療装置である．本装置は，強度変調放射線治療（Intensity-Modulated Radiation Therapy（以下，IMRT））及び画像誘導放射線治療（Image-Guided Radiation Therapy（以下，IGRT））を併用した，コンピューター断層撮影装置(Computed Tomography（以下，CT))と一体化された，放射線治療装置及びその制御コンピューターシステムである．
図 25 に TomoTherapy のトリートメントシステムの概略図を示す（Jaffray, 2007）．TomoTherapy は，大まかに，線形加速器（Linear Accelerator（LA）），マルチリーフ・コリメーター（Multi-Leaf Collimator（MLC）），リング・ガントリー，患者用の寝台（カウチ），イメージング・ディテクターとビーム・ストップから構成される．この装置では，治療において，放射線が患者の腫瘍に対して複数方向から照射される．基本的には，線形加速器がリング状のガントリー内を連続して回転して，リングの中心に向けて放射線を照射する．患者は，寝台上に乗り，この寝台がリングの奥へと進む．そして，患者の腫瘍部位に対して，放射線が照射される．放射線照射中，線形加速器に付帯するマルチリーフ・コリメーターの動きを高性能コンピューターシステムでコントロールすることによって，線量集中性が高く且つ線量均一性に関して自由度の高い線量分布を作成することができる．それにより，従来の放射線治療装置と比較して正常組織への被曝を低減させ，照射対象となる腫瘍の形状に合わせた放射線照射が実現できる．
従来の放射線治療では患者の皮膚表面に記してあるマーキングに基づいて照射を行なっていた．そのため，各回の治療毎に，照射される部位への誤差（放射線量や位置）が大きいという問題があった．しかし，TomoTherapy では CT 撮影を各回の治療前に実施して照射位置を補正することで，放射線による正常組織の被爆を低減し，高い精度での治療の実施を実現している．



参考文献[Jaffray, 2007]を元に著者作成

図　25. TomoTherapy のトリートメントシステムの概略図

4.3 要件定義工程でのシステム構成要素とその関係を明確化する手法の適用

本節及び次節にて，開発元の Accuray Incorporated から提供されている，システムの機能要件が包含されているシステム情報文書から取得できる情報を利用して，本論文の提案内容を活用した STPA の適用を示す．本節では，3.1 節にて提案した内容の適用のため，STPA の Step2 までの結果を示している．なお，この適用では，上記のシステム情報文書から得られる情報をもとに実施したものであるため，その結果においても，システム情報文書から識別した範囲に限定した結果となっている．つまり，必ずしも厳密な解析を行った結果を本論文で示しているのではなく，あくまで提案する手法の適用を以下で示している．

まず，STPA の Step1 では，解析の目的の定義段階として損失とハザードを識別する．今回の放射線治療装置における損失の一部と，それに対して本論文の以後の解析に関係する可能性があるハザードは以下のようになる．

[損失]

Loss 1（L1）：治療中の放射線照射において，患者の身体が重大な損傷や命の危険に晒される

Loss 1（L2）：患者の症状が悪化する

[ハザード]

Hazard 1 (H1)：患者の正常な組織に放射線が照射される（L1）

Hazard 2 (H2)：患者の患部が，治療において望ましい線量より過剰な線量にさらされる（L1, L2）

Hazard 3 (H3)：患者の患部が，治療において望ましい線量より少ない線量にさらされる（L2）

なお，STPA の安全解析において，上記以外の，損失やハザードとして識別したものがいくつか考えられる．それらは，STPA の Step1 のガイド（Leveson, 2012）に従うと，表 4 と表 5 のようになるため，ここで例示しておく．

表 4. システムの損失

No.	損失
L1	治療中の放射線照射において，患者の身体が重大な損傷や命の危険に晒される
L2	患者の症状が悪化する
L3	治療中に，放射線照射以外の身体的な被害により，人が死亡あるいは重大な傷害を受ける
L4	装置を喪失あるいは損傷する（ミッションを達成できない）
L5	周囲環境へ放射線が漏洩する

表 5. ハザードとシステムレベルの安全制約

ハザード	ハザードの定義	システムレベルの安全制約 （System-level safety Constraints（SC））
H1.患者が間違った線量の放射線にさらされる（a）（L1）	患者の正常な組織に放射線が照射される	[SC-1] 正しい治療箇所が正しい線量の放射線に照射されなければならない
H2. 患者が間違った線量の放射線にさらされる（b）（L1, L2）	患者の患部が，治療において望ましい線量より過剰な線量にさらされる	[SC-2] SC-1 と同じ
H3. 患者が間違った線量の放射線にさらされる（c）（L2）	患者の患部が，治療において望ましい線量より少ない線量にさらされる	[SC-3] SC-1 と同じ
H4. 患者ではない者が放射線にさらされる（L2）	患者ではない者（オペレーター等の医療従事者）が誤って装置からの放射線にさらされる	[SC-4] 患者ではない者（オペレーター等の医療従事者）が誤って装置からの放射線にさらされてはならない
H5. 放射線治療システムが放射線照射以外の身体的な被害を人に与える（L3）	放射線治療システムのオペレーション中あるいは治療中に，人々が装置によって，放射線照射以外の身体的な被害を受ける	[SC-5] 放射線治療システムは，オペレーション中あるいは治療中に，人々に放射線照射以外の身体的な被害を与えてはならない
H6. 装置が不必要な負荷（ローディングタイム等）にさらされる（L4）	装置が不必要な負荷（ローディングタイム等）のため，適切に動作しないあるいは故障する	[SC-6] 装置は不必要な負荷（ローディングタイム等）にさらされることなく，適切に動作しなければならない

H7.放射線治療装置の周囲環境が放射線にさらされる（L5）	放射線治療装置の周囲環境が装置から照射された放射線にさらされる	[SC-7] 放射線治療装置の周囲環境は装置からの放射線照射にさらされてはならない
H8. 放射線治療が患者に与えられない（L2）	放射線治療が必要な患者に対して，放射線治療が実施されない	[SC-8] 放射線治療はそれを必要とする患者のみに実施されなければならない

STPA の Step1 では，識別したハザードからシステムレベルの安全制約が導出される．また，表 5 にシステムレベルの安全制約も示す．上記の H1 から H3 のハザードについては，「正しい患者の患部が計画された適正な放射線量で治療されなければならない」という案件がシステムレベルの安全制約となる．なお，このシステムレベルの安全制約は，要件定義工程へシステム開発のための，安全要件を開発へ取り込むためにフィードバックする．

次に STPA の Step2 を実施する．ここではコントロールストラクチャをモデル化し，作成する．そのためには，解析対象となるシステムの構成情報が必要となる．システム要件が包含されているシステムに関する情報は，前述の通り，Accuray Incorporated から提供されており，本適用ではそれを利用する（Accuray Incorporated, 2014）．

TomoTherapy では主に，次の 3 つのメカニカルコントローラーからのシステムとして構成されている．

- オペレーターステーション
- トリートメントプランニングシステム
- トリートメントシステム

まず，オペレーターステーションの役割を説明する．オペレーターステーションは，患者のトリートメントプランを作成するための処理を実行する．そして，オペレーターによって作成されたトリートメントプランに従って，患者に対して正確かつ適正な放射線治療を実施するようにトリートメントシステムを制御する．また，トリートメントルームの状態を放射線治療に適した状態となるように制御する．オペレーターステーションの機能としては，以下が挙げられる．

- トリートメントプランニングシステムの制御によるトリートメントプランの作成
- トリートメントルームの状態（温度，湿度等）の監視および制御
- 治療中における照射対象となる腫瘍の形状に合わせた放射線照射量の制御／ガントリー内の寝台の位置の調整／各種情報の登録／画像取得／放射線照射パラメータの設定
- 放射線治療装置本体の起動／緊急停止ボタンによる緊急停止／停止／稼働状況等のオペレーションの制御

次に，トリートメントプランニングシステムの役割について説明する．トリートメントプランニングシステムは，オペレーターステーションを介したオペレーターからの命令により患者のトリートメントプランを作成する．また，患者の情報やトリートメントプランを蓄積する．作成したトリートメントプランは，トリートメントシステムに供給される．

トリートメントシステムは，患者のトリートメントプランに従って正確に放射線治療を実施することを主要な役割としており，トリートメントシステムは，患者の患部の CT 画像や解剖学的構造のデータをデータサーバーへと蓄積する．放射線治療の実施においては，ガントリー／マルチリーフ・コリメーター（MLC）／線形加速器（LA）／ビーム・ストップの動作制御を行う．

上記の要素に加え，TomoTherapy の使用に際して，ヒューマンコントローラーとなるのは，オペレーター，患者の 2 つの要素（ヒューマンコントローラー）となる．

まず，オペレーターは，最新のトリートメントプランに応じて，オペレーターステーションを介して患者に対する放射線治療を実施する責任を持つ．治療実施のために，治療中や治療前後において患者に指示を与え，適切な放射線治療を実施する．そのため，実施すべき項目としては，以下が挙げられる．

- 患者の個別識別情報を検証する
- 治療中あるいは治療前後における動作支持を与える
- 患者の最新のトリートメントプランを確認して治療に適用する
- 患者の臨床情報（CT 画像，トリートメントプラン，トリートメント履歴）を分析する
- 放射線治療のスタート／ストップ等の操作を実施する

次に患者ついては，対象となる患部に対して治療を受ける役割となる．そのため，治療や他の構成要素のアクションに対して自身が把握している適切な情報をフィードバックする必要がある．

以上のシステム構成要素が，ヒューマンコントローラーあるいはメカニカルコントローラーとなり，それぞれの役割とコントロールアクションの一覧を表 6 に示す．なお，表 6 は，前述のシステム要件が包含されているシステム情報文書から取得できる情報から，表 3 の項目に相当する内容を抽出して作成したものである．

表　6. TomoTherap システムにおけるコントローラーの説明

No.	コントローラー	役割	コントロールアクション
1	オペレーター（セラピスト）	・最新のトリートメントプランに応じて，オペレーターステーションを介して，患者に対する放射線治療を実施する責任を持つ． ・治療実施のために，治療中や治療前後において患者に指示を与え，適切な放射線治療を実施する．	・患者の個別識別情報を検証する． ・治療中あるいは治療前後における動作指示を与える． ・患者の最新のトリートメントプランを確認して治療に適用する． ・患者の臨床情報（CT 画像，トリートメントプラン，とトリートメント履歴）を分析する． ・放射線治療のスタート／ストップ等の操作を実施する．
2	オペレーターステーション	・トリートメントプランを作成するためのコマンドやその作成されたトリートメントプランに従って，患者に適切な放射線治療を提供するためにトリートメントシステムを操作するコマンドを発する．	・トリートメントプランニングシステムの制御によりトリートメントプランを作成する． ・トリートメントルームの状態（温度，湿度等）を監視および制御する．

		・トリートメントルームの状態（温度／湿度等）を放射線治療に適した状態となるように制御する.	・治療中における照射対象となる腫瘍の形状に合わせた放射線照射量を制御／ガントリー内の寝台の位置を調整／各種情報を登録／画像を取得／放射線照射パラメータを設定する. ・放射線治療装置本体を起動／緊急停止ボタンにより緊急停止／停止／稼働状況等のオペレーションを制御する.
3	トリートメントプランニングシステム	・オペレーターステーションを介したオペレーターからの命令により患者のトリートメントプランを作成する. ・患者の情報やトリートメントプランを蓄積するコマンドを発する.	・作成したトリートメントプランをトリートメントシステムに供給する.
4	トリートメントシステム	・トリートメントシステムは，患者のトリートメントプランに従って正確に放射線治療を実施する.	・患者の CT 画像や解剖学的構造データをデータサーバーに蓄積する. ・患者に放射線治療を実施する（ガントリー／マルチリーフ・コリメーター（MLC）／線形

		・トリートメントシステムは，患者の CT 画像や解剖学的構造データをデータサーバーに蓄積する.	加速器（LA）／ビーム・ストップの動作制御）.
5	患者	対象となる患部に対して放射線治療を受ける.	－

表 6 の情報を元に作成した，TomoTherapy への STPA 適用のための要件定義書の一部を表 7 に示す．ここでは，コントローラーからコントロール対象のプロセスに作用するコントロールアクションが，機能要件あるいは非機能要件という形で表現される．この表を元に，コントロールストラクチャを構築することができる（図 26）．

このコントロールストラクチャの構成要素は，大きくヒューマンコントローラーとメカニカルコントローラーの 2 種類に分類される．本論文の提案内容の適用において，TomoTherapy の構成要素として，3 つのメカニカルコントローラーと 2 つのヒューマンコントローラーの計 5 つを抽出した．また，表 6 に記載した情報から各コントローラーの安全責任を表 7 では明確化しており，その範囲内におけるコントローラーの役割を把握することができる．

表　7. STPA 実施のための TomoThepray システムの要件の詳細

ID	分類	アクター（From）	アクター分類（From）	コントロールアクション	アクターの責任（From）	アクター（To）	アクター分類（To）
1	非機能	オペレーター	ヒューマンコントローラー	放射線治療のための準備に関する事項の患者への指示及び，治療中あるいは治療の前後における動作指示を与える．	・最新のトリートメントプランに従って，オペレーターはオペレーターステーションを介して，放射線治療を実施する責任を持つ． ・治療前後や治療中，患者に指示を与える責任を持つ． ・オペレーターは緊急時において，緊急停止ボタンを押して放射線治療を緊急停止する責任を持つ．	患者	ヒューマンコントローラー

2	非機能	オペレーター	ヒューマンコントローラー	治療対象として正しい患者であるか認証する.	同上	患者	ヒューマンコントローラー
3	機能	オペレーター	ヒューマンコントローラー	トリートメントプランを適用する.	同上	オペレーターステーション	メカニカルコントローラー
4	機能	オペレーター	ヒューマンコントローラー	患者のデータ（CT 画像，トリートメントプラン，治療履歴）を参照／分析する.	同上	オペレーターステーション	メカニカルコントローラー
5	機能	オペレーター	ヒューマンコントローラー	放射線治療を開始する.	同上	オペレーターステーション	メカニカルコントローラー
6	機能	オペレーター	ヒューマンコントローラー	放射線治療を終了する.	同上	オペレーターステーション	メカニカルコントローラー
7	機能	オペレーター	ヒューマンコントローラー	放射線治療を緊急停止する.	同上	オペレーターステーション	メカニカルコントローラー

8	機能	オペレータースステーション	メカニカルコントローラー	システムに与えられたトリートメントプランの情報に基づいてトリートメントプランを作成する.	・トリートメントプラン作成のためのコマンド及び，適切な放射線治療（オペレーターによる制御のもとでオペレーターにより作成されたトリートメントプランに応じて患者に必要な放射線量を正確に照射する等）を実施するために，トリートメントシステムを制御するためのコマンドを発する責任を持つ. ・放射線治療のために最適な環境を準備するため，トリートメントルームの状態（温度，湿度等）を制御する責任を持つ.	トリートメントプランニングシステム	メカニカルコントローラー

9	機能	オペレーターステーション	メカニカルコントローラー	治療中における照射対象となる腫瘍の形状に合わせた放射線照射量の制御／ガントリー内の寝台の位置の調整／各種情報の登録／画像取得／放射線照射パラメータの設定を行う.	同上	トリートメントシステム	メカニカルコントローラー
10	機能	オペレーターステーション	メカニカルコントローラー	トリートメントシステムの開始コマンドを発する.	同上	トリートメントシステム	メカニカルコントローラー
11	機能	オペレーターステーション	メカニカルコントローラー	トリートメントシステムの停止コマンドを発する.	同上	トリートメントシステム	メカニカルコントローラー
12	機能	オペレーターステーション	メカニカルコントローラー	トリートメントシステムの緊急	同上	トリートメントシステム	メカニカルコントローラー

				停止コマンドを発する.			
13	機能	オペレーターステーション	メカニカルコントローラー	トリートメントシステムにトリートメントプランを供給する.	同上	トリートメントシステム	メカニカルコントローラー
14	機能	トリートメントシステム	メカニカルコントローラー	ガントリーのモーターを作動させる.	・トリートメントシステムは，患者のトリートメントプランに従って装置内の各機能（ガントリー／MLC／LA／ビーム・ストップ等）の動作を制御し，正確に放射線を照射する責任を持つ. ・トリートメントシステムは，患者の CT 画像や解剖学的構造データをデータサーバーに蓄積する責任を持つ.	患者	ヒューマンコントローラー

15	機能	トリートメントシステム	メカニカルコントローラー	MLC を ON にする.	同上	患者	ヒューマンコントローラー
16	機能	トリートメントシステム	メカニカルコントローラー	MLC を OFF にする.	同上	患者	ヒューマンコントローラー
17	機能	トリートメントシステム	メカニカルコントローラー	LA を ON にする.	同上	患者	ヒューマンコントローラー
18	機能	トリートメントシステム	メカニカルコントローラー	LA を OFF にする.	同上	患者	ヒューマンコントローラー
19	機能	トリートメントシステム	メカニカルコントローラー	ビームストップを有効にする.	同上	患者	ヒューマンコントローラー
20	機能	トリートメントシステム	メカニカルコントローラー	ビームストップを無効にする.	同上	患者	ヒューマンコントローラー

コントロールストラクチャ

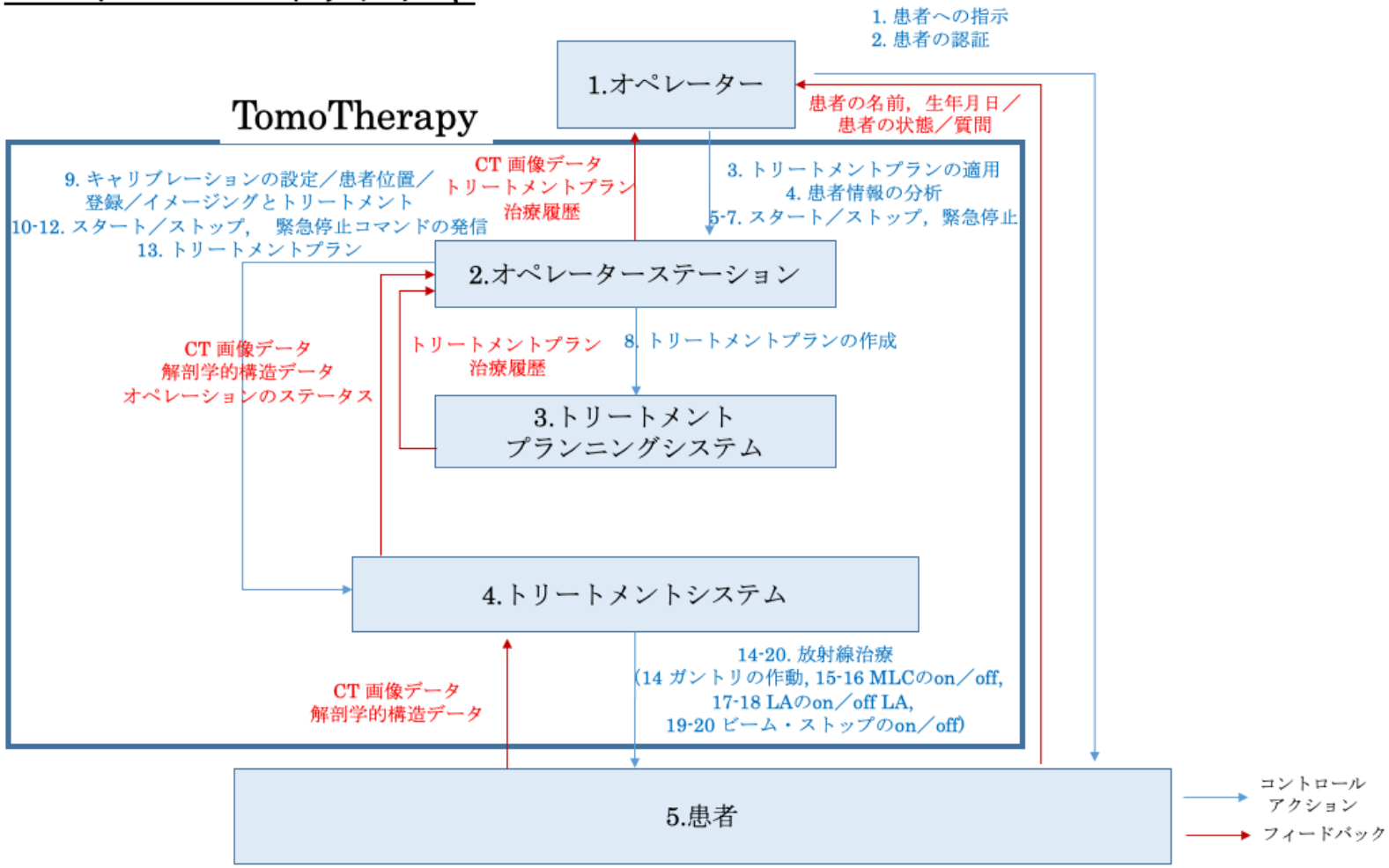


図　26. TomoTherapy システムのコントロールストラクチャ

4.4 STPA による安全解析に優先順位をつける手法の適用

本節では，3.3 節で提案した内容に従い，4.3 節で示した STPA の以降の Step の適用を示す．なお，ここでは前述の通り，放射線治療装置（TomoTherapy）を対象とし，開発元の Accuray Incorporated から提供されている，システム要件が包含されているシステム情報文書から取得できる情報のみを利用している．

まず，STPA の Step3 ではモデル化し，作成したコントロールストラクチャを元に，表 7 の各コントロールアクションに対し，本 Step である UCA の抽出を実施する．ここでは，図 26 において示した図中のコントロールアクションの No.12 「 トリートメントシステムの緊急停止コマンドを発する」（表 7 の「ID」の No.12）についての UCA の一部を示す（表 8）．

その結果として，まずは，「トリートメントシステムの緊急停止コマンドを発する」というコントロールアクションに対して，そのコントロールアクションが与えられないと「患者の正常な組織に放射線が照射される」また「患者の患部が，治療において望ましい線量より過剰な線量にさらされる」というシステムのハザード状態を引き起こす「UCA-1：トリートメントシステム内の患者が，もはや寝台上の適切な位置に整列していないとき，オペレーターステーションが停止コマンドを発しない」という UCA を抽出した．なお，このシステムの使用時にはある程度患者の位置は物理的に固定された状態ではあるが（Accuray Incorporated, 2014），その固定が無効になってしまうほど患者が動いてしまった場合を想定している．

次に，コントロールアクションが与えられると「患者の患部が，治療において望ましい線量より少ない線量にさらされる」というハザードを引き起こす，「UCA-2: 緊急状態ではないときに，オペレーターステーションが停止コマンドを発する」という UCA を抽出した．

そして，コントロールアクションが早すぎ／遅すぎ／誤順序の場合においても，本システムの使用時には，患者の位置はある程度，物理的に固定された状態であり治療中に患者が適切な状態を保って治療を受けていた状況において（Accuray Incorporated, 2014），　まずは「患者の患部が，治療において望ましい線量より少ない線量にさらされる」というハザードを引き起こす，「UCA-3：放射線治療を完了する前にオペレーターステーションが緊急停止コマンドを発する」という UCA を抽出した．さらに，「患者の患部が，治療

において望ましい線量より過剰な線量にさらされる」というハザードを引き起こす場合が想定される，「UCA-4：緊急停止ボタンが押された後，オペレーターステーションが緊急停止コマンドを発するのが大幅に遅れる」というUCAも抽出した．

各UCAは，Step1で定義したハザードと関連づけられている．また，このとき，CCも導出する（表9）．UCA-1, UCA-2, UCA-3, UCA-4についてそれぞれ，「CC-1：患者の体がもはや寝台上の適切な位置にいないとき，オペレーターステーションは緊急停止コマンドを発しなければならない」，「CC-2：緊急状態ではないとき，オペレーターステーションは，緊急停止コマンドを発してはならない」，「CC-3：放射線治療を完了した後，オペレーターステーションは緊急停止コマンドを発してはならない」，「CC-4：オペレーターステーションは緊急停止ボタンが押された後，緊急停止コマンドを適切に発しなければならない」となる．なお，このCCは，要件定義工程へシステム開発における，安全要件を開発するためにフィードバックする．

なお，前記の緊急停止というのは，「治療中に放射線を遮断する必要が発生した場合」と，放射線機器品質管理のマニュアルとして利用されている「外部放射線治療装置—放射線機器品質管理実践マニュアル」（社団法人日本放射線技師会　放射線機器管理士部会, 2008）には明記されているのみであり，明確にはその定義がなされていない．あくまで緊急状態の定義は現場での個別の定義あるいはオペレーターの判断に委ねられているのもと解釈できる．ここで示したUCAは，システム情報から把握できた情報を元に作成した一部のUCAであり，このコントロールアクションに対して考えられうる様々なコンテキストを考慮して，網羅的に抽出したUCAのすべてを示しているわけではない．このコントロールアクションを例とすると，患者が寝台上を徐々に動いているという動的な状況や，寝台上の患者の動きに関してどの程度，初期状態からずれると問題となるのかが定量的に定義され，その値と比較した上で患者が寝台にもはや整列できていないといった判断をするような厳密な状況も考えられる．しかし，前記のシステム情報文書からのシステム要件からこのような事項が考慮できているわけではない．このような厳密な内容は，開発の下流工程に進むにつれて検討内容がブレークダウンされ，明確になる．そのため，ここでは，そのような厳密な状況を考慮しているわけではなく，上記の「緊急停止」という大まかな状況にて，UCAを抽出した例を示している．つまり，本節では前述の通り，必ずしも厳密な解析を行った結果を本論文で示しているのではなく，あくまで提案する手法の適用を示したものである．

表 8. 「トリートメントシステムの緊急停止」の UCA

コントロールアクション	与えられないとハザード	与えられるとハザード	早すぎ，遅すぎ，誤順序	早すぎる停止，長すぎる適用
No.12：トリートメントシステムの緊急停止コマンドを発する	[UCA-1] トリートメントシステム内の患者が，もはや寝台上の適切な位置に整列していないとき，オペレーターステーションが停止コマンドを発しない [H1, H3]	[UCA-2] 緊急状態ではないときに，オペレーターステーションが停止コマンドを発する [H3]	[UCA-3] 放射線治療を完了する前にオペレーターステーションが緊急停止コマンドを発する [H3] [UCA-4] 緊急停止ボタンが押された後，オペレーターステーションが緊急停止コマンドを発するのが大幅に遅れる[H2]	－

表 9. 「トリートメントシステムの緊急停止」のコントローラー制約

No.	UCA	コントローラー制約 (CC)
1	[UCA-1] トリートメントシステム内の患者が，もはや寝台上の適切な位置に整列していないとき，オペレーターステーションが停止コマンドを発しない[H1, H3]	[CC-1] 患者の体がもはや寝台上の適切な位置にいないとき，オペレーターステーションは緊急停止コマンドを発しなければならない[SC-1, SC-3]
2	[UCA-2] 緊急状態ではないときに，オペレーターステーションが停止コマンドを発する [H3]	[CC-2] 緊急状態ではないとき，オペレーターステーションは，緊急停止コマンドを発してはならない [SC-3]
3	[UCA-3] 放射線治療を完了する前にオペレーターステーションが緊急停止コマンドを発する[H3]	[CC-3] 放射線治療を完了した後，オペレーターステーションは緊急停止コマンドを発してはならない[SC-3]
4	[UCA-4] 緊急停止ボタンが押された後，オペレーターステーションが緊急停止コマンドを発するのが大幅に遅れる[H2]	[CC-4] オペレーターステーションは緊急停止ボタンが押された後，緊急停止コマンドを適切に発しなければならない[SC-2]

続いて，図 24 に示した本提案に従って STPA の Step4 を実施する．Step4 では，損失シナリオを識別する．前述の L1 あるいは L2 の損失を引き起こす可能性のある，ハザード H1, H2, H3 は，前述の影響度の評価点数を用いて，UCA の内容を確認しながら各々の点数をつける．UCA-1 は H1, H3 と関連する．つまり，患者がもはや寝台上の適切な位置に整列していないということ

で放射線の照射位置がずれ，正常な組織は被爆し，患部の腫瘍には十分な放射線量の治療がなされないということになる．まず H1 のハザードについて，この UCA では，正しい患者の正常な組織に放射線を被曝しうるため，前述の評価点数から 8 点とする．次に H3 に関しては，腫瘍への治療が十分になされないことについて，6 点をつける．続いて，UCA-2 は，H3 に関連づいており，腫瘍への治療が十分になされないことから 6 点をつける．UCA-3 では，腫瘍への治療が完了する前に放射線治療を止めてしまうことから望ましい線量には足りていないため，不完全な治療となる．そのため，軽微であるとして 4 点をつける．最後の UCA-4 については，過剰な線量を患部に照射させて重大な損傷を与えてしまう可能性があることから，8 点をつけるものとする．

前述の UCA の優先順位の計算式から，UCA-1, UCA-2, UCA-3, UCA-4 の点数を計算すると，それぞれ 14, 6, 4, 8 点となる．よって，UCA-1, UCA-4, UCA-2, UCA-3 の優先順位で損失シナリオを識別していく．

本論文では，この中で最も点数の高い UCA-1 についての損失シナリオと，そのシナリオの発生を未然に防ぐためのコンポーネント安全要求を解析例として以下に示す．この計算式から算出した点数を考慮することで，より多くの損失を引き起こしうるハザード群に関連づけられている UCA を優先的に解析し，損失シナリオの発生を防ぐためのコンポーネント安全要求をいち早くシステム開発へフィードバックできる．

UCA-1：トリートメントシステム内の患者が，もはや寝台上の適切な位置に整列していないとき，オペレーターステーションが停止コマンドを発しない．

損失シナリオ-1：トリートメントシステム内の患者が，もはや寝台上の適切な位置に整列していないとき，オペレーターステーションが停止コマンドを発しない．このことは，もしオペレーターステーションが，患者がトリートメントシステム内で適切に寝台上に整列していると誤認識しているときに起こりうる．この誤認識は，もし患者が治療開始後に動いたときに，起こりうる．

コンポーネント安全要求-1_1：オペレーターは治療の間，患者の動きを監視すべきである．その動きはトリートメントシステム内に設置された赤外線カメラ等を通して間接的に監視されていなければならない．

コンポーネント安全要求-1_2：寝台は，患者の動きを自動検知する機能を持たなければならない．もし，ある閾値以上の大きな動きが検知されれば，オペレーターにオペレーターステーションを介してその情報が通知され，オペレーターの監督責任の下，その治療は強制的に緊急停止される．
コンポーネント安全要求-1_3：フレキシブルな患者用の固定具（頭部，腕部，胴体部，脚部用）は物理的に患者の体の位置を固定するように使用されなければならない．

損失シナリオ-2：オペレーターステーションが緊急停止コマンドを発するが，治療が止まらない．緊急停止コマンドは，ケーブルの断線やネットワークを介したデータ伝送での遅延のため，ワークステーションに到達しないかもしれない．もし，緊急停止コマンドがワークステーションに到達しても，ハードウェア故障やコマンド実行前のワークステーションの電源停止のために，実行されないかもしれない．

コンポーネント安全要求-2_1：オペレーターは治療が始まる前までに，ワークステーションと電源が適切に稼働していることを点検しなければならない．
コンポーネント安全要求-2_2：オペレーターステーションは，突然発生した主電源がエネルギーを供給できないという障害に備え，副電源を保持していなければならない．
コンポーネント安全要求-2_3：オペレーターステーションは，コマンド群が実行されたか否かを示すためにオペレーターへ確認のメッセージを送信しなければならない．そのメッセージを受けて，オペレーターは緊急停止コマンドが実行されたのかを確認する．もし停止されていない場合のために，オペレーターはオペレーターステーションを介さずに直接停止できる，代替の緊急停止手段を持たなければならない．

前節の STPA の結果及び本節の結果は，STPA の開発者である MIT の Leveson 教授とそれを専門とする研究者である MIT の Thomas 博士に，STPA による，損失からハザード，そして，UCA と損失シナリオ間におけるトレービリティを確保し，コンポーネント安全要求までの導出の結果を確認してもらうことで今回の解析結果の信頼性を確保した．その確認の中におい

て，当初，Step4 を損失シナリオ識別のためのガイドワード「因果関係シナリオ生成を支援する以前の一般モデル」（Leveson, 2014; Leveson and Thomas, 2018）を利用した解析を行なっていた．そのため，STPA の開発者である Leveson 教授が意図する損失シナリオの識別ができておらず，コンポーネント安全要求が正しく導出できていない旨の指摘を受け，解析を再実施した．その結果，STPA の考え方に基づき，各 Step が実施され，最終的なコンポーネント安全要求が正しく導出されているとの見解をもらっている．

第5章　考察

5.1 放射線治療装置への適用結果

放射線治療装置への適用結果により，本論文で提示した 3 つの課題に有効である事が確認できた．1 つ目と 2 つ目の課題を解決するために，まず要件定義工程での STPA の実施を想定して，システムの開発工程の中で安全解析工程を実施する統合プロセスを提示した．次に，STPA の実施に必要なコントローラーとコントロール対象のプロセス，及びコントロールアクションが既存の要件定義書では明示されていなかったので明確化する事ができた．この明確化によって，コントロールストラクチャと要件定義書が結び付く．この事で，開発プロセスと STPA による安全解析プロセスを統合したシステム開発ができる．それにより，安全要件を漏れなく，システムへの開発要件として要件定義工程で取り込み，開発の早期においてより安全性の高いシステム開発が実現できる効果が期待できる．これは，開発の早期工程で安全要件をシステム開発に取り込むことは，開発プロセス全体を通してのシステムの開発コストの削減に寄与できる（Young, 2017; Leveson, 2018）と考える．

なお，本提案では，本論文で示した要件定義書へ追記する記載項目及びその記載ルールとプロセスを用いて，放射線治療装置への適用の仕方を実際に示した．これは，要件定義工程においてシステムの複数構成要素とその要素間の相互作用の関係を明確にできることを意味する．なぜなら，表 7 で STPA に必要なコントローラー，コントロール対象のプロセスとコントロールアクションを明示できているからである．このことは，開発の要件定義工程において，従来から日本で広く使用されている要件定義書の形式では明確化されていなかった．例えば，2.2.3 節で示した USDM（清水, 2010）が抜け漏れしにくい仕様書の表記法として使用され，また ESPR の要求仕様書（独立行政法人情報処理機構（IPA），2007）も要件定義書のフォーマットとして日本では広く普及している．しかし，これらの形式では，このシステム構成要素とその要素間の関係及びその相互作用が明確化されていない．そのため，STPA のようなシステム理論に基づく安全解析手法を実施することが困難である．また，実際に開発プロセスとは別のプロセスで，STPA を適用するための安全解析を実施しなければならなくなる．そこで，要件定義工程でのシステム構成要素とその関係の明確化を行い，システム開発プロセスと STPA によ

る安全解析プロセスを統合したプロセスを提案することで，この点を解決する事ができたと考える．

3 つ目の課題について，コントロールストラクチャのメンテナンス作業は，使用者に対してその作業負荷が高いものだと考えられており（独立行政法人情報処理推進機（IPA）, 2018），STPA で導出した安全要件をシステム開発にすぐにフィーバックできない．そのため，要件の一部についても適宜，STPA をすぐに実施することで損失シナリオから導出したコンポーネント安全要求を開発の早期にシステム開発にフィードバックすることを意識した．そして，3.1 節に示した要件定義書へ追記する記載項目及びその記載ルールと要件定義工程への適用プロセスを提案し，その適用事例も示した．その結果，本論文の提案では必ずしもコントロールストラクチャ全体のメンテナンスをすることなく STPA を実施できることを示したことから，この課題に有効であると考えられる．また，先の放射線治療装置の適用事例では，表 7 で示した 1 つのコントロールアクションに対して，部分的に STPA の実施を示すことができたので，実際の開発の現場に適したものであると考えられる．なぜなら，コストや未然防止の観点からもできる限り早い段階で，部分的にでも STPA を実施し，損失シナリオから導出したコンポーネント安全要求をシステム開発へ早急にフィードバックすることは，開発プロセスでの安全要件をシステム開発に取り込むというコスト面における要件対応の効率性からも有効である（Young, 2017; Leveson, 2018）．さらに，STPA での安全解析において，発生確率等を使用せず，UCA に優先順位をつけて解析を実施する手法を提案した．各 UCA に対して，損失へのトレーサビリティを確保できる形で，関連するハザードの影響度から UCA の優先順位を数値化し，優先して解析すべき UCA を判断できることが確認できた．

この優先順位がない場合，解析者は明確な基準を持たずにその後の解析を実施していく事になる．STPA を含む多くの安全解析手法は一般に膨大な量の解析を行うことが多い．しかし，実際の開発プロジェクトでは限られたリソース（時間，人員など）の中でシステムを納期までに開発しなければならない．そのような状況下，安全性の観点から重要な箇所を優先して解析できることは有効であると考える．特に，本手法では，UCA に関連するハザードの評価点数を導入し，前述の計算式により各 UCA の総合的な点数を数値化した．それにより，定性的ではなく，定量的に優先して解析すべき UCA を判断することができた．上記の放射線治療装置における事例では，4 つの UCA についての総合的なハザード影響度を本手法で判断した結果，UCA-1 の優先順位が最も高かった．UCA-1 では，患者の腫瘍への放射線治療が不十分になるのみならず，正常な組織に損失を与え，後遺症を引き起こす危険性がある．

実際に，過去にも放射線医療装置の誤照射の報告及び製品リコールは数多く報告されている（Johnson, 2016; SC Times, 2017; the ST. Cloud Times, 2016; Meshbesher&Spence, 2015; South Florida Times, 2015）．このような事故は患者だけでなく，システム開発あるいは使用側にとっても多大な損失を引き起こす．そのため，そのような事故や損失を引き起こさないように考慮された，安全性の高いシステムを開発しなければならない．3.3 節で提案した手法では，STPA の Step3 で識別した UCA に対して，その UCA と関連を持つハザードの影響度から優先順位を判断する．その優先順位に従って Step4 を実施する手順を示した．その解析の結果として得られた，損失シナリオから導出したコンポーネント安全要求を開発の要件定義工程へ直ちにフィードバックする．それにより，さらなる安全性の高いシステムへの設計変更が実現できると考える．

STPA の実施工数については，MIT の Thomas 博士により，その作業の多くが Step4 の実施に費やされていることが報告されている（Thomas, 2017）．Step4 をすべて実施した後と，逐次的に Step4 の結果をシステム開発にフィードバックするのでは，損失シナリオから導出したコンポーネント安全要求を開発に取り込む点において，そのシステムの開発コストに大きな違いが出てくると考える．なぜなら，MIT の Young らが示すように（Young, 2017; Leveson, 2018），開発のより早期の段階でコンポーネント安全要求をシステム開発に取り込むことは，開発プロセス全体を通してのシステムの開発コストの削減に寄与できるからである．

以上の内容から 1.2 節で述べた課題に対する，本手法の成果をまとめすると表 10 のようになる．課題 1 と 2 について，本手法の成果による効果としてまず，開発の早期において，より安全性の高いシステム開発の開発及び設計変更を実現できるものと考える．また，開発プロセス全体を通してのシステムの開発コストの削減に寄与できると考える．課題 3 については，開発プロセスの早期工程でコンポーネント安全要求をシステム開発及び設計変更に取り込むというコスト面における要件対応の効率性からも有効であると考える．

表 10. 課題に対する本手法の成果

課題 No.	課題の内容	本手法の成果
1	STAMP/STPA の使用者が，どの工程で適用するのかを明確化すること	・要件定義工程での STPA の実施を前提として，システムの開発工程の中で安全解析を実施できる統合プロセスを提示した
2	開発プロセスと安全解析プロセスを個々に独立して実施することなく効率的に実施できるようにすること	・既存の要件定義書では明示されていなかった STPA の実施に必要なコントローラーとコントロール対象プロセス及びコントロールアクションを明確化した
3	STAMP/STPA のために作成するコントロールストラクチャのメンテナンスに時間をかけず，損失シナリオから導出したコンポーネント安全要求をシステム開発にすぐにフィードバックすること	・要件定義書へ追加する記載項目及びその記載ルールと要件定義工程への適用プロセスを提案した ・必ずしもコントロールストラクチャ全体のメンテナンスをする必要もなく STPA を実施できるプロセスを提案した ・要件の一部についても適宜，STPA をすぐに実施するプロセスを示すことで，損失シナリオから導出したコンポーネント安全要求を開発の早期にシステム開発へフィードバックするプロセスを提案した ・優先順位の高い UCA から，損失シナリオの導出とコンポーネント安全要求を導出して，要件定義工程へフィードバックする方法を提案した

本論文において，実際に UCA の抽出の事例も示した．UCA はコントロールアクションの否定形であるため，否定形のパターンの網羅性に関してはその発生のコンテキストを考慮するとあらゆるパターンが考えられるため，抽出の抜け／漏れに関するリスクが存在する．STPA の場合は，「与えられないとハザード」，「与えられるとハザード」，「早すぎ，遅すぎ，誤順序」，「早すぎる停止，長すぎる適用」の 4 つの視点で UCA を抽出する．このパターンで抜け／漏れがないかの検証を行い，可能な限りその抜け／漏れを防止する事に関する検討は今後，行う必要があると考える．STPA の UCA の抽出では，コントロールアクションが「与えられる場合」と「与えられない場合」の 2 つの場合分けとしているが，特に，そのトレーサビリティの上位にある，コントロールアクションの抜け漏れについて，そのコントロールアクションの抽出に関する抜け／漏れ防止をできるような事項も検討する必要があると考えている．その場合，コントロールアクションは，コントロールストラクチャの一部であるため，コントロールストラクチャの作成で重要となるシステム境界の設定と，システム及びシステムとして捉えられるコンポーネント群の粒度に関する事項も，その検討に重要な要素になると考えている．

本論文で作成したコントロールストラクチャは，システム要件が包含されているシステムに関する情報を利用して抽出した情報に基づいて作成したものである．しかし，放射線治療装置において，この他にも考慮すべきコントローラー及びコントール対象プロセスがいくつかあると考えられる．例えば，メカニカルコントローラーとして，メカニカルサポートシステムが存在する．これは放射線治療装置の動作に関わるハードウェア機器の状態を制御するシステムである．そして，メカニカルサポートシステムは，トリートメントルームの状態をある一定の状態となるように制御する機能を持つ．例えば，トリートメンルーム内の気温や湿度をエアーコンプレッサー，エアタンク，コンプレスド・エアーライン，乾燥機やエアーレギュレーターによって，オペレーターステーションからの指示に従って制御する役割を持つが本論文ではその構成要素として明確化していない．次にヒューマンコントローラーの例を述べる．まず，放射線腫瘍学専門家は，患者の放射線治療計画を作成する上で中核的な役割を果たす．放射線腫瘍学専門家は，放射線治療計画に対して，各回の放射線治療時において照射すべき放射線の線量を決定し，照射のタイミングや照射部位の指定などの患者の放射線治療計画に必要とされる情報を決める上で，専門的な知識を提供する．さらに，患者の治療に対する促進や治療に関して経過を把握し，患者に対するフォローアップなどのケアを実施する．治療が必要とされる患者に対しては，放射線治療を

進めるなどの業務も行う．また，医学物理士は，トリートメントプラン作成のために臨床知識を提供し，患者の治療への状態を評価する．また，医用画像に対する専門的な知識と技術を患者の治療のために提供する．そのため，それらの知識と技術を用いて具体的なトリートメントプランの作成に協力し，実際の治療への最適化を図る．このように本論文で作成したコントロールストラクチャについても，より詳細な放射線治療装置に関する情報をもとに作成するよう，検討する必要があると考える．

放射線治療において，FMEA と STPA の解析結果を比較検討した事例はすでに報告されている（Blandine, 2013）．その結果によると，STPA での解析結果において FMEA では識別できなかったコンポーネント安全要求を導出し，STPA の優位性が確認されている．また，FMEA と STPA の放射線治療装置への適用結果についての比較検討もすでにいくつか行われ，STPA の有効性が報告されている（Pawlicki, 2016; Yamaguchi, 2019）．著者らの TomoTherapy への STPA の適用結果では，6 つのシステムレベルの安全制約，99 個の UCA，88 個のコントーラ制約，10 個の損失シナリオ，及び 33 個のコンポーネント安全要求が導出された（Yamaguchi, 2019）．一方，FMEA では 74 個の故障モードと 30 個の潜在する故障原因が導出された（Broggi, 2013; Broggi, 2015）．表 11 では FMEA と STPA の適用結果を比較した結果を示す．なお，ここでは，Ford らによる原因分類（Ford, 2012）を利用し，FMEA による解析結果（Broggi, 2013; Broggi, 2015）と STPA の解析結果を比較している（Yamaguchi, 2019）．この原因分類は，放射線腫瘍学における事故データベースの内容を元に作成した分類であり，事故の根本原因や要因となる因子の特定とヒューマンファクターによる主観的な判断によるミスを低減することを目的として作成されたものである．この分類には，大きく，技術的な側面（物理システム），技術的な側面（その他），医療従事者のオペレーションに関する側面，患者の周囲環境に関する側面，手続きに関する側面の 5 つが存在する．

表　11. STPA と FMEA の結果の原因分類の網羅性

原因分類	FMEA	STPA
技術的な側面 （物理システム）	13%	30%
技術的な側面 （その他）	0%	10%
医療従事者のオペレーションに 関する側面	87%	40%
患者の周囲環境に関する側面	0%	10%
手続きに関する側面	0%	10%
計	100%	100%

この結果によると，FMEA の結果は主に，物理システムにおける技術面に関する項目と医療スタッフによるオペレーションに関する項目の 2 つに分類されている．一方，STPA の結果は，医療システム全体から，技術的な側面，ヒューマンファクター，環境や手続き面に至るまで幅広く網羅している．また，FMEA は，線形なプロセスツリーに基づいて単一故障の原因を特定しており，システム全体の振る舞いを考慮していない．現実問題として，事故や損失は，ハードウェア，ソフトウェア，ヒューマンファクター間における複雑な相互作用の関係から創発されている現状がある．STPA はこの点を考慮した安全解析手法であると本論文の第 1 章でも述べたが，この結果からも STPA は，FMEA よりも事故や損失の原因を幅広い側面から網羅していることが分かった．また，FMEA と STPA を併用することでも，安全解析における解析の網羅度を広げることができるとも考えられる．

さらに，この STPA による解析結果において，Broggi らによる FMEA の結果（Broggi, 2013; Broggi, 2015）では見つからなかった項目を導出することができた．その一例としては，STPA ではオペレーションにおける手続き面の観点（Ford, 2012）での解析ができ，オペレーターあるいは看護師が，治療時に患者の認証を行うときに音として酷似している名前の患者への確認に対して，患者が誤って Yes と答えることで認証が成立している場合を抽出している．そして，それを防止できるコンポーネント安全要求の例として，「オペレーターや看護師は誤った患者がトリートメントルームに入らないよう

に，名前だけでなく，生年月日や出身の州等を確認しなければならない」というものを導出している．また，「オペレーターは患者のフルネームのスペルを確認しなければならない」というコンポーネント安全要求も導出している．このような結果は，システムにおける複数の側面（ハードウェア，ソフトウェア，ヒューマンファクター）からシステムホリスティックに安全解析を実施することで，そのシステム内における要素間のコントロールループの形成を阻害する要因を検討し，コントローラーのコンロールアルゴリズムを考慮したことから抽出することが出来たと考える．

この解析結果から，従来の代表的な手法である FMEA では見つからなかった項目が STPA で見つけることをできたわけであるが，放射線治療装置における過去の事故の事例の中で，実際にそのような事故が報告されている．この事例として，2009 年に横浜市立大学付属病院にて発生した患者の取り違え事故である（神奈川新聞, 2009）．この報告によると，この取り違えは乳がん治療の治療過程で発生したものであった．これは，40 代女性の順番を一つ繰り上げた際，放射線技師が前の順番の患者の照射範囲のまま放射線治療を実施してしまった．その直後，別の技師が人違いに気付き早急に中止した．しかし，患者の胸から肩の正常部位に対して，自然界で受ける半年分の放射線を照射してしまったと報告されている．この事故はまさに，患者の認証過程（表 11 における手続きに関する側面）で発生した事故と類似するケースである．このような事故は本論文で対象とした TomoTherapy では現状，報告されていないが，システムの設置あるいは設定状態やヒューマンコントローラーの振る舞い等を考えれば発生しうる事故だと考えられる．また，同付属病院では 1999 年に手術で患者を取り違えた事故が発生した．この事故では，医師や看護師の計 6 人が業務上過失傷害で有罪判決を受けている．実際にこのようなケースは再発しているにも関わらず，安全解析の初期段階での検討漏れがあったと考えられる．それに対して，本論文で提案した内容による STPA では，このような事故の発生を上記の患者の認証で示した一例のように，要件定義工程というシステム開発の早い段階で検討して損失シナリオを識別し，コンポーネント安全要求という形でフィードバックすることができる．

放射線治療装置に関して，実際に起こっている事故として 4.1 節や上記で述べた通り，いくつもの事例が報告されている．この他にも，コスタリカ共和国のサンホセで起きた放射線治療装置での被ばく事故がある．この事故は，同国同都市の基幹病院のひとつであるサン・ファン・デ・ディオス病院において，1997 年の 8 月 26 日から 10 月 3 日にかけて，コバルト 60 線源の放射線治療を受けている患者が過剰な線量の放射線照射を受けるという事故が発生した．この間，放射線遅漏装置で治療を受けた 115 人の患者のうち，少な

くとも 3 人はこの事が原因で死亡し，少なくとも 46 人は過剰な線量の放射線照射の影響を受けた（国立研究開発法人　日本原子力研究開発機構，1999）．この事故の調査結果によると，患者は本来受けるべき線量より 50 から 60%多い線量の放射線を照射されていた．装置自体には問題がみられなかったが，放射線治療の体制自体にいくつかの問題点が報告された．その問題点のいくつかを以下に示す．

- トリートメンルームの天井のシールドが不十分であり，照射の方向に制限があった
- 放射線の照射時，患者に施すべき遮蔽が正しく行われていなかった
- トリートメンプランがたてられてなかった
- 放射線事故を防ぐ二重三重のシステムを考慮していなかった
- 放射線業務の医療従事者への教育が不充分で，責任体制も不明確だった

また，このサン・ファン・デ・ディオス病院における放射線照射装置の線量の測定値に関して 1977 年以降，International Atomic Energy Agency（IAEA）は繰り返し，自前の測定値とのずれの存在を通報していた．そして，1996 年 7 月に専門家がその原因を調査に訪れたときに過去の放射線ビームのキャリブレーションの記録や照射条件の記録も存在せず，この病院にて開発された吸収線量率を計算するためのコンピューター・プログラムにも誤りが認められた．上記の問題点の中で，安全責任の明確化は，まさに，本論文の 3.1 節の安全責任の箇所で明確にすべき項目として挙げているものである．また，ヒューマンエラー，ソフトウェアエラーの要因も複合的に関係しており，まさにシステムホリスティックにシステム全体を俯瞰してその安全性を検討しなければならなかった事例と言える．

なお，このように装置自体には問題がみられないケースの事故が近年，多々発生している．先に述べた CentraCare Health Coborn Cancer Center の事例においても，装置自体には問題がなかったと報告されている（the ST. Cloud Times, 2016; Meshbesher&Spence, 2015; South Florida Times, 2015）．装置自体の安全性には，FMEA などの従来手法が長年利用されているが，前述の表 11 に示したような，FMEA などの手法で網羅できないケースにおいて実際に事故が発生している．その網羅できていない箇所の安全解析において，STPA の方が，網羅性が高いことから，本論文の提案を踏まえた STPA の適用により，この点の安全性を高められる可能性があると考えられる．

次に，国立弘前病院においても放射線治療における過剰照射事故が報告されている（医学放射線物理連絡協議会，2004）．この事故では，医師と技師の間の線量表示に対する解釈の相違があったため，医師の意図した線量と実際に投与された線量が異なっていた．この事は両者の間のコミュニケーションの欠如とそれぞれの技量の不足により引き起こされ，長期間にわたり継続したと報告されている．これはまさに，STPA におけるコントロールアクションがヒューマンコントローラーの場合の安全解析となる対象である．

他にも，多数の事故が報告されており，その一部として表 12 に日本医療機能評価機構が報告した結果を示す（公益財団法人　日本医療機能評価機構，2014）．なお，この報告内容における事故は，2004 年から 2014 年に発生した放射治療に関連した医療事故を調査したものであるが，この間に発生した放射線治療に関する事故をすべて網羅しているものではない．その内訳として照射部位の取り違えが最も多く 20 件であり，次に過剰照射が 8 件であった．また，患者の取り違えにおいても，5 件あったと報告されている．なお，この報告によると，その要因のほとんどがオペレーションミス，プロセスが明確でないこと，作業者の思い込みや意思疎通の不足などのヒューマンファクターによるものとされており，これらも STPA での安全解析の対象とする領域である．

表　12．放射線治療に関連した近年の医療事故

原因	件数
照射部位の間違い	20
過剰照射	8
熱傷	5
患者の取り違え	5
機器の不具合	4
機器の設定間違い	3
その他	3
計	48

参考文献[公益財団法人　日本医療機能評価機構，2014]を元に著者作成

以上のようにSTPAと，システムの単一側面を見るFMEAのような手法と比較し，これらの実際に起こった事例からもSTPAの方が現実により多くのものが指摘でき，優位であると考える．つまり，実際に起こった事故の事例を確認しても，表11で示したように，様々な局面でSTPAでの解析結果の方が，網羅性が高く，こういった事故もSTPAによる解析で検討できるものと考えられる．なお，その検討も，本論文で提案したような内容により，システム開発の早期である要件定義工程で可能であるのは特徴的である．このように，実際に起こっている事例として，システムホリスティックにとらえた場合の，システム安全における全体の網羅性の観点から見てもSTPAの方が優れていると考えている．

5.2 本提案の適用に関する制限事項

ここでは，本論文で提案した内容の活用に関し，その制限事項を明確化する．まず，本提案は，MIT の Young らの主張（Young, 2017; Leveson, 2018）を踏まえ，システム開発におけるコスト面での効果を考慮しているため，可能な限りシステム開発の早期工程での STPA の適用する場合を対象とした．そこで，本論文ではシステム開発における要件定義工程を対象とし，それ以外の工程における適用は範囲外としている．つまり，設計工程や製造工程での適用を想定していない．また，V-Model が繰り返し実行されるようなシステム開発も現実にはある．しかし，提案したプロセスは階層的にシステムをサブシステムに分けて開発するような，要件が繰り返し詳細化される場合にも明確には対応できていない．特にソフトウェアにおいては，開発の初期段階では本提案内容を適用することができるが，その後，要件が段階的詳細化される場合における，開発の下位で詳細化される要件に対しての適用プロセスは明確にしておらず，その範囲外となる．これは，本提案はできる限り開発の早期でコンポーネント安全要求をシステム開発へフィードバックすることを目指したからである．また，本論文ではその提案内容を評価するために放射線治療装置を対象とした．しかし，現状としては，これよりも大規模かつ複雑なシステムが存在しており，今後，益々そのようなシステムは増加するものと考えられる．STPA の実施においては，コントロールストラクチャの作成が安全解析の中核となる．そのため，大規模かつ複雑なシステムにおいても，そのようなシステムを適切な粒度のサブシステムに分割／階層化し，そのシステム境界を適切に設定すること等を考慮して，STPA での安全解析を実現できる方法を検討する必要があると考える．

次に，要件定義書が自然言語で記載されていない，ある特定の表記法で記載されいてる場合に本論文の提案内容が対応できていないことが挙げられる．つまり，本論文で示した提案の適用の範囲は，表形式の自然言語で要件を記載する場合に限定している．前述の通り，本論文の 3.1 節にて要件定義書への記載ルールを提案した．これは要件定義書を自然言語である文章で各ケースを想定している．しかし，実際の開発の現場では様々な表記法が使用されている．近年では，大規模化／複雑化するシステム開発においてシステムズエンジニアリングの必要性の高まりから，モデルベースの表記法が注目を集めている．そのため，Object Process Methodology（OPM）や Systems Modeling Language（SysML）が使用されている現状がある（Dori, 2016）．また，ソフトウェア開発においては，オブジェクト指向分析や設計

のための表記についての統一がなされた Unified Modeling Language（UML）が広く普及している（Booch, 2005）．要件定義工程あるいはシステム開発の全工程において，これらの表記法に追従できるように，本提案内容をどのように対応させるのかは今後，検討する必要がある．

さらに，本論文では要件のみを解析対象として限定していることが挙げられる．本論文の提案の対象としているのは，要件定義工程であり，システム情報からの抽出した要件を元に解析することを前提としている．しかし，今後の適用対象も様々な産業となる場合となる可能性があり，ハードウェア，ソフトウェア，組織及びそれらの組み合わせたシステムが解析対象になると考えられる．その場合，システムの開発の対象によっては本論文で使用している要件という用語は，「要求」と表現される場合もあり，本論文で想定している要件と要求の粒度も異なると考えられ，要件というものを厳密に定義していない．そのため，本提案が様々な産業において幅広く活用されるためにも，本論文で用いられるこのような用語に関して，厳密に再定義することを検討する必要性があると考える．

5.3 従来手法と本論文の提案による STPA

放射線治療装置での安全解析において，FMEA が広く普及しており，FMEA と STPA との結果の比較に関しては，前節にて言及した．この他にも安全解析に関する従来手法の代表的なものとして，2 章で示した FTA，HAZOP，PRA，ESPR などが存在する．

特に，医療機器の分野において，FMEA は AAPM と ICRP により，その使用が推奨されている（Huq, 2008; International Commission on Radiological Protection, 2009）．本論文にて示した要件定義工程での UCA の優先順を考慮した STPA の実施は，この FMEA の実施と競合しないと考える．なぜなら，両者では適用する工程が異なるからである．本来，STPA はどの開発工程においても適用可能とされている（Leveson, 2012）．一方，FMEA は，安全解析のためにシステムの詳細な設計情報を必要としており，詳細設計工程以降に実施される場合が多い（Marvin, 2004）．つまり，詳細設計工程以降での両者の実施は，競合する可能性がある．しかし，本論文では，要件定義工程で STPA を実施することを提案しているため，要件定義工程に限れば，両者は競合しない．また，アクシデントモデルの違いの観点からも STPA は，システムの詳細設計レベルの情報をもとにした単一故障モードからの Chain of events モデルに基づく従来法とは同じ結果を包含する可能性はあるが，STPA ではシステムにおける構成要素間の相互作用に着目した手法であるため，FMEA では識別できなかった損失シナリオ及びコンポーネント安全要求を導出できると考える．つまり，従来の単一故障モードによる安全解析と，STPA によるシステムの複数要素間の相互作用を考慮した安全解析を併用したシステム開発が実現できる．それにより，近年の大規模／複雑化するシステム開発のための安全解析を，より包括的に実施できると考える．

次に，FTA は FMEA と同様に，その特徴としてはシステムにおける機器や組織の単一故障をハザード要因として識別していることが挙げられる．また，詳細なシステムの設計情報を元として（これは特に FMEA にあてはまる），分岐条件を論理的にくむことで網羅的に解析できる反面，全体的な視野での解析が難しいという特徴もある．一方，STPA はシステムにおける複数の機器や組織（ヒューマンファクター）が相互作用を持つ大規模かつ複雑なシステムにおいて，相互作用のハザード要因を識別して損失シナリオを特定することが挙げられる．また，システム全体の振る舞いを確認しながら解析できることを特徴としている．なお，PRA は，単一故障を扱うのみならず，その組み合わせにより，あらゆるケースを網羅できる安全解析手法ではあ

り，HAZOP は，その装置あるいは動作プロセスについての詳細なシステム逸脱状態あるいは状況が把握できる入力情報を必要とする．しかし，本論文の提案では要件定義工程での安全解析手法の適用を前提としている．つまり，PRA や HAZOP においては，解析対象となるシステムが仕様として明確化され，ある程度使用できる状態になっていることが前提となっていたりするので，要件定義工程での安全解析を実現することは困難であり，本手法を活用した STPA との比較対象としては対象外になると考える．

最後に組込みソフトウェアの開発プロセスガイドである ESPR については，STPA による安全解析と以下のような類似する観点を持つ．

- ソフトウェア単独ではなく，関連するハードウェア動作なども考慮して，システム全体としての安全が保たれるように考慮
- システムの動作モード（始動，自動，手動，半自動，定常／非定常）に対応した安全機能の洗い出し
- システムに対する外乱や入力データの誤差，あるいは，ユーザーの操作ミスなどの可能性も含めて，これらの影響を最小化するように検討
- システムとして実装する安全機能以外にも，システムの使用や運用の際の方式面（システム異常時のシステム管理者やユーザーの対応など）での安全性確保なども考慮
- 不具合やトラブルの発生頻度とそれらによる影響度合いを考慮して，安全機能がどの程度機能することを保証するかを検討し，安全機能毎に安全性の水準を決定

しかしながら，ESPR はあくまで，開発プロセスを実施する上でのガイド（チェックしておくべき項目）をリスト形式で示しており，そのリストの各項目の実施を推奨しているのみである．そのため，これらの観点が，導入する組織の判断で抜け落ちてしまう可能性がある．また，ESPR は解析手法としては確立されておらず，その具体的な実施のためのプロセスまでは提示していない，開発プロセスに対するチェックリスト形式のガイドとなっている．つまり，STPA システム理論に基づいて安全解析を実施し，コンポーネント安全要求のような安全要件を導出できるような手法としては確立されてはいないと考える．

ESPR による解析の観点に関しても，例えば，STPA のコントロールストラクチャから形成されるコントロールループを意識したシステム理論に基づく

方法論となってはない．ESPR は組込みソフトウェアの開発プロセスについてのガイドであり，FMEA，FTA，HAZOP，PRA や STPA と同列で比較できる解析手法という位置づけではなく，解析のためのチェックリストである．この安全要求仕様書のガイドにおいては，以下の記載項目が示されている．

- 概要：ドキュメントの目的，位置付け，記載内容などの安全要求仕様書の概要及び参照しているドキュメント名称などを記載．
- システム構成：ハードウェアを含めたシステム全体の構成とソフトウェアの位置付け，およびソフトウェアを取り巻く関係／条件を記載．また，システム要求仕様書やハードウェア仕様書等の関連資料より要求，条件などを整理して記載．
- 想定システム障害リスト：システムが想定する安全逸脱状況とそのハザード解析結果を記載．
- システム安全要求リスト：安全性を実現するためにシステム及びシステム周辺（外部システム，ユーザーなど）に求められる要件を記載．
- システム安全度水準：システムに求められる安全性の水準（安全度水準（IEC61508））を記載．
- その他：特記しておくべき事項がある場合に記載．

すでに ESPR を導入している組織についても，上記の「システム構成」，「想定システム障害リスト」，「システム安全要求リスト」との項目に関して，本論文の提案内容を活用し，その内容を反映させることができると考える．それにより，本提案による STPA の導入のオーバーヘッドを減らした上で，システム開発における安全解析を，より強固なものとすることができると考える．この ESPR への反映の仕方は今後，具体的に検討する必要がある．

第6章　結論と今後の展望

6.1 結論

本論文では，STPA の要件定義工程での適用に着目し，システムの開発現場のために考案した要件定義書へ追記する記載項目及びその記載ルールと，その適用プロセスを考案し，STPA の現場適用の 3 つの課題への解決方法を提示した．さらに，STPA の適用において，解析対象となるコントロールアクションから識別した UCA に優先順位をつけて解析を実施する手法を示した．UCA は，システムハザードに至り，そのハザードは損失を引き起こす．そのトレーサビリティを使用して，UCA に関連づくハザードの影響度から，安全解析の優先順位をつける．

システム全体を構成する各要素に対して，本論文で提案する手法で STPA を適用し，優先順位の高い非安全なコンロールアクションから順次，解析する．その結果として得られた，損失シナリオから導出したコンポーネント安全要求を要件定義工程へ逐次的にフィードバックする．それにより，開発早期でのより安全性の高いシステム開発をより強固とするための提案を行った．

そして，本論文で示した手法を用いて，放射線治療装置への適用の仕方を実際に示した．さらに，その適用において得られた結果から，STPA の優位性を確認することができた．

6.2 今後の展望

本論文で考えられる今後の展望として，まずは，現状の開発現場で使用されている様々な表記法への適用の検討が挙げられる．本論文では，要件定義書に項目を追加する事による課題の解決を提案した．しかし，実際の様々な産業における開発の現場では，多様な表記法が使用されている．特にモデルベースの表記法として，OPM や SysML，そしてソフトウェア開発においては UML が近年，注目を集めている．これらの表記との STPA の適用における追跡性をどのように対応するのかは今後，検討する必要があると考える．また，ESPR を導入している組織については，本論文の提案内容をそのまま活用し，その内容を安全要求仕様書に反映させることができると考える．それにより，本提案の導入のオーバーヘッドを減らした上で，システム開発における安全解析を，より強固なものとする．そのための方法を，今後，検討する必要があると考える．

次に，UCA はコントロールアクションの否定形であるため，否定形とするパターンの抜け／漏れに関するリスクがあることをすでに述べた．現状の STPA の適用における UCA の導出において，抜け漏れが出ないか，そして可能な限りその抜け漏れを防止する事についても今後，検討する必要があると考える．

さらに，今後は，他の放射線治療装置あるいは医療機器だけではなく，ハードウェア，ソフトウェア，組織（ヒューマンファクター）を含めた幅広いシステム開発への適用事例を増やす．特に，様々な機器がクラウドを介してエッジ端末で繋がっていく時代に今後は移行してくことから，より大規模かつ複雑なシステムを 1 つのシステムとして捉え，システムの安全解析の対象として検討していく．その適用事例を増やす中で，各産業における専門家からのレビューを受けることにより，本提案内容を含む形での STPA による解析内容自体の信頼性の向上とその内容の検証を行う．そして，そのような様々な活用事例を増やす中で，さらなる課題を抽出し，解決していく必要があると考える．

参考文献

AAPM Radiation Therapy Committee Task Group 35, 1993. Medical accelerator safety consideration, Med. Phys. 20: 1261-1275

Abdulkhaleq, A., 2017. A System-Theoretic Safety Engineering Approach for Software-Intensive Systems, Stuttgart University Ph.D dissertation

Accuray Incorporated, 2014. TomoTherapy HTM Series Site Planning Guide, http://www.accuray.com/sites/default/files/T-SPG-00725.pdf

Accuray Incorporated, 2018. TomoTherapy, http://www.tomotherapy.com

Blandine, A., 2013. Systems Theoretic Hazard Analysis (STPA) Applied to the Risk Review of Complex Systems: An Example from the Medical Device Industry, Ph.D. thesis, MIT, Cambridge, MA (U.S.A.), dissertation

Booch, G., Rumbaugh, J., Jacobson, I., 2005. Unified Modeling Language User Guide, The, 2nd Edition. Addison-Wesley

Borgovini, R., 1967. “Design Analysis Procedure For Failure Modes, Effects and Criticality Analysis（FMECA）.” In: Society for Automotive Engineers, pp. 25, 34, 55

Borgovini, R., 1993. Failure Mode, Effects, and Criticality Analysis (FMECA). Defence Critical Information Center

Broggi, S., et al., 2013. Application of failure mode and effects analysis (FMEA) to pretreatment phases in TomoTherapy. J.Appl. Clin. Med. Phys. 14, pp.265-277.

Broggi, S., et al., 2015. Application of failure mode and effect analysis to tomotherapy treatment delivery. Radioprotection 50(3), pp.171-175.

Burns, D.J., Pitblado, 1993. R.M., A modified HAZOP methodology for safety critical system assessment, Springer Verlag.

Cagno, E., Caron, F., 2002. Mancini, M., Risk analysis in plant commissioning: the Multilevel Hazop. Reliability Engineering & System Safety, 77(3): pp. 309-323.

Cancer Treatment Centers of America, 2017. What is TomoTherapy. http://www.brachytherapy.com/tomotherapy.aspx

Chudleigh, M.F., Clare, J.N., 1993. The benefits of SUSI: Safety analysis of user system interaction, DTIC Document

Collett, E. R., Bachant, W. P., Integration of BIT Effectiveness with FMECA, 1984. Proceedings of the Annual Reliability and Maintainability Symposium, New York (U.S.A.), IEEE

Crawley, F., Preston, M., Tyler, B., 2008. Hazop: Guide to Best Practice: Guidelines to Best Practice for the Process and Chemical Industries, Inst of Chemical Engineers.

Cupryk, M., 2011. Starndardizing Patient Safety Risk Management. Pharmaceutical Engineering, Vol.31, No.2

de Weck, O., 2009. Fundamentals of systems engineering

de Weck, O., Roos, D., and Magee, C. L. , 2011. Engineering systems: Meeting human needs in a complex technological world, The MIT Press

Dhillon, B.S., 2006., Maintainability, maintenance, and reliability for engineers, Boca Raton: CRC/Taylor & Francis, pp.217

Dori, D., 2016. Model-Based Systems Engineering with OPM and SysML. Springer

Duckworth, H.A., Moore, R.A., 2010. Social Responsibility: Failure Mode Effects and Analysis. Industrial Innovation Series, Taylor and Francis.

Dunjó, J., et al., 2010. Hazard and operability (HAZOP) analysis. A literature review, Journal of Hazardous Materials, 173(1–3): pp. 19-32.

Fields, B., Wright, P., 1988. Error tolerance in collaborative systems

Fleming, C., Leveson, N., 2015. Integrating Systems Safety into Systems Engineering during Concept Development. 25th Annual INCOSE International Symposium (IS2015)

Fleming, C., 2015. Safety-Driven Early Concept Analysis and Development, Ph.D. thesis, MIT, Cambridge, MA (U.S.A.), dissertation

Ford, C. E., Gaudette, R., Myers, L., Vanderver, B., Engineer, L., Zellars, R., Song, Y. D., Wong, J., DeWeese, L. T., 2009. Evaluation of safety in a radiation oncology setting using failure modes and effects analysis. Int. J. Radiat. Oncol., Biol., Phys. 74(3), pp.852–858

Ford, C. E., Fong de Los Santos, L., Pawlicki, T., Sutlief, S., Dunscombe, P., 2012. Consensus recommendations for incident learning database structures in radiation oncology. Med. Phys. 39(12), pp.7272-7290

Fragola R., Frank MV., et al., 1995. Probabilistic risk assessment of the Space Shuttle: A study of the potential of losing the vehicle during nominal operation: System models and data analysis, NASA-CR-197808 NASA-CR-197811

Franklin, B., 2015. TerranearPMC Safety Share, https://eteba.org/wp-content/uploads/2015/02/SafetyShare-2-9-2015-Risk-Assessment-Codes.pdf

Frola, F., et al, 1984. System Safety in aircraft management, Logistics Management Institute, Washington DC

HAZOP and Plant Safety Promotion, 2018. HAZOP Q&A, http://hazop.jp/hazop_a18.html

Heinrich, W. H., 1931. Industrial Accident Prevention: A Scientific Approach 1st ed., New York (U.S.A.), NY: McGraw-Hill Book Company, Inc.

Huq, M., Fraass B., Dunscombe P., et al., 2008. A method for evaluating quality assurance needs in radiation therapy. Int J Radiat Oncol Biol Phys. 2008; 71(1 Suppl):S170–S173

ICRP, 2001. Prevention of accidental exposures to patients undergoing radiation therapy, ICRP Publication 86

International Commission on Radiological Protection, 2009. Preventing accidental exposures from new external beam radiation therapy technologies. Annals of the ICRP, 39(4)

International Electrotechnical Commission（IEC）, 2006, IEC 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), https://webstore.iec.ch/publication/3571

Jaffray, P., et al. , 2007. TomoTherapy Incorporated PROSPECTUS, http://www.nasdaq.com/markets/ipos/filing.ashx?filingid=4901989

Jeffrey W. V, 2014. Basic Guide to System Safety, Third Edition, Wiley

Johnson, A. J., 2016. FDA Regulation of Medical Devices, https://fas.org/sgp/crs/misc/R42130.pdf

JPL, N., 1990. Jet Propulsion Laboratory Reliability Analyses Handbook, http://everyspec.com/NASA/NASA-JPL/download.php?spec=JPL_D-5703_JUL1990.015049.pdf

JPL, N., 2010. Failure Modes, Effects and Criticality Analysis (FMECA), http://www.klabs.org/DEI/References/design_guidelines/analysis_series/1307.pdf

JPL Special Review Board Report, 2000. Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions, https://spaceflight.nasa.gov/spacenews/releases/2000/mpl/mpl_report_1.pdf

Kevin F., Harold M., 1991. The Relationship of System Engineering to the Project Cycle, in Proceedings of the First Annual Symposium of National Council on System Engineering, October 1991: 57–65.

Kletz, T.A., 2006., Hazop and Hazan. The Institution of Chemical Engineers.

Lawley, H.G., 1974. Operability studies and hazard analysis. Chemical Engineering Progress, 70(4): pp. 45-56.

Leplat, J., 1987. Occupational accident research and systems approach, New Technology and Human Error, pp.181-191

Leveson, N., 2004. A New Accident Model for Engineering Safer Systems, Safety Science, Vol.42, No.4, April, pp.237-270

Leveson, N., 2012. Engineering a safer world: systems thinking applied to safety, MIT Press

Leveson, N., 2018. Safety Analysis in Early Concept Development and Requirements Generation, 28th Annual INCOSE International Symposium, Washington, D.C. (U.S.A.), INCOSE

Leveson, N., Thomas, J., 2018. STPA HANDBOOK, http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Leveson, N., 2019. STAMP Introduction and Overview, 2019 STAMP Workshop, http://sunnyday.mit.edu/workshop2019/STAMP-Intro2019.pdf

Lutz R., Nikora, A., 2005. “Failure Assessment.” In: 1st International Forum on Integrated System Health Engineering and Management in Aerospace, pp.33-34

Meshbesher&Spence, 2015. Radiation Errors Under Investigation, https://meshbesher.com/news-and-updates/medical-malpractice/radiation-errors-under-investigation/

Military, U.S., 1949. MIL-P-1629 Procedures for Performing a Failure Modes Effects and Criticality Analysis

NASA, 1989. Independent Assessment of Shuttle Accident Scenario Probabilities for the Galileo Mission,1, Washington D.C. (U.S.A.)

NASA, 2000. Probabilistic Risk Assessment (PRA), https://www.nasa.gov/pdf/415263main_ProbriskAssessment_200_July.pdf

NASA, 2005. GENESIS Mishap Investigation Board Report Volume I, https://www.nasa.gov/pdf/149414main_Genesis_MIB.pdf

NASA, 2012. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20120001369.pdf

National Academy of Engineering, 1972. Outer continental shelf resource development safety: a review of technology and regulation for the systematic minimization of environmental intrusion from petroleum products, National Academy of Engineering, Marine Board

National Research Council, 1981. Safety and offshore oil, National Academy Press

Pawlicki, T., et al, 2016. Application of systems and control theory-based hazard analysis to radiation oncology. Med Phys, Mar; 43(3), pp.1514-1530.

Project Management Institute, 2018, プロジェクトマネジメント知識体系ガイド PMBOK ガイド 第 6 版. Project Management Institute

Rausand, M., Hoylan, A., 2004. System Reliability Theory: Models, Statistical Methods, and Applications, Wiley Series in probability and statistics—second edition, pp.88

Reason, J., 1990. Human Error, Cambridge, England: Cambridge University Press.

Reason, J., 2000. Human Error: Models and Management. British Medical Journal, 320(March), pp.768–770.

SAE, 1967. ARP926 Design Analysis Procedure For Failure Modes, Effects and Criticality Analysis

SC Times, 2017. 3 more cancer patients sue CentraCare, https://www.sctimes.com/story/news/local/2017/03/10/3-more-cancer-patients-sue-centracare/99000968/

South Florida Times, 2015. Radiation Errors Under Investigation, http://www.sfltimes.com/health-and-fitness/radiation-errors-investigated-at-st-cloud-cancer-center

Stamatis, D.H., 2002, Design for Six Sigma. Six sigma and beyond, ST LUCIE PR

Stewart, M., 2015. Probabilistic Risk Assessment (PRA) How to quantify and understand risk, https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150003057.pdf

Strafaci, A., 2008. What does BIM mean for civil engineers?, CE news, Transportation, pp.62-65

The New York Times, 2019. 80,000 Deaths. 2 Million Injuries. It's Time for a Reckoning on Medical Devices. Patients suffer as the F.D.A. fails to adequately screen or monitor products, https://www.nytimes.com/2019/05/04/opinion/sunday/medical-devices.html

the ST. Cloud Times, 2016. Lawsuits allege radiation errors, http://www.advisen.com/tools/fpnproc/fpns/articles_new_2/P/271732451.html?rid=271732451&list_id=2

Thomas, J., 2017. Implementing STPA Successfully in Industry, MIT STAMP Conference, March 2017, MA (U.S.A.)

U.S. Department of Defense, 1949. MIL-P-1629 - Procedures for performing a failure mode effect and critical analysis. United States Department of Defense, pp.5, 34

U.S. Department of Interior, 2012. Operational Risk Management&Risk Assessment, https://www.bia.gov/sites/bia.gov/files/assets/public/pdf/idc-017618.pdf

Beitia, T., 2012. Operational Risk Management&Risk Assessment, https://www.bia.gov/sites/bia.gov/files/assets/public/pptx/idc017549.pptx

U.S.NRC, 1975. Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400

U.S.NRC, 2018. Probabilistic Risk Assessment (PRA), https://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html

Vesely, W.E., Roberts, N.H.,1981. Fault Tree Handbook. US Independent Agencies and Commissions.

Vincoli, W. J., 2014, "Basic Guide to System Safety, Third Edition," Wiley.

Watson, H., Launch Control Safety Study, 1961, Bell Laboratories: Murray Hill, NJ.

Yamaguchi, S., Thomas, J., 2019. A System Safety Approach for Tomographic Treatment, Safety Science, Vol.118C, pp.772-782

Young, W., 2017. System-Theoretic Process Analysis for Security (STPA-SEC): Cyber Security and STPA, 2017 STAMP Conference, MA (U.S.A), http://psas.scripts.mit.edu/home/wp-content/uploads/2017/04/STAMP_2017_STPA_SEC_TUTORIAL_as-presented.pdf

医学放射線物理連絡協議会，2004．国立弘前病院における過剰照射事故の原因及び再発防止に関する調査報告書，
https://www.jastro.or.jp/customer/guideline/2016/10/hirosakireport.pdf
公益財団法人　日本医療機能評価機構，2014．医療事故情報収集等事業　第40 回報告書, http://www.med-safe.jp/pdf/report_2014_4_T003.pdf
国立研究開発法人　日本原子力研究開発機構, 1999．原子力百科事典 ATOMICA, https://atomica.jaea.go.jp/data/detail/dat_detail_09-03-02-14.html
神奈川新聞, 2009．横浜市大付属病院でまた患者取り違え、健康被害はなし，
https://www.kanaloco.jp/article/entry-121936.html
株式会社テプコシステムズ, 2001．確率論的リスク評価（PRA），
http://www.tepsys.co.jp/assets/pdf/PRA.pdf
兼本　茂, 2018．システムズ理論で考える複雑システムの安全 STAMP/STPA，安全工学，57-5，pp.362-369
原子力委委員会, 2014．確率論的評価手法（PRA）について，
http://www.aec.go.jp/jicst/NC/iinkai/teirei/siryo2014/siryo16/siryo1-1.pdf
後藤　伸寿, 2014．みずほ情報総研　-注目されるリスク評価手法：確率論的リスク評価（PRA）-，　https://www.mizuho-ir.co.jp/publication/column/2014/0408.html
社団法人日本放射線技師会　放射線機器管理士部会　編集，2008．外部放射線治療装置—放射線機器品質管理実践マニュアル（放射線機器管理シリーズ), 日本放射線技師会出版会
清水　吉男，2010. [改訂第 2 版] [入門+実践]要求を仕様化する技術・表現する技術−仕様が書けていますか?，技術評論社（2010）
清水　吉男, 2012．要求仕様記述手法「USDM」ってどんなの？　~明日から使える USDM のエッセンス~，
http://swquality.jp/temp/nagasakiqdg15_usdm.pdf
杉江　俊治，藤田　政之，1991．フィードバック制御入門（システム制御工学シリーズ），コロナ社
日本工業規格（JIS），2000, JIS Z8115:2000 デイペンダビリティ（信頼性）用語, https://kikakurui.com/z8/Z8115-2000-01.html
日本情報システムユーザー協会（JUAS)，2014．ユーザー企業　ソフトウェアメトリックス調査 2014,
http://www.juas.or.jp/cms/media/2017/02/14swm.pdf

日本情報システムユーザー協会（JUAS)，2016．ユーザー企業 ソフトウェアメトリックス調査 2016,
http://www.juas.or.jp/cms/media/2017/02/swm16_ppt.pdf
独立行政法人情報処理機構（IPA），2007．組込みソフトウェア向け開発プロセスガイド, https://www.ipa.go.jp/files/000005126.pdf
独立行政法人情報処理推進機（IPA），2018. STAMP 向けモデリングツール STAMP Workbench,
https://www.ipa.go.jp/sec/tools/stamp_workbench.html
派生開発推進協議会, 2016. USDM 小冊子基礎編,
http://affordd.jp/tech_documents/affordd-t2-usdmtext-basic_1.3.pdf
松岡 猛，2005. FMEA（故障モードおよび影響解析）実施手順,
https://www.nmri.go.jp/oldpages/main/publications/paper/pdf/23/06/02/PNM23060201-00.pdf
山口 晋一，2018．安全解析手法 STAMP/STPA の要件定義工程への適用評価，安全工学，57-5，pp.370-379
山口 晋一，2019．安全解析手法 STAMP/STPA によるハザード影響度に基づく逐次的な安全解析方法の構築評価，安全工学，58-2，pp.124-132

謝辞

本研究を進め，論文としてまとめる過程に至るまで，多くの方々からのご支援，ご指導を頂きましたこと，心より感謝いたしております．そして，今後とも，どうぞよろしくお願いいたします．

本研究の指導教員であり，本論文の主査を務めて頂きました，慶應義塾大学大学院システムデザイン・マネジメント（以下，SDM）研究科の白坂成功教授には終始，研究者として自立できるような心構え，研究活動についての所作や発表に至るまで，幅広くご指導いただきました．白坂教授のお言葉一つ一つが，私にとって大変貴重なものであり，物事に対して深く考えるきっかけを与えてくださいました．その一つ一つを，後に噛み締め，その時には分かり得なかった真意を推察することで，研究者としてより高いレベルを目指して行ける多くのきっかけとなりました．

SDM 研究科の前野研究科委員長には，SDM 研究科への入学前には博士課程への進学と研究を継続するきっかけ，及び多くのご助言を惜しみなくくださり，今日に至るまで大変お世話になりました．SDM 研究科にて学んだことは，学問横断的な内容であり，私にとって何ものにも変えがたい貴重な経験となっております．また，前野委員長のなされている研究の内容を知ることで，私の研究及び生活，公私において，とても充実したものとすることができました．ご教授頂いたライフスキルは，人生を通して大変貴重なものであると思っております．

副査の SDM 研究科の高野教授には，私の入学後の最初の投稿論文に対してのご支援を惜しみなくしてくださり，とても感謝しております．また，在学中の研究の中間報告においても，高野教授のご意見により，今後，さらなる研究を進めていくためのきっかけと安全工学に関する研究会へ参画する貴重な機会を与えてくださいました．そして，本論に対する細部に渡るアドバイスを頂きました．特に安全工学に関する観点からの的確なアドバイスは本論文をまとめる上で非常に助けとなりました．さらには，今後の本研究の発展につながるようなご助力も頂くことができました．

副査の SDM 研究所の狼顧問には，工学的な研究に対する本質的な観点からの，本研究の必要性について大変貴重なご意見を頂きました．また，研究に関して，システムズエンジニアリングの観点からの最新のトレンドを考慮に入れられるきっかけとなるご意見や，本研究にて陥りがちなリスクに至るま

での幅広いご意見を頂きました．これらのご意見は，今後，工学的研究の視野を広げる上で大変，有効なものになると考えております．特に，システムズエンジニアリングに留まらない，多くのご経験から来るご意見は，学問横断的な考え方に基づくものとして捉えられ，今後の研究に対する視野を広げる上で，大変貴重なものとなっております．

副査の長崎県立大学日下部教授には，システムに対する安全性及びソフトウェア工学についての深い知見の中から，私では気づき得なかった本研究で留意しておくべき視点と気づきを与えてくださいました．また，研究者として相手に伝わる的確な表現について考えることの重要性についての気づきとなる，とても重要なご指南を頂きました．さらに細かい箇所に関して，論文中の内容における整合性やその箇所を記載する必要性に至るまでのコメントを頂きました．それにより論文の品質を向上させることができました．システムの安全性あるいはソフトウェアに関する研究に関して，今後とも議論をさせて頂く機会があればと考えております．

SDM の白坂研究室 M ラボの皆様には，特にラボミーティングを通して，皆様の貴重な体験や技術を惜しみなく共有して頂くことで，入学前には得られなかった知見を獲得することができ，人生の視野を広げることができました．また，研究生活における大変有意義な機会を多々，得ることができました．

このように皆様のご支援，ご指導のもと，学問及び研究に真摯に向き合う機会を与えてくださいましたこと，この場を借りてお礼を申し上げたいと思っております．本当にありがとうございました．

研究業績

原著論文（査読付き）

・山口晋一，白坂成功，2018. 安全解析手法 STAMP/STPA の要件定義工程への適用評価，安全工学，57-5，pp.370-379

・山口晋一，白坂成功，2019. STAMP/STPA によるハザード影響度に基づく逐次的な安全解析方法の構築評価，安全工学，58-2，pp.124-132

・Yamaguchi, S.，Thomas, J., 2019. A system safety approach for tomographic treatment，Safety Science，Vol.118C，pp.772-782

※ アンダーライン：本博士論文著者

付録

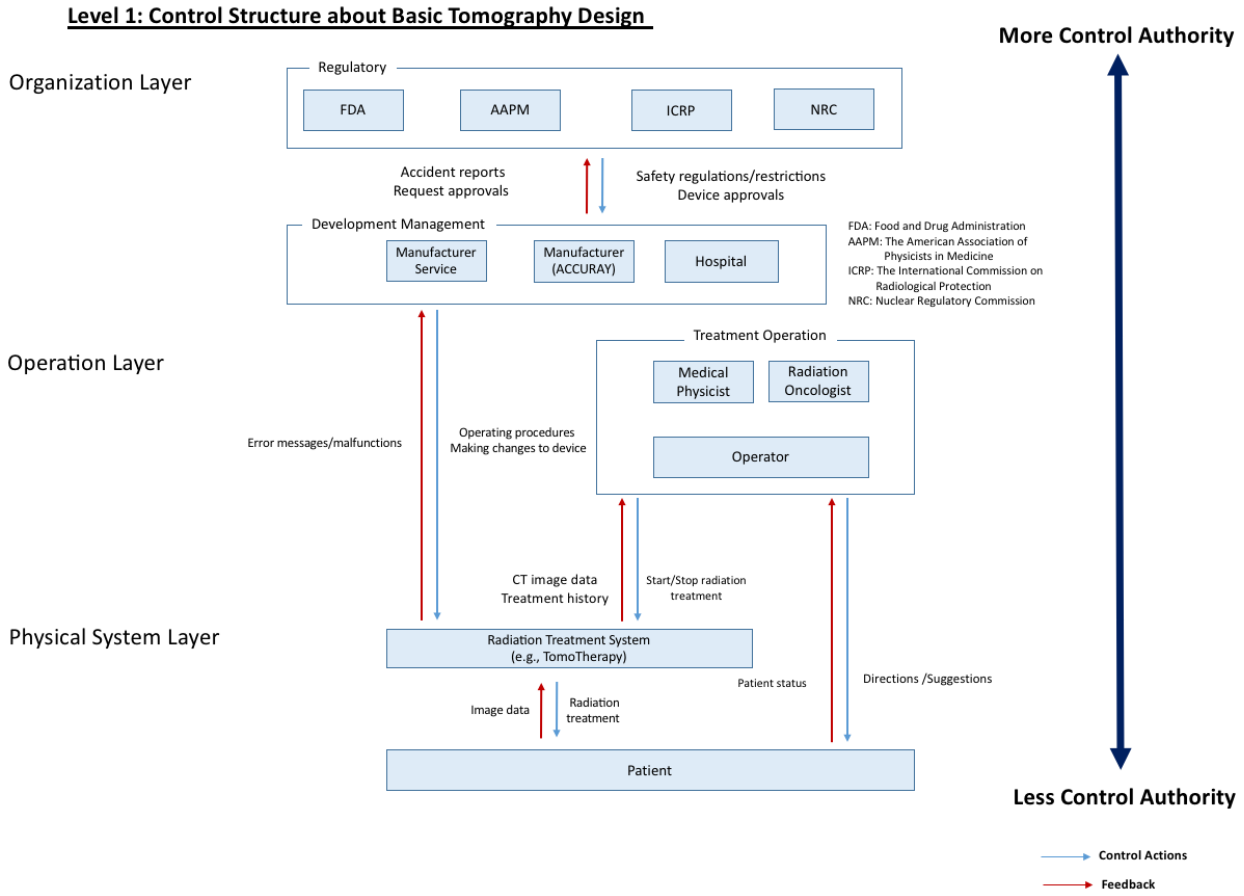


図 A. コントロールストラクチャ（レベル 1）

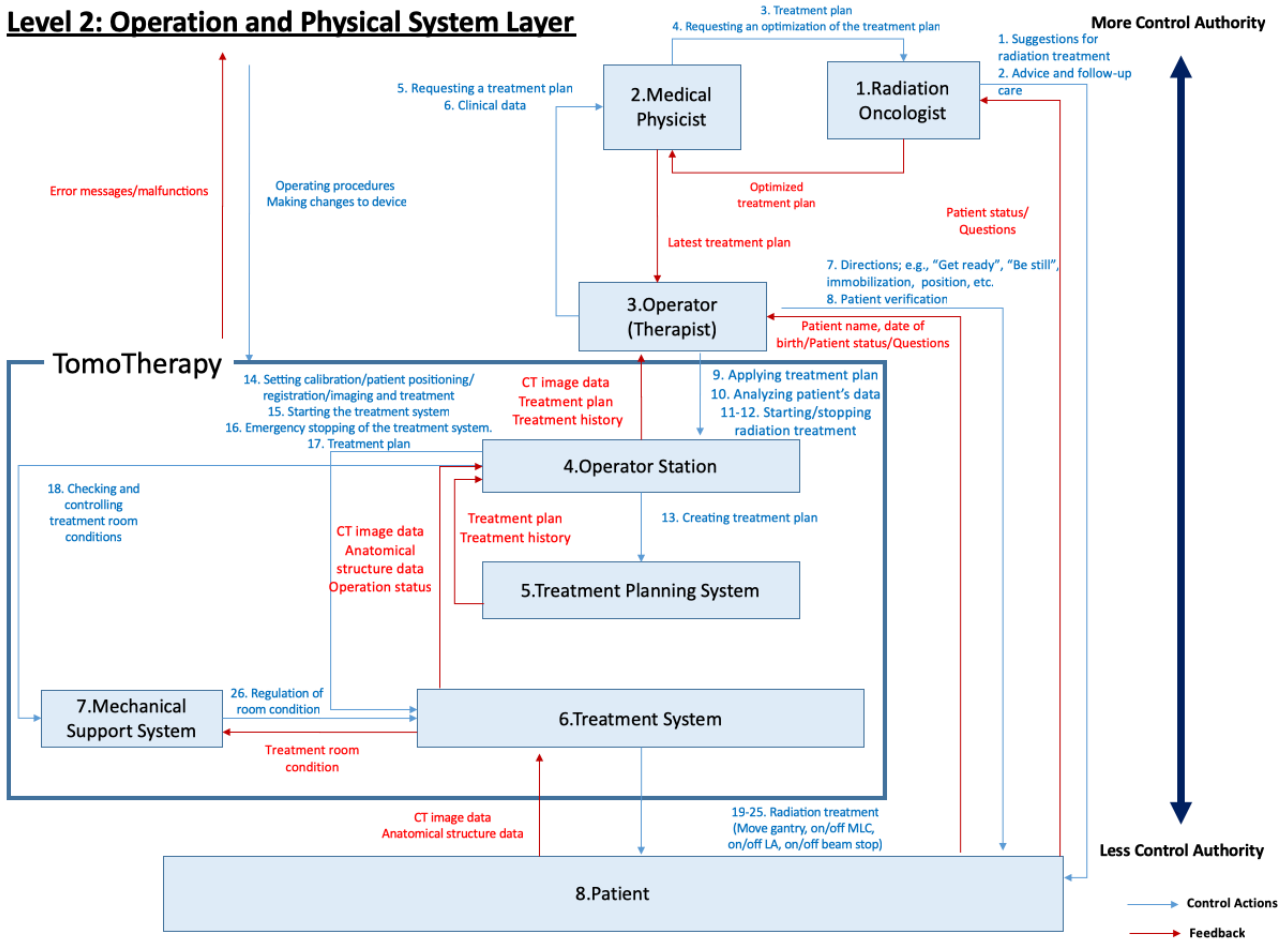


図 B. 詳細化されたコントロールストラクチャ（レベル 2）