論文審査の要旨および担当者

報告番号	甲　第　　号	氏　名	山口　晋一

論文審査担当者：	主査	慶應義塾大学大学院教授　博士（システムエンジニアリング学）	白坂　成功
	副査	慶應義塾大学大学院教授　博士（工学）	高野　研一
	副査	慶應義塾大学附属ｼｽﾃﾑﾃﾞｻﾞｲﾝ・ﾏﾈｼﾞﾒﾝﾄ研究所　顧問　工学博士	狼　嘉彰
	副査	長崎県立大学教授　博士（工学）	日下部　茂

（論文審査の要旨）

山口晋一君提出の学位請求論文は「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」と題し，本文 6 章から構成される．

本論文では，近年の大規模/複雑化するシステムが深刻な事故や損失を引き起こしている現状を踏まえ，システム理論に基づく新しい安全解析手法である STAMP/STPA 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の実現に貢献することを目指している．

具体的には，STAMP/STPA を適用できる 3 つの事項を提案している．第一に，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している．第二に，開発プロセスと安全解析プロセスを統合するプロセスを提案している．第三に，事故に至りうるハザードの影響度を使用して STAMP/STPA での解析の優先順位を考慮した手法を考案している．そして，放射線治療装置へ適用／評価することで提案した内容の有効性を示している．

1 章では，本研究の背景，課題と先行研究，目的と新規性を明確化している．ここではまず，近年の事故の起こりうる原因の特徴を示し，そのような事故を未然に防ぐためにシステム理論に基づく安全解析手法である STAMP/STPA が必要となってきた背景を示している．そして，STAMP/STPA の適用の 3 つの課題を示している．第一の課題は，STAMP/STPA の使用者が，開発プロセスのどの工程で適用するのかを明確化できていないことである．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ていないことである．第三の課題は，STAMP/STPA のために作成するシステムの制御構造図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から導出した安全要件をシステム開発へすぐにフィードバックできていないことである．そして，上記 3 つの課題を解決するために，要件定義工程へ STAMP/STPA を適用するという本研究の意義を述べている．

2 章では，本研究で利用あるいは考慮するべき理論や手法の概要を示している．特に，様々な産業で幅広く使用されている従来の安全解析手法と，システム開発における開発プロセス及び開発コストの関係性を示している．

3 章では，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の 3 つ提案事項を詳細に示している．上記の第一の課題と第二の課題を解決するために，まず 1 つ目として，STAMP/STPA を適用する上で必要な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している．次に 2 つ目として，実際の現場適用を考慮したプロセスフローを提案している．このプロセスフローは，開発プロセスと STAMP/STPA の安全解析プロセスを統合している．さらに，上記の第三の課題を解決するために，3 つ目として， STAMP/STPA での解析対象のシステムにおける非安全な制御指示に優先順位をつけて解析を実施する手法を提案している．特に，提案事項の 2 つ目と 3 つ目については，STAMP/STPA を部分的に実施して導出した安全要件をシステム開発へすぐにフィードバックすることを実現する提案となっている．

4 章では，3 章で提案した要件定義工程へ STAMP/STPA を適用する手法の適用とその適用結果を示している．ここでは，本論文の提案内容を適用対象のシステムである，放射線治療装置の説明及び当該システムを対象とした理由を述べている．そして，3 章で提案した 3 つの事項を活用した STAMP/STPA の適用した結果を，当該システムでの事例を通して詳細に示している．

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．まずはじめに，1 章で述べた 3 つの課題について有効であることを示している．次に，本論文で提案した手法の適用に関する制限事項を示している．そして，従来手法と提案した手法による STAMP/STPA についての考察がなされている．

最後に 6 章では，結論および今後の展望を示している．

以上を要するに，本論文は STAMP/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，開発プロセスと安全解析プロセスを統合するプロセスと STAMP/STPA での安全解析の優先順位をつける手法を考案することで，システム開発の早期工程でシステム理論に基づく安全解析を適用することが可能になったといえる．

本論文は，近年，要件定義工程起因での事故が増加傾向にあるシステム開発に対して，STAMP/STPA を要件定義工程へ効果的に適用できる手法を提案し，放射線治療装置に適用することで，その効果を示す研究を行ったものであり，学術上の寄与が少なくない．従って，本論文の著者は博士（システムエンジニアリング学）の学位を受ける資格があるものと認める．