ソフトウェア要求仕様における HAZOP を応用したリスク項目設計法

河野 哲也†

†株式会社 日立製作所 ソフトウェア事業部 品質保証部
〒244-8555 横浜市戸塚区戸塚町 5030 番地
E-mail: †tetsuya.kouno.cb@hitachi.com

あらまし ソフトウェアに起因するトラブルが後を絶たない．そのようなトラブルを未然に防止するためには，ソフトウェア開発の早い段階からプロダクトリスクの識別・分析・軽減といったリスクマネジメントを徹底的に実施・運用することが重要である．本研究では，ソフトウェア開発におけるリスクマネジメントのうちリスクの識別・分析に焦点をあて，USDM（Universal Specification Describing Manner）で記述された要求仕様を対象とし，HAZOP（HAZard and OPerability study）を応用したリスク項目を設計する手法を提案する．

キーワード USDM，HAZOP，ガイドワード，リスク識別，リスク分析，ソフトウェアレビュー

An Application of HAZOP to Risk Analysis of Software Requirement Specification

Tetsuya KOUNO†

† Software Division, Hitachi, Ltd.
5030, Totsuka-cho, Totsuka-ku, Yokohama, 244-8555 Japan
E-mail: †tetsuya.kouno.cb@hitachi.com

Abstract Troubles resulting from software are increasing. In order to prevent such a trouble beforehand, it is important to carry out risk management, such as identification, analysis, and mitigation of a product risk, from the early stage of software development.. This paper applies HAZOP (HAZard and OPerability study) to risk identification and analysis of software requirement specification written in USDM (Universal Specification Describing Manner). Moreover this paper presents a design method of risk items.

Keyword USDM, HAZOP, Guide words, Risk identification, Risk analysis, Software Review

1. はじめに

近年，ソフトウェアは我々の生活に欠かせない存在になった．そのため，ソフトウェアによる不具合が大きなトラブルに発展することが多い．しかしながら，ソフトウェアに起因する問題は後を絶たない．

そのような問題を未然に防止するためには，ソフトウェア開発の早い段階で不確実で望ましくない事柄，すなわちリスクを徹底的に検討する必要がある．つまり，リスクの識別・分析・軽減[1]といったリスクマネジメントを徹底的に実施・運用することが重要となる．ここで，本研究で論述する「リスク」は，プロジェクトリスクではなく，プロダクト（製品）リスクを指す．

ソフトウェア開発の初期段階で作成される成果物の一つにソフトウェア要求仕様（以降，要求仕様と略す）がある．近年，ソフトウェア要求仕様の記述方法において，USDM[2]の普及・取り組みが進んでおり，またいくつかの報告もある[3][4][5].

現在，ソフトウェア開発現場で USDM の普及が進んでいるものの，USDM で記述された要求仕様に対してどのような望ましくない事柄，振舞い，状態などが考えられるのかといったリスクの識別・分析は各現場・各組織でなされていると推察されるが，その報告は少ない．

例えば，そのような報告の一事例として，形式検証アプローチによる研究がある[6]. この研究では，USDM で記述された要求仕様の論理構造に着目し，その構造を利用することで形式検証を行い，仕様間の矛盾・不整合や仕様の漏れや未定義などの検出に効果を示している．

本研究では，形式検証とは異なるアプローチとして，HAZOP[7]というリスク解析手法を応用し要求仕様の仕様項目個別に対してリスク識別・分析の検討を進める．具体的には，USDM で記述された仕様項目に対し，仕様に関わる振舞いの逸脱（ズレ）をリスクとして捉え，HAZOP を応用することで，それらの抽出およびリスク項目を設計する方法の検討を行う．

HAZOP は，これまでハードウェアを主軸として用いられてきた手法であるが，ソフトウェア開発において

応用した研究がいくつか報告されている．例えば，ガイドワードを利用し，UML や状態遷移図などのモデルの構成要素における逸脱を洗い出すことでリスクの識別・分析を行っている[8][9]．このようにソフトウェア開発において HAZOP を応用した研究はいくつか報告されているが，USDM で記述された要求仕様に関して検討は行われていない．

本研究では，現在多くの現場で取り組みが進んでいるという背景に基づき USDM に焦点をあて，HAZOP を応用しリスク項目を設計するための手法を提案することを目的とする．

以降，2 章では本研究のスコープを整理する．3 章ではリスク項目設計法を提案する．4 章では提案の有効性を確認するために検証を行う．

2. リスク項目の設計

2.1. 要求仕様

要求仕様を記述する方法は，今まで様々な取り組みが行われてきたが，その中でも近年，注目されているのが USDM である．まず，図 1 に USDM で表現された要求仕様を例示する．

図 1 が示すように，USDM は，要求と仕様を階層構造で表現する方法である．要求を分割・階層化してその範囲を制御し，範囲が制御された要求の中で仕様の抽出・表現を行う．また，要求に対してその理由を記述することにより，要求の理解を助けるように工夫が施されている．さらに，設計しながら記述されがちな仕様を開発の早い段階で要求とセットで表現することがこの方法の重要なポイントである．

要求1	受信した電子メールをキーワード検索したい		
	理由1	メールが多くて、関連するメールが探せない	
	要求1-1	検索対象のメールボックスを 指定してグループ化できる	
		理由1-1	仕事上のメールとニュース等の メールを分けて扱いたい
		仕様1-1-1	メーラーが管理するメールボックスを一覧表示する
		・・・	・・・
		仕様1-1-4	一覧からメールボックスを選択したグループに指定する
	要求1-2	いくつかのキーワードを 組み合わせて検索できる	
		理由1-2	可能性のあるキーワードで探したい
		仕様1-2-1	検索したいキーワードを入力できる

図 1　要求仕様の例（文献[2]から引用）

ここで文献[2]では，仕様とは「要求（実現してほしいこと）を満たすべき具体的な振舞いの記述」と定義している．本研究ではこの定義に従い，USDM で記述された仕様という前提を置き，検討を進める．

2.2. リスクマネジメントと HAZOP

リスクマネジメントは，大きく「リスク識別」・「リスク分析」・「リスク軽減」の 3 つに分けて実施・運用される[1]．リスク識別では，想定されるリスクを可能な限り抽出し，各ステークホルダで合意・識別を行う．

リスク分析では，識別されたリスクを分類・整理し，リスクに関連する可能性や影響を調査し，リスクの評価を行う．

リスク軽減では，評価されたリスクに対して，リスクの軽減策を検討し，設計対応やレビュー・テストでの確認などのリスク軽減措置をとる．

ここでリスク識別・リスク分析をサポートするための手法が，HAZOP や FMEA，FTA などのいわゆるリスク解析手法である．これらのリスク解析手法は，従来，ハードウェアを主として適用・実践されてきたが，ソフトウェアにおいてもさまざまな取り組みが報告されている．例えば，HAZOP では先に述べた研究事例があり，FMEA や FTA でもいくつかの取り組み・検討が報告されている[10][11][12]．

ここで，FMEA や FTA のように系統立てて実施される手法に対して，HAZOP はガイドワードをベースにして広く動的に実施される手法である[13]が，その反面発散する傾向もある．そのため，リスク解析を行う際には，解析対象のスコープや設計目標を事前に定めておく必要がある[7]．このような点を踏まえると，USDM では，要求と仕様とがセットで表現・列挙されているため，相性が良いと考えられる．

以上の背景を踏まえ，本研究では USDM で記述された要求仕様を対象として HAZOP というリスク解析手法を応用することにする．

HAZOP とは，主に化学プラントのリスク解析に使われてきた手法であり，流量や圧力，温度などの解析対象の特性に対して，「ない」「早い」「遅い」などの正しい状態・動作からの逸脱（ズレ）を表すガイドワードを組みわせることで，リスクの抽出を試みているのが特徴である．

また，HAZOP は，元々化学プラントに用いられていたという背景もあり，流れや処理，手続きなどのプロセスに着目し，それらの正常な状態からの逸脱を検討しリスクを抽出しているのも特徴である．

2.3. HAZOP によるリスク項目の設計

本研究では，USDM で記述された仕様に対し HAZOP を応用する．すなわち，USDM で記述された仕様，つまり「要求を満たすための具体的な振舞い」からの逸脱をリスクとして捉え，USDM で記述された仕様項目とガイドワードを組み合わせてリスクの抽出・検討を進める．

例えば，図 1 の仕様 1-1-1「メーラーが管理するメー

ルボックスを一覧表示する」に対して，ガイドワード「ゆっくり」を組み合わせると「メーラーが管理するメールボックスをゆっくり一覧表示する」というリスクが考えられる．

ここで，「メーラーが管理するメールボックスをゆっくり一覧表示する」のように仕様とガイドワードを組み合わせてリスクを表現したものをリスク項目と呼ぶ．また，それらを抽出・検討する行為をリスク項目の設計と呼ぶ．

以上，仕様とガイドワード，およびリスク項目のイメージを図２に整理する．

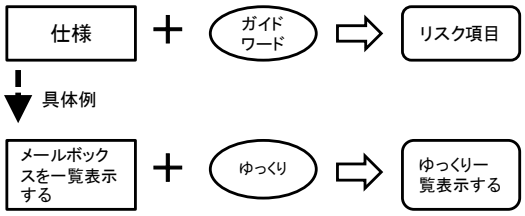

図２　リスク項目設計のイメージ図

図２が示すように仕様に対してリスク項目を設計する際，ガイドワードがその支援を行うことになる．例えば，経験の浅いエンジニアがリスク項目の設計を行うような場合は，特に有効に働くものと考えられる．

本研究では，従来提案されているガイドワードを応用し，リスク項目設計法を提案する．次章では，まず提案手法の全体像を示し，次にガイドワードの整理を行う．

3. HAZOP を応用したリスク項目設計法

本章では，まず HAZOP を応用したリスクマネジメントの全体の流れを整理し提案する手法の全体像を示す．次に，本手法で利用するガイドワードを整理する．

3.1. 提案する手法の全体像

本研究では，応用 HAZOP の手順[14]に従い，提案手法の全体像を以下のように定める．

手順１：対象仕様の選定
手順２：リスク項目の設計
手順３：リスク項目の評価
手順４：リスク項目の対策

以降，各手順の詳細について述べる．

手順１では，リスク項目の設計の対象とする仕様を選定する．HAZOP は，使用するガイドワードの数にも依存するが，多くの時間を要するという欠点がある．そのため本研究では，要求仕様全体ではなく，対象とする要求項目を選定し，それに属する仕様項目に対してリスク項目の設計を行うこととする．なお，要求項目を選定する際には，要求の優先順位やそれに属する仕様のリスク潜在度合いなどを考慮する．

手順２では，まず表１に示すような対象仕様項目とガイドワードを組み合わせたリスク項目抽出表を作成する．次に，仕様項目と各ガイドワードの交点（表のセル）に対してリスク項目案を抽出する．リスク項目案は，表１のセル部分に示すような仕様に対しての正常な状態や振舞いからのズレを表現したものとなる．このように仕様項目とガイドワードを組み合わせて検討を進めるため，網羅的なリスク項目案の抽出が可能となる．そして，抽出したリスク項目案に対してユーザにとっての影響を検討し，望ましくない影響を及ぼすと判断されたリスク項目案をリスク項目として採用する．

例えば，表１の「すばやく表示される」というリスク項目案はユーザの使用性という観点からは良い影響を及ぼすことが想定されるが，「遅く表示される」というリスク項目案からはユーザの業務に遅延が生じるという望ましくない影響が想定される．よって，この場合は，リスク項目案「遅く表示される」はリスク項目として採用され，リスク項目案「すばやく表示される」はリスク項目として採用されない．

なお，以上の検討は，ユーザにとっての影響であり，例えば「遅く（ゆっくり）表示される」は望ましい影響を与える場合もあるため，一意に判断できないことに注意されたい．

表１　リスク項目抽出表

		仕様項目		
		検索されたメールの「Subject」を一覧で表示する	検索されたメールに連続番号を付けて表示する	.....
ガイドワード	ない	.....	番号が付かずに表示される	.....
	早い	すばやく表示される	.....	.....
	遅い	遅く表示される	.....	.....
	・・・	.....	.....	.....

表２　リスク項目評価表

リスク項目	影響	想定原因	影響度	発生可能性	リスク度	対策
「Subject」の一覧が遅く表示される	業務が遅延する	表示時に並列で検索を走らせている	3	3	9	メール検索の並列処理を禁止する
検索されたメールに番号が付かずに表示される	.....	.....	...	...	...	...
.....	.....	.....	...	...	...	...

手順３では，手順２で得られるリスク項目を列挙し，表２に示す FMEA 表のような形式で整理する．そして，各リスク項目に対して影響度と発生可能性の指標を用いてリスク度を算出し，その値により対策の可否を評価する．

手順４では，手順３で得られた表において，リスク

度の高いリスク項目に対して対策の実施を進める．なお，対策は一時的なものではなく，設計や実装におけるレビューやテスト項目への反映とテスト実行での確認など開発ライフサイクル全体を通して実施することが肝要である．

以上，手順１～手順４で手法の全体像について述べたが，手順２においてリスク項目案を漏れなく網羅的に抽出することが特に重要である．そのために，次節では，リスク項目案の抽出を支援するガイドワードに焦点を当て，検討を進める．

3.2. ガイドワードの整理

元々,HAZOP は化学プラントの安全解析に用いられたこともあり，化学工業分野で発展してきた．また，主に英語によってガイドワードが提案されていたという背景もあり,HAZOP は適用の範囲が限られた手法であった．

そのような課題に対して，鈴木らが提案した応用 HAZOP では，ヒューマンエラーの解析のために，日本語でガイドワードの整理を行い，さらにガイドワードを拡充している[14]. そのガイドワードを図３に示す．

ガイドワードの特徴		ガイドワード		
動作の量	動作の有無	全く～しない		
	カの程度	強く	弱く	
	動作の速度	急いで	ゆっくり	
	持続時間	ずっと	短く(一時的に)	
	動作範囲	余分に	不十分に	
動作の向き	方向	反対に	他に	
	回転	反対に		
動作の種類		違う		
動作の対象	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	
時間		まだ	すでに	同時に
		別々に		
順序		前に	抜かして	後に
		余分に	繰り返し	反対に
回数		多く	少なく	

図３　鈴木らが提案したガイドワード

本研究では，鈴木らが提案したガイドワードの拡張・整理を行う．具体的には，鈴木らのガイドワードでは人の動作に着目している点を，仕様で記述される振舞いに置き換えガイドワードを整理する．先に，整理した結果を図４に提示しておく．

まず，鈴木らが提案したガイドワードの「動作」という視点に対して，仕様が対象とするのは「振舞い」であるため，その置き換えを行う．

そして，仕様で表現されるのは,「表示する」や「検索する」といった「振舞いそのもの」と「検索結果一覧」や「保存メール」といった「振舞いの対象」と大きく２つに分けることができる．よって，図４に示すように，２つの着目点でガイドワードを分類する．

加えて，ガイドワードの整理として,「対象物の量」の着目点に対して,「null」や「０」を意味する「なし」というガイドワードを追加する．また，図３では,「動作の向き－回転」のガイドワード「反対に」は,「動作の向き－方向」のガイドワードで補うことができると考え，除外する．

本研究では，図４に示す２９のガイドワードを活用し，リスク項目案の抽出を行っていく．なお，今後，活用をより支援するために，これらのガイドワードに対しての考え方や具体例を整備していく必要がある．

着目点		ガイドワード		
振舞いそのもの	有無	全く～しない		
	程度	強く	弱く	
	速度	急いで	ゆっくり	
	持続時間	ずっと	短く(一時的に)	
	範囲	余分に	不十分に	
	向き	反対に	他に	
	種類	違う		
	タイミング	遅く	早く	同時に
		別々に		
	順序	前に	抜かして	後に
		余分に	繰り返し	反対に
	回数	多く	少なく	
振舞いの対象	対象物	違うものに		
	対象物の向き	反対に		
	対象物の量	多く	少なく	なし

図４　本研究で提案するガイドワード

4. 検証

本章では，3 章で提案したリスク項目設計法の有効性を確認するため，実際にリスク項目を設計する実験を行う．

4.1. 検証方法

本検証では，図５に示す電子メールソフトの仕様を対象とし,実験の時間的な制約により仕様１,仕様３,仕様４の３つの仕様に絞って実施した．

要求	検索された電子メールのリストを表示し、 そこから目的のメールを選択する
理由	メールの中身を開いて確認する必要がある
<検索件数の表示>	
仕様1	検索されたメールの件数を一覧の上に表示する
<検索メールの表示>	
仕様2	検索されたメールの「Subject」を一覧で見せる
仕様3	検索されたメールに連続番号を付けて表示する
仕様4	検索されたメールの件数10件を超えるときは スクロールバーを見せる

図５　適用対象（文献[2]から引用）

本検証では，提案手法を使用せず経験的にリスク項目を設計するグループ（経験ベースグループと呼ぶ）と提案手法を使用してリスク項目を設計するグループ（手法使用グループと呼ぶ）との２つのグループによりリスク項目を設計する実験を行い，その結果を比較・評価する．以上の概要を図６に整理する．

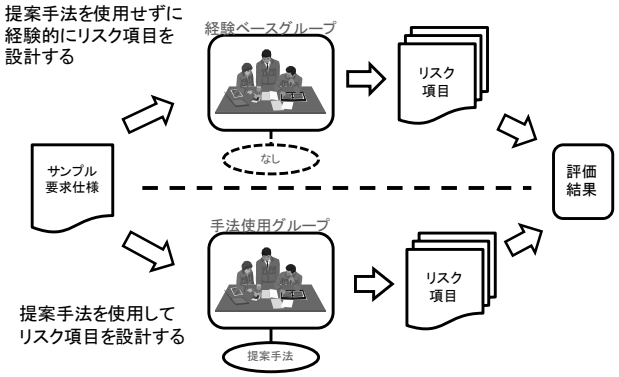

図６　検証の概要

そして，実験協力者はオープンミドルウェアやプラットフォーム分野の品質保証業務に従事する技術者とし，それぞれのグループに２名ずつアサインした．また，実験協力者をアサインする際には，業務経験が提案手法の方に有効に働かないように配慮した．実験協力者の詳細を以下に示す．なお，実験協力者は，品質保証業務の一環としてＦＴＡを実施しているため，その経験もあわせて以下の括弧内に示す．

・経験ベースグループ
　実験協力者Ａ１：業務経験約９年
　　（通常業務で２年程度実施）
　実験協力者Ａ２：業務経験約１２年
　　（経験なし）
・手法使用グループ
　実験協力者Ｂ１：業務経験約４年
　　（業務で一回程度実施）
　実験協力者Ｂ２：業務経験約３年
　　（経験なし）

加えて，実験の手順は，次のように設定した．

・経験ベースグループ
　まず，各仕様項目に対して経験に基づきリスク項目案を抽出する．そして，抽出したリスク項目案に対してユーザにとっての影響を検討し，望ましくない影響を及ぼすと判断されたリスク項目案をリスク項目として採用する．
・手法使用グループ
　3.1節の手順２に従い，リスク項目を設計する．

両グループの手順の差異は，リスク項目案の抽出を経験に基づくものにするのか，ガイドワードに基づくものにするのかの違いである．

また，本実験では，上記手順のリスク項目案の抽出を１時間，リスク項目の採用を３０分で実施することとした．なお，本実験では，実業務に近づけるため，リスク項目案の抽出は個人作業としリスク項目の採用はグループ作業とした．

また，両グループとも，リスク項目案を抽出する作業からを開始とし，組合せ表やワークシートの作成は事前に筆者が行った．

4.2. 実験結果と評価

まず，両グループの各実験協力者によって抽出されたリスク項目案の数を表３に示す．

表３　抽出したリスク項目案数

グループ	実験協力者	仕様1	仕様3	仕様4
経験ベース	A1	9項目	11項目	10項目
	A2	9項目	9項目	7項目
手法使用	B1	29項目	29項目	29項目
	B2	25項目	26項目	25項目

経験ベースグループの実験では実験時間として，実験協力者Ａ１・Ａ２ともに１時間を要することなく４５分で想定されるリスク項目案を出し尽くす結果となった．

そして，抽出したリスク項目案に対しユーザにとっての影響の検討を行った．その結果，全てのリスク項目案が採用され，その数は，仕様１では１４項目，仕様３では１８項目，仕様４では１３項目となった．また，この検討を行った際に，仕様３に対して２項目のリスク項目が抽出された．

次に，手法使用グループの実験では実験時間として，実験協力者Ｂ１・Ｂ２ともに１時間全てを要してリスク項目案の抽出を行う結果となった．また，時間的な制約もあり，実験協力者Ｂ２は３～４個のガイドワードに対してリスク項目案の抽出ができなかったが，２９のガイドワードに対して概ねリスク項目案の抽出は実施できたと考えられる．

そして，抽出したリスク項目案に対して，ユーザにとっての影響の検討を行った．その結果，採用したリスク項目の数は，仕様１では２２項目，仕様３では２７項目，仕様４では２２項目となった．採用されなかったリスク項目案の具体例として，「すぐ表示される」や「表示するタイミングが早い」といったものが見られた．

以上の経験ベースグループと手法使用グループの結果を表４に整理する．

表４が示すように，全ての仕様項目に対して，手法使用グループのほうが多くのリスク項目の設計が行え，

提案手法が有効に働いたと考えられる．次に，リスク項目の質的な考察を行う．

表４　実験結果

グループ	仕様1	仕様3	仕様4
経験ベース	14項目	18項目	13項目
手法使用	22項目	27項目	22項目

まず，お互いのグループで設計したリスク項目に対して，もう一方のグループでも設計されたリスク項目の有無を調査した．その結果を表５に示す．なお，リスク項目の記述内容によって，一項目同士の対応にならないものもあった．例えば，リスク項目「件数が表示されない（常に０や空白)」に対して「件数が空白で表示される」と「件数が０で表示される」という対応が見られた．

表５　リスク項目の包含関係

グループ	重複の有無	仕様1	仕様3	仕様4
経験ベース	しない	9項目	11項目	7項目
	する	5項目	7項目	6項目
手法使用	しない	15項目	19項目	16項目
	する	7項目	8項目	6項目

表５が示すように，両グループでリスク項目の重複は見られるものの，一方で重複しないリスク項目もそれ以上に見られる．

例えば，仕様４では重複するものとして
・１０件以上でもスクロールバーが表示されない
・１０件以下でスクロールバーが表示される
・スクロールバーが動かない
といったリスク項目が見られた．

一方で，経験ベースグループに限られるものとして，
・スクロールバーを動かしても一覧が動かない
・一度スクロールバーを表示すると再検索で１０件以下になっても消えない
といったリスク項目が見られ，手法使用グループに限られるものとして，
・スクロールバーの表示位置が違う
・スクロールバーの表示タイミングが遅い
・スクロールする範囲が不十分
といったリスク項目が見られた．

経験ベースグループによって設計されたリスク項目では、「スクロールバーを表示する」という仕様に対して、より広い視点、例えばユーザシナリオの視点によって抽出されているという特徴が見られた。

以上の結果を実務での運用という視点で捉えると，いずれかの方法の一方に限定して適用するのではなく，経験と手法を併用して適用するほうが望ましい．

一方で，設計されたリスク項目の有効性の評価に関しては別途検討を進める必要がある．

5. おわりに

本研究では，ＵＳＤＭで記述された要求仕様を対象とし，リスク解析法の一つである HAZOP を応用しリスク項目の設計法を提案した．さらに，リスク項目を実際に設計する実験を行い提案の有効性が確認できた．

今後の課題として，適用を容易にするためのガイドワードの整理，実際のソフトウェア要求仕様書への適用，および USDM 以外の方法によって記述された要求仕様への展開などが考えられる．

文　献

[1] Japan Software Testing Qualifications Board 技術委員会(訳) (2011)：「テスト技術者資格制度 Advanced Level シラバス 日本語版 Version 2007 .J02」.

[2] 清水吉男 (2005)：「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.

[3] 中井栄次 他(2009)：無知見プロジェクトに対する XDDP の適用- USDM, プロセス設計によるプロセス改善 -，第 28 回 ソフトウェア品質シンポジウム 2009.

[4] 本多慶匡 他(2010)：XDDP と USDM でプロジェクトの課題解決，派生開発カンファレンス 2010.

[5] 久保明(2011)：測色計の組込みソフトウェア開発における QCD 同時達成への挑戦 ～XDDP、USDM、PFD の活用～，派生開発カンファレンス 2011.

[6] 藤倉俊幸(2011)：ユースケースと USDM にセミフォーマル手法を適用した要求検証，派生開発カンファレンス 2011.

[7] 小野寺勝重 (2006)：「グローバルスタンダード時代における実践 FMEA 手法」，日科技連出版社.

[8] 金周慧 他(2011)：状態遷移図に着目した安全要求分析手法，第 8 回クリティカルソフトウェアワークショップ.

[9] Hansen K.M., Wells L., Maier T., (2004) : HAZOP Analysis of UML-Based Software Architecture Descriptions of Safety-Critical Systems, Proceedings of Nordic Workshop on the Unified Modeling Language 2004.

[10] 山科隆伸 他(2008)：保守開発型ソフトウェアを対象としたソフトウェア FMEA の実証的評価，ソフトウェア品質シンポジウム 2008.

[11] 夏目珠規子 他(2011)：ソフトウェア開発における FMEA の適用可能性検討，第 41 回信頼性･保全性シンポジウム.

[12] 高山啓(2010)：ソフトウェア製品開発における FTA による信頼性リスク分析，ソフトウェア品質シンポジウム 2010.

[13] 中谷多哉子(2010)：安全性向上への要求工学の貢献の可能性，組込みソフトウェアによる信頼性及び安全性, SEC journal Vol.6, No.3.

[14] 鈴木和幸他(2002)：未然防止のための潜在的エラーモード抽出，信頼性学会誌, Vol.24, No.7.