Institute of Electronics, Information, and Communication Engineers

一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
KBSE2013-45 (2013-9)

シーケンス図に基づくディペンダビリティケース作成法の適用性検討

丁　峰† 山本　修一郎‡

†名古屋大学　大学院情報科学研究科　山本研究室〒464-8601 名古屋市千種区不老町
‡名古屋大学　情報連携統括本部 情報戦略室〒464-8601 名古屋市 464-8601 名古屋市千種区不老町
E-mail: †ding.feng@i.mbox.nagoya-u.ac.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

あらまし　筆者らはこれまでシーケンス図に基づくディペンダビリティケースの作成法を提案した.また名古屋大学の物品購入のシーケンス図を用いてこの作成法の有効性を確認した.本稿では、実際のシステムのシーケンス図を対してHAZOPによるリスク分析に基づく実験を行うことにより提案手法の適用性を評価する.

キーワード　ディペンダビリティケース，UML，シーケンス図，適用性,HAZOP,リスク,ガイドワード

A method to verify the applicability of the D-case based on Sequence diagram

Feng Ding †　　Shuichiro Yamamoto ‡

† Nagoya University, Gruduate School of Information Science, Yamamoto Lab.

Furo-cho. Chikusa-ku, Nagoya 464-8601 Japan

‡ Nagoya University, Strategy Office, Information and Communications Headquarters

Furo-cho. Chikusa-ku, Nagoya 464-8601 Japan

E-mail: †ding.feng@i.mbox.nagoya-u.ac.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

Abstract　We have proposed the method for developing a D-case based on Sequence diagrams. In this paper, an experimental result will be shown to evaluating the applicability of the method using HAZOP.

Keyword　Dependability case, UML, Sequence diagram, Experiment, HAZOP

1. はじめに

1.1. 研究の背景

現代のシステムは大規模化と複雑化が急速に進展している.このようなシステムの仕様書に対する要求は完全性だけではなく、その信頼性、安全性も注目されている.[1]

このため、システムのディペンダビリティに関する研究が最近注目されている.ディペンダビリティケースはシステムがディペンダビリティ要求を満足することを示すために必要となる確認手法である.[2][3][4]

システムのディペンダビリティを保証するためには、システム開発プロセスの各段階のディペンダビリティを確認しなければならない.現場のシステム開発において、UMLがよく使われている.[5]このため、UMLの各モデルについてディペンダビリティケースを導入して、それらのディペンダビリティを確認する必要がある.したがって、UML の各モデルに対してのディペンダビリティケース作成法は重要な課題になっている.[6][7][8][9]

筆者らによる論文[10]では UML の中のシーケンス図に基づくディペンダビリティケースの作成法を提案した.さらに名古屋大学の物品購入の手順に基づいて作成するシーケンス図を具体的な例として、このディペンダビリティケースの作成法の有効性を検討した.

1.2. 本稿のねらい

前回の論文で提案したディペンダビリティケースの作成法の有効性を確認したが、この作成法の適用性についてはまだ検討していなかった.このため、本稿では実験を用いてこの作成法の適用性を確認する.また実験の結果を分析することにより、提案手法を改善する.

シーケンス図の各要素についての検討はディペンダビリティケースを作成するために不可欠である.とくにシーケンス図に対するリスク分析は、ディペンダビリティを確認するために重要である.このため、本稿では HAZOP（Hazard and Operability Analysis）を利用して、シーケンス図の各要素のリスク分析手法について研究する.[11][12][13]

This article is a technical report without peer review, and its polished and/or extended version may be published elsewhere.
Copyright ©2013 by IEICE
NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

とくに、具体的な例を利用することにより、HAZOPを利用してリスク分析を実施するという新しい作成法の適用性を検討する.すなわち、シーケンス図の各要素のリスク項目への対策結果に基づいた、ディペンダビリティケース作成手順を説明する.さらに任意のシーケンス図にこの作成法を適用してディペンダビリティケースを作成できることを本研究の目標とする.

以下では、まず第２章で関連研究を説明する.第３章で作成法の適用性についての実験結果に基づいて、ディペンダビリティケース作成法を改善する.第４章では、HAZOP 分析を UML に応用する意味を考察する.第５章で、シーケンス図の各要素についての HAZOP に基づくリスク管理の考え方を提案する.第６章では、HAZOP を利用したリスク分析結果を用いたディペンダビリティケース作成手順を明らかにする.さらにディペンダビリティケース作成法の適用性を評価する.最後に第７章ではまとめと今後の課題を明らかにする.

2. 関連研究

社会的に大きな影響をもつシステムの安全性が注目されている.最近、安全性だけでなくセキュリティーやディペンダビリティなども社会的に大きな話題になってきている.このため、高いディペンダビリティが要求されるシステムの開発運用においてディペンダビリティケースを導入することが必要である.

現在でも開発運用文書を用いてシステム開発や運用を効率化している.しかし、このような開発文書だけでは、ディペンダビリティに付いての主張や、主張が成立することを示す明示的な証拠がない.ディペンダビリティケースでは，主張，説明（Strategy），前提（Context），証拠（Evidence）によって，システムのディペンダビリティに関する議論を構造化して確認することができる.

現在,多くのシステム開発プロセスで UML(Unified Modeling Language)を使っている.UML は、開発対象システムをモデルかする際の記法を規定した言語である.システムの構成と機能を UML モデルから理解することができる.したがって、システムの開発文書のディペンダビリティを確認するためには、開発プロセスで利用された UML の各モデルのディペンダビリティを確認すべきである.しかし、現在では、各モデルに対してのディペンダビリティケースの作成法はまだ明確ではない.このため前回の論文で、筆者らは UML モデルの一つとしてのシーケンス図に基づくディペンダビリティケースの作成法を提出した.

本稿ではこの提案手法の適用性を検討する.とくに本作成法ではリスク緩和のために，どのような対策が証拠として用意されているかを明らかにする必要がある.したがって、リスクについて考慮することも重要である.このため、本稿では HAZOP を応用して UML モデル要素のリスク分析を実施することを考える.

以上をまとめると、次のようである.現在のソフトウェア開発現場で UML の普及が進んでいる．しかし，UML で記述された開発生産物に対するディペンダビリティを保証する方法と、HAZOP によるリスク分析手法が明確ではないという問題がある．このため、HAZOP を用いたリスク分析に基づくディペンダビリティケース作成手法が必要である.

3. 実験と作成法改善

3.1 実験

前の作成法に基づく実験を実施した.この実験は山本研究室のメンバーの協力を得て実施した.この実験の目的は次の２つである.（１）実験の結果を利用して作成法を改善すること（２）改善した作成法の適用性を評価すること.

まず、従来の作成手順を説明する.

ディペンダビリティケースを作る前に、シーケンス図の各要素について検討する.シーケンス図はオブジェクト、実行仕様、実行順位、メッセージ、と結合フラングメントから構成されている.この五つの要素が主張（ゴール)、前提（コンテクスト)、戦略（ストラテジー)、証拠（エビデンス)、四つの方面で検討する.シーケンス図に基づくディペンダビリティケース作成手順はGSNのTop-Down作成法に基づいて作成した.

作成手順＜A＞はシーケンス図なかの結合フラングメントを検査して、存在したら、結合フラングメントの属性によってシーケンス図を分解する.作成手順＜B＞と作成手順＜C＞では、シーケンス図の他の要素が主張、前提、戦略、証拠の方面で検討する結果を用いて、ディペンダビリティケースを作成する.以上は作成手順を終わる.具体的な内容を示す.

「作成手順」＜A＞

1.結合フラグメントがあれば、結合フラグメントの種類によって分析して、複合シーケンス図は単純なシーケンス図に分解する.

2.各シーケンス図についてディペンダビリティケースを作成する.

「作成手順」＜B＞

1.シーケンス図に対する主張（シーケンス図がディペンダブルである）を作成する

2.シーケンス図の各要素について説明する

3.主張に対する前提を提示する

4.オブジェクトをサブゴールにする

5.メッセージをサブゴールにする

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

6.実行順序をサブゴールにする
7.実行仕様をサブゴールにする
「作成手順」＜C＞
1.オブジェクトのディペンダビリティケースを作成
2.メッセージのディペンダビリティケースを作成
3.実行仕様のディペンダビリティケースを作成
4.実行順序のディペンダビリティケースを作成

作成法に対する実験は問答の形式を出る.実験の内容には、次の三つの部分がある.（1）作成手順を紹介する.（2）作成手順を応じて、提供する順序によってディペンダビリティケースを作成することについての質問に回答する.（3）実験についての質問に回答する.

二つ目の作成手順には6個のステップがある.(前提：提供するシーケンス図は単純なシーケンス図に分解した、例は付表Aに示した)

Step1:

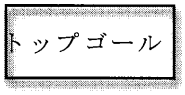


図1トップゴール

質問1：作成手順＜B＞を参考して、トップゴールに何を入れるか？

Step2,3:

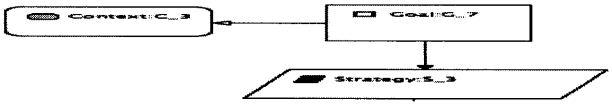


図2　前提と戦略

質問2、3：作成手順＜B＞を参考にすると、前提と戦略は何か？

Step4:

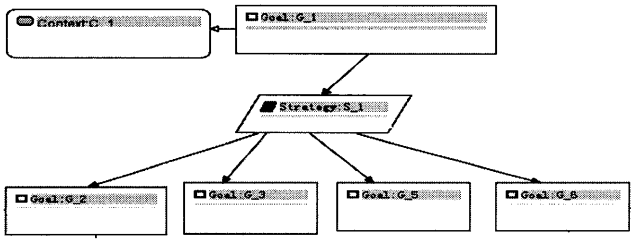


図3　主なディペンダビリティケー

質問4：サブゴールになにを入れるか？

Step4を終わったら、主なディペンダビリティケースの構造を終わり.

Step5:

Step5 からサブゴールについてディペンダビリティケースを作成する.この段階で具体的な例からシーケンス図の要素を抽出して、各要素の検討結果に基づいてStep5を実施する.例は付表Aに示した.

表1対応表

管理員、登録画面、主な画面などがディペンダブルである（a）	サブゴール　（1）
オブジェクトがディペンダブルである（b）	戦略「ストラテジー」（2）
オブジェクト一覧（c） オブジェクトリスク一覧	ゴール（3）
各オブジェクトを（d）	前提（コンテクスト）（4）

質問5：表の左右の内容が対応するローマ字と数字を組み合わせる

メッセージ、実行仕様、実行順序も同じやり方で作業する.

Step6. サブゴールにエビデンスを付ける

1.オブジェクト

オブジェクトの要件定義の資料を参照して、リスクへの対策を作成する

2.メッセージ

メッセージのリスクの対策とシナリオ

3.実行順序

実行順序とシステムのシナリオの経路が一致することとリスクへの対策

3.2 実験結果と作成法の改善

山本研究室の3人を被験者として、この実験を実施した.この実験結果から二つ目の質問に対する答えを集計した結果を表に示す.

表2　実験結果

質問集	参加者ア	参加者イ	参加者ウ
質問1	社員基本情報管理システムのシーケンス図はディペンダブルである	システムのシーケンス図はディペンダブルである	社員基本情報管理システムのシーケンス図はディペンダブルである
質問2	リスク一覧	リスク一覧 シーケンス図	シーケンス図
質問3	シーケンス図の各要素について議論する	シーケンス図の各要素について分解する	シーケンス図の各要素について議論する
質問4	各要素がディペンダブルである	各要素がディペンダブルである	各要素がディペンダブルである
質問5	正解	正解	正解

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

最後に、この実験についてのアンケートを実施した.アンケート結果から、被験者はこの作成法を利用するとシーケンス図に基づくディペンダビリティケースを作成することができることを確認した.しかし、被験者から、作成手順が若干複雑であるため、修正が必要であると指摘された.このため筆者らは被験者の意見を参考にして、実験結果を分析して後、作成法をより理解しやすくする改善を実施した.

改善した作成手順は以下のようである：

(1) シーケンス図が複雑である場合、ディペンダビリティケースを記述する前に簡単にする

結合フラグメント：結合フラグメントの種類によって単純なシーケンス図に分解

(2)シーケンス図に対する主張をトップゴールに記述

(3)主張に対しての前提条件をコンテクストに記述

(4)ストラテジーを記述してシーケンス図の各要素について議論

(5) サブゴールをストラテジーの下に記述

オブジェクト、メッセージ、実行順序、実行仕様

(6) 必要があれば、サブゴール以下で (3) から (5) を反復

(7) サブゴールの下で根拠をエビデンスに記述

4. HAZOP を UML に応用

4.1 UML と HAZOP

HAZOP は,これもではハードウェアを主軸として用いられてきた手法,ソフトウェア開発において応用した研究が幾つか報告されている.例えば、ガイドワードを利用し、UMLのモデルの構成要素についてのリスク識別・分析を行っている[12]. UMLを用いてシステムの開発プロセスに、HAZOPを応用してリスク管理することができる.本稿はディペンダビリティケースの作成するため、UMLモデル中のシーケンス図にHAZOPを用いてリスク項目管理の設計を提出する.[14]

4.2 リスク項目管理の設計

リスク管理では、「リスク識別」、「リスク分析」、「リスク軽減」「リスク対策」を実施する.[14]

リスク識別とは,想定されるリスクを可能な限り抽出し,各ステークホルダの合意を得ることである.

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する.

リスク対策では、設計対応やレビュウ・テストでの確認などのリスク軽減措置を実施する.

シーケンス図でリスク管理するために、シーケンス図の要素を整理する必要がある.たとえば、表3に示すようなシーケンス図で記述する要素の属性に対しHAZOPを応用することができる.具体的には、表3の属性とガイドワードを組み合わせてリスク項目にすることにより、リスク抽出と、検討を進める.

表３　シーケンス図要素の属性

要素	属性
オブジェクト	権限、職能
メッセージ	順序、動作

以下では付録Aで提供するシーケンス図を利用して説明する.このシーケンス図のオブジェクト属性「管理員の登録権限」に対して、ガイドワード「なし」と組み合わせると「管理員の登録権限がない」というリスクが考えられる.したがって、「なし」のようなガイドワードと「管理員の登録権限」と組み合わせろことでリスク項目を構成することができる.このように考えることで、次のシーケンス図要素の属性に対するリスク項目の抽出公式を得る.

[リスク項目抽出公式]

「要素属性」＋「ガイドワード」＝「リスク項目」

[例]

「管理員の登録権」＋「なし」＝「管理員の登録権限がない」

本稿ではこのリスク項目抽出公式を利用して、シーケンス図の要素属性に対するリスク管理を実施する.

4.3 公式を応用する手順

シーケンス図でこの公式を利用してリスク管理をするために、次の手順を用いる.

手順１：要素属性の選定

手順２：リスク項目の設計

手順３：リスク項目の対策

手順１では、リスク項目の設計の対象とする要素属性を選定する.リスク項目はガイドワードの数によって、多く時間がかかる可能性がある.したがって、シーケンス図の全体の要素属性ではなく、信頼性優先度の必要性が高い属性を選定する.手順２では、公式を示すことのように、選定される要素属性とガイドワードを組み合わせてリスク項目表を作成する.手順３では、リスク項目表に対して対策の作成を進める.

この三つの手順を利用して、具体的な例に応用することを考える.ここで、社員情報管理システムに対するシーケンス図の要素属性に対するリスク項目を抽出する.

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

ここでは管理者の権限、登録画面の検証応答、社員の情報増加の順序を選んで説明する.

表4　リスク項目

		要素属性		
		管理者登録権限	登録画面検証応答	社員情報増加順序
ガイドワード	ない	権限がない	登録できない	
	遅い		応答が遅い	
	抜かす			表示しない

表5　リスク項目の対策

リスク項目	対策
管理者登録権限がない	管理者の登録権限を検査して、登録権限を付与する
登録画面検証応答が遅い	登録検証の処理を修正する
社員情報増加順序が示されない	シーケンス図にこの順序を追加する

以上でシーケンス図の要素属性のリスク管理が完成した.この結果はシーケンス図に基づいて作成するディペンダビリティケースのコンテクストとエビデンスとして利用する.

5. 作成法の適用性を評価

前回の論文では名古屋大学の物品購入の手続きを基として物品購入シーケンス図を作成した.物品購入シーケンス図に基づいて、提供するディペンダビリティケースの作成手順に従って、このシーケンス図を対象としてのディペンダビリティケースを作成した.この結果、提案した作成法の有効性を確認した.しかし、作成法の適用性を確認するためには、この物品購入シーケンス図だけの評価では不十分である.

本稿では被験者実験を通じて作成法の適用性を検討した.この実験では、人的資源管理システムの設計段階で作られている社員基本情報管理シーケンス図を用いて作成法の適用性を検討した.

実験では質問回答形式で評価した.この被験者の回答を統計する表を見ると、回答間の差異が小さいことがわかる.また、この実験の結果として回答したディペンダビリティケースに対して、HAZOP を応用することにより、シーケンス図のリスクを分析してリスク項目とリスク対策ドキュメントをディペンダビリティケースに添加することができる.このようにして、完全性の高いディペンダビリティケースを作成することができる.第3章で提案した改善されたディペンダビリティケース作成手順は前回の作成手順と比べてより洗練されていると考えられる.

6. まとめと今後の課題

本稿では、筆者らが提案しているシーケンス図に基づくディペンダビリティケースの適用性を実験的に評価した.この結果、被験者による適用上の差異が小さいことが判明した.一方、リスク分析の方法に対する支援が必要であることが明らかになった.このため、HAZOP を用いたリスク分析手法をシーケンス図に応用することによって改善手法を提案した.さらに、社員情報管理システムに、改善手法を適用することによって有用性を確認した.

今後は、本稿で提案した手法を定量的に評価していく予定である.

文　献

[1] ISSRE 2013,The 3rd International Workshop on Open Systems Dependability: Adaptation to Changing World, http://www.ubicg.ynu.ac.jp/wosd/wosd2013/index.html

[2] 松野裕, 高井利憲,山本修一郎, D-Case 入門～ディペンダビリティ・ケースをかいてもよう！～. 株式会社ダイテックホールディング,2012.ISBN978-4-86293-079-8.

[3] Yutaka Matsuno and Shuichiro Yamamoto. Consensus building and in-operation assurance for service dependability. In Proc. of CD-ARES, LNCS 7465, pages 639–653. Springer, 2012.

[4] Yutaka Matsuno, Jin Nakazawa, Makoto Takeyama, Midori Sugaya, and Yutaka Ishikawa. Toward a language for communication among stakeholders. In Proc. of the 16th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC'10), pages 93–100, 2010.

[5] Object-oriented systems analysis and design usigng UML, Bennett S, pp.21-50

[6] 山本修一郎, 松野裕, ディペンダビリティケース作成法に関する一考察, KBSE 研究会, IEICE-112, vol. IEICE-SS-164, No. IEICE-KBSE-165, pp.61-66, 2012

[7] 松野 裕, 高井利憲, ヴァイセ パテゥー, 山本修一郎, アシュアランスケース構築法の提案, KBSE 研究会, 2012

[8] 山本修一郎, 松野裕, ユースケース分析に基づくディペンダビリティケース作成法の提案, KBSE 研究会,信学技報, vol. 112, no. 419, KBSE2012-61, pp. 19-24, 2013 年 1 月

[9] Vaise Patu, Yutaka Matsuno, Shuichiro Yamamoto, Application of D-Case to the usage flow diagram scenario of the Distributed E-Learning System called KISSEL in Asian Pacific Universities, KBSE 研究会, 2012

[10] 丁峰、山本修一郎、シーケンス図に基づくディペ

NII-Electronic Library Service

Institute of Electronics, Information, and Communication Engineers

ンダビリティケース作成法の研究，学技報，vol. 113, no. 71, KBSE2013-2, pp. 7-12, 2013

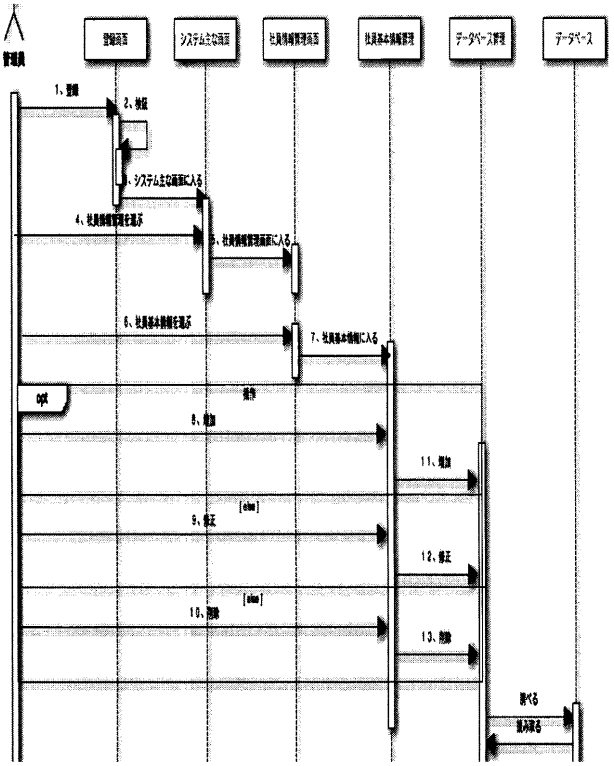
[11]河野 哲也，ソフトウェア要求仕様における HAZOP を応用したリスク項目設計法，ソフトウェアテストシンポジウム 2012

[12]Klaus Marius Hansen, Lisa Wells, Thomas Maier, HAZOP Analysis of UML-Based Software Architecture Descriptions of Safety-Critical Systems

[13]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.

[14]澤部直太，プロジェクト遂行に関する様々なリスクとは何かを理解し、リスク計画について学ぶ http://www.tuat.ac.jp/~asiaprog/courses/project/lesson10/

付録 A



付図　1 社員基本情報管理シーケンス図

社員情報管理のプロセス

1 人力資源管理者はシステムをログインする

2 検証する後システムの主な画面に入る

3 人力資源管理メニューのウプションを選ぶ

4 システムはメニュー明細を提供する

5 人力資源管理員はメニュー明細の中の「社員基本情報」を選ぶ

6 システムは社員基本情報の画面を送る

7 この画面で人力資源管理員は増加、添削などの操作を行う

8 操作をデータベースに保存する

NII-Electronic Library Service