

信頼性分析による品質確保の取り組み —重要度の高い故障要因洗い出し、QFD、FTA の導入と実績—

田中 桂三

オムロン株式会社 オートメーション統轄事業部 ソフトウェア開発部 第2開発課
〒525-0035 滋賀県草津市西草津2丁目2-1

E-mail: keizo_tanaka@omron.co.jp

あらまし ソフトウェア開発において、重要度の高い故障の流出防止のために、「信頼性分析」を導入し QFD、FTA を活用したテスト設計プロセスを定義、導入した。本論文では、この一連のプロセス、効果について報告する。

キーワード 品質確保, 信頼性分析, QFD(Quality Function Deployment), FTA(Fault Tree Analysis), JIS-Z8115(2000), 信頼性, 故障

Quality Assurance activity by Reliability Analysis —Coverage of causes about high level failures by manipulating QFD and FTA—

Abstract In order to prevent high level failures from occurring in the market, we introduced Reliability Analysis by manipulating QFD and FTA and defined our Test designing process. I report this process and the effectiveness..

Keyword Quality Assurance, Reliability Analysis, QFD(Quality Function Deployment), FTA(Fault Tree Analysis), JIS-Z8115(2000), Dependability, failure

1. まえがき

ソフトウェア製品を開発するメーカーとしての責務として、お客様に安心して使っていただけるソフトウェア製品を提供するために、特に重要度の高い故障の市場への流出を防止する必要がある。このために、JIS-Z8115(2000)で、Dependability (信頼性) が制定されている。これは重要度の高い故障防止の観点となる、信頼性用語とその定義がされている。しかしながら、実際の信頼性の確保のプロセスは様々である。また、JIS-Z8115(2000)で推奨されている手法として FTA (Fault Tree Analysis)があるが、ソフトウェアの場合、すべての FTA を実施することはコストから考えて非常に難しい。さらに信頼性分析の手法として QFD (Quality Function Deployment) が幅広く使われているものの、製品の品質特性の定義に人ごとのばらつきが出やすい。

そこで、重要度の高い故障の流出を防止するために、弊社で確立しているソフトウェア開発プロセスに加えて、信頼性分析に QFD、FTA を導入したテスト設計プロセスを定義し、弊社ソフトウェア開発プロジェクトで実践した。

2. 課題・狙い

弊社の某ソフトウェア開発プロジェクトにおいて、重要度の高い故障の流出防止のために、「信頼性分析」を導入し QFD、FTA を活用したテスト設計プロセスを定義、弊社ソフトウェア開発プロジェクトで実践した。本プロセスの流れとして、以下の手順で実施した。

2.1 重要度の高い故障流出防止要件の抽出

重要度の高い故障の流出防止要件の洗い出しのために、QFD を採用した。その際重要度の高い故障の選定に人ごとのばらつきをなくす目的で客観的指標を取り入れるため、QFD の品質要求項目として、「JIS-Z8115(2000)」出典の「Dependability (安心・信頼)」を活用した。

2.2. 少ない工数での FTA の導入

すべての故障発生要件において、FTA を実施することは工数的に現実的ではない。そのため、QFD 中から最も重要度の高く、かつ QFD では深堀りの足りない品質要求項目について FTA を実施した。

2.3. テスト設計プロセスの定義

2.1、2.2 を活用したテスト設計プロセスを定義し、評価を実施した。

3. 課題達成のための具体的な手段

3.1 重要度が高い故障流出防止要件の抽出

(1) 重要度が高い故障流出防止要件の洗い出し

重要度の高い故障の選定に人ごとのばらつきをなくす目的で客観的指標を取り入れるため、「JIS-Z8115(2000)」出典の「Dependability (安心・信頼)」の用語の意味に該当する某ソフトウェア製品の重要度が高い故障の発生要件を洗い出した。その際、ソフトウェア製品の過去の市場で発生した故障情報も参照した。

JIS要件	某ソフトウェア重要流出防止要件	JIS要件	某ソフトウェア重要流出防止要件
完全性	種別エラー発生防止要件	可用性	ソフトウェアの一般稼働防止要件
	異常終了によるデータの破損防止要件		異常終了によるデータの破損防止要件
	異常終了によるデータの破損防止要件	信頼性	信頼性の低下防止要件
	ソフトウェアの更新時のデータ破損防止要件		信頼性の低下防止要件
	ソフトウェアの更新時のデータ破損防止要件		信頼性の低下防止要件
	ソフトウェアの更新時のデータ破損防止要件		信頼性の低下防止要件
保水性	種別エラー発生防止要件		信頼性の低下防止要件
	異常終了によるデータの破損防止要件		信頼性の低下防止要件
	ソフトウェアの更新時のデータ破損防止要件		信頼性の低下防止要件

図 1. 「JIS-Z8115(2000)」出典の「Dependability (安心・信頼)」に該当するソフトウェア製品の重要度が高い故障流出防止要件

(2) QFD の導入

弊社の某ソフトウェア開発プロジェクトでは、重要度が高い故障の抽出の手法として、QFD (品質機能展開) を導入した。以下に作成方法を説明する。

① 軸 (重要度が高い故障の流出を防止するための品質要求項目) の抽出方法と最適なレベル設定

- ・具体的な事象を、ソフトウェア製品の過去の市場で発生した故障情報から洗い出し
- ・以下の 3 階層で実施。
- ・最上位 (4 項目): 「JIS-Z8115(2000)」の「Dependability (安心・信頼)」の要件
- ・2階層目 (22 項目): 最上位の要件に該当する某ソフトウェア製品の重要度が高い故障 (不具合) の要件
- ・3階層目 (最下層 65 項目): 2階層目の故障 (不具合) を引き起こす外部・内部的要因。これが設計・評価で押さえるべきアクションとなる。

・再下層 65 項目については、設計 (ホワイトボックス)・評価 (ブラックボックス) の両面で品質要求項目を挙げた。いずれも第三者でも内容が理解できるよう、構造設計・コードレビューチェックリストの記載レベルに合わせた。

② 軸: 弊社の某ソフトウェアの機能

- ・機能毎に設計・テスト担当者が特定できるような機能一覧を作成。



図 2. 某ソフトウェア製品の QFD(Quality Function Deployment)

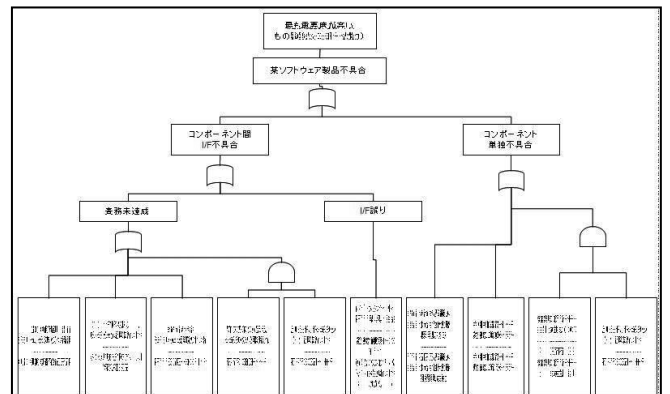
3.2 少ない工数での FTA の実施

品質特性のうち最も重要度が高い要件で、かつ QFD で展開した品質要求項目の粒度では不足しており、さらに、深掘りが必要なものについて、FTA を導入。FTA 対象の選定と FTA 作成の際、内部設計に精通している設計キーマンからの情報と過去の故障情報を元に実施した。

ツリー展開方法は以下の通り。

- ・最上位: 品質特性のうち最も重要度が高い要件
- ・2階層目: 複数機能 (コンポーネント) 単独での故障、複数機能間の I/F で分類
- ・3階層目: 複数機能間の I/F において、「責務未達成」「I/F 誤り」で分類
- ・4階層目 (最下層): 2、3階層目の故障 (不具合) を引き起こす外部・内部的要因。これが設計・評価で押さえるべきアクションとなる。

図 3. 某ソフトウェア製品の FTA (Fault Tree Analysis)



3.3 テスト設計プロセスの定義と実施

テスト設計プロセスの中で 3.1、3.2 の OUTPUT を活用し、検証すべき項目を明確にして評価を実施した。またホワイトボックスで実施すべき項目については設計側に実施を依頼し、実施結果を確認した。

- (1) QFD (品質機能展開) でのカバレッジ 100%実施方法

①縦軸（各品質要求項目）と横軸（各機能）の表中で、該当箇所には○を付け、カバレッジすべき箇所を明確にした。

②縦軸（各品質要求項目）に、「分類」列を設け、「設計（実装）」または「評価（テスト）」を記載。これにより、設計で押さえるべき項目なのか、あるいは評価で押さえる項目を明確にした。

図 4. QFD でのカバレッジ 100%実施方法

(2)FTA でのカバレッジ 100%実施方法

最下層の各要因を、設計（実装）で押さえるべき項目なのか、あるいは評価（テスト）で押さえる項目を明確にした。

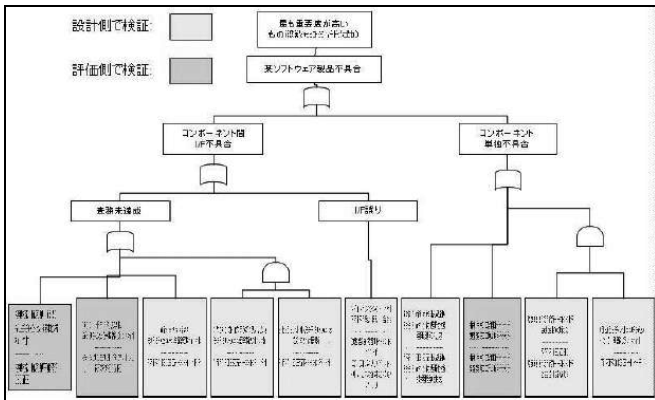


図 5. FTA でのカバレッジ 100%実施方法

4. 信頼性分析プロセス導入の効果

弊社ソフトウェア開発プロジェクトにおいて、本テスト設計プロセスを導入した結果、QFD の品質要求項目として、「JIS-Z8115(2000)」出典の「Dependability（安心・信頼）」を活用することで、製品の品質特性定義のばらつきを防ぐことができた。これにより、QFD での重要度の高い故障の検出が向上した。また、FTA 導入により、設計（ブラックボックス）、評価（ホワイトボックス）両面で確認することで、最も重要度の高い故障の発生要因を開発プロジェクト実施中に検出した。

これらの効果により、本ソフトウェアをご利用頂いたお客様のシステムに影響を及ぼすような重要度の高い故障の発生を防止することができた。

5. 課題・今後の展開

5.1 課題

テスト設計プロセスの中での、FTA 対象の選定と FTA の作成の際、内部設計に精通した設計キーマンの情報を元を実施した。その際、設計キーマンから必要な情報を収集するのに時間を費やした。

5.2.課題の原因と今後の展開

課題の原因としては、設計キーマンの繁忙により、信頼性分析の実施者との時間が合わなかったためである。今後の展開として、設計キーマンから効率よく情報を収集するために、あらかじめ明確に実施のタイミングを定義しておく、設計キーマンの時間を確保しておくことが必要である。そのために、FTA の最適な実施タイミングを検討し、テスト設計プロセス手順の中で明確に定義し、今後のソフトウェア開発プロジェクトで実践していく。

文 献

- [1] Dependability (JIS Z 8115:2000) 信頼性用語
- [2] QFD（品質機能展開）の概説 玉川大学工学部経営工学科助教授 大藤正 氏 2000 年 1 月
- [3] 国際標準化時代の実践 FTA 手法 小野寺勝重 氏 日科技連出版社 2000 年 6 月