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
KBSE2011-26(2011-09)

故障分析票の最簡形について

芳川 大佑† 山本 修一郎‡

†‡名古屋大学工学部 〒464-0814 愛知県名古屋市千種区不老町

E-mail: †yoshikawa.daisuke@a.mbox.nagoya-u.ac.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

あらまし ソフトウェアの故障を分析する FMEA 技法では故障分析票を網羅的に作るため故障分析票の作成量が増大するという問題があった．このため故障分析票の構成要素間の関係に基づいて作成量を削減する技法を提案するとともに，適用事例を紹介する．

キーワード ソフトウェア FMEA，プロセス記述票，状態遷移図，リスク分析表，故障分析票

On a reduced form of software Failure Analysis Table

Daisuke YOSHIKAWA† and Shuichiroh YAMAMOTO‡

†‡Nagoya University Hurou-tyo, Tikusa-ku, Nagoya-si,Aiti, 464-0814 Japan

E-mail: †yoshikawa.daisuke@a.mbox.nagoya-u.ac.jp, ‡yamamotosui@icts.nagoya-u.ac.jp

Abstract FMEA method has the problem that volume of describing Failure Analysis Table is increasing. In this paper, we propose a method to reduce the number of Failure Analysis Tables based on equivalence relationship.

Keyword Software FMEA, Process description, State transition diagram, Risk Analysis table, Failure analysis table

1. はじめに

ソフトウェアの故障を分析する FMEA 技法では故障分析票を網羅的に作るため故障分析票の作成量が増大するという問題があった．このため故障分析票の構成要素間の関係に基づいて作成量を削減する技法を提案するとともに，適用事例を紹介する．

以下では，まず 2 節で筆者らが提案しているソフトウェア FMEA 分析法[3]について説明する．次に 3 節で，ソフトウェア FMEA 分析法を適用実験する対象システムについて述べる．4 節で適用結果を明らかにする．5 節でこの結果に基づいて故障定義票の簡約可能性について議論する．6 節では簡約方法，簡約方法の特徴，限界について考察する．7 節では関連研究について述べる．最後に 8 節で今後の課題をまとめる．

2. ソフトウェア FMEA 分析法の提案

プロセス記述票を用いたソフトウェア FMEA 分析法を提案する．すなわち以下の手順でソフトウェア FMEA 分析を実施する．

(1) システムコンテクストの定義
システムコンテクトを入力・システム・出力を明確にして、図で記述する．

(2) 状態遷移に基づくシステムの振る舞いの定義
システムの状態に基づいてシステムの処理を振る舞いにより定義する．

(3) 故障の定義
プロセス記述票をもとにイベント、データ、コンポーネント、処理について故障を考える．
プロセス記述票をもとにイベント、データ、コンポーネント、処理について故障を考える．記述する項目として下記の 5 点を考え故障分析票にまとめる．

① 対象
故障の対象となるものを記す．プロセス記述票から項目を取り出していくことになる．

② 故障の型
故障対象にはイベント故障，データ故障，コンポーネント故障，処理故障が考えられる．イベント故障には不正終了・脱落・不正推移・タイミングミスの 4 つがある．データ故障にはデータ欠如・不正データ・データタイミングミス・データ重複の 4 つがある．コンポーネント故障には物理故障とソフトウェア故障がある．処理故障には状態遷移条件誤りがある．

③ 説明
故障がどのようなものかを説明する．

④ 影響
故障がシステムにどのように作用するの

か記述する.

⑤ 対策

定義された故障について対策を考える.

対象	故障型
故障の対象となるものを記す	対象を4種類に分類し，その中での故障の型を記す
説明	**影響**
故障がどのようなものかを説明する	故障がシステムにどのように作用するのか記述する
対策	
定義された故障について対策を考える	

図 1，故障分析票

3. 適用対象

本提案の適用対象である話題沸騰ポット（GOMA-1015 型）[4]について説明する．このポットの仕様書は組込みソフトウェア管理者・技術者育成研究会（SESSAME）が作成したものである．本ポットは操作パネルにある沸騰ボタンを押すことで中の水を沸騰させ所定の３つの温度（98℃，90℃，60℃）に保温することができる．ポッドにはロックボタンがありロック中は給水をすることはできない．ポット内に水位センサが 4 つ付いており蓋を閉めた時に自動で中の水の量を感知し操作パネルに表示する．またポットにはタイマの機能を持っており，指定の時間（1～60 分，1 分刻み）後にブザーを鳴らすことができる．

センサ，アクチュエータ，ポットの関係を図 2 に示す．

表 1 では図 2 の 10 個のセンサについて説明する．ただし水センサはまとめて 1 つにしている．表 2 では図 2 の 9 個のアクチュエータについて説明している．

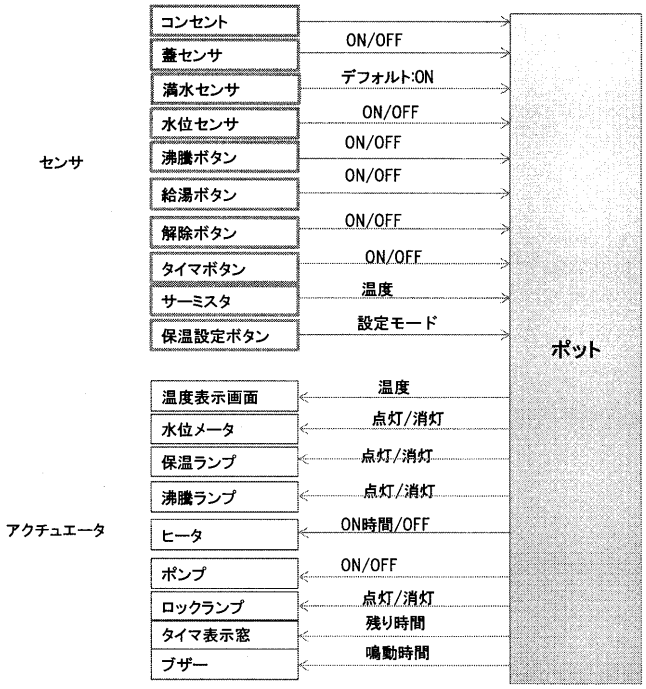

図 2 センサ・アクチュエータ・ポット相関図

表 1，センサ表

センサ	機能
コンセント	コンセントをつなぐと電力が供給状態になる
蓋センサ	蓋が閉じているかを検出
満水センサ	水位が，このポットの許容上限を超えているかを検出
水位センサ	水位を検出
保温設定ボタン	3種類の保温温度を設定
沸騰ボタン	沸騰行為をさせる
給水ボタン	給水口から給湯
解除ボタン	給湯に対するロック/ロック解除機能の設定
タイマボタン	時間を分でセットし，タイマを起動
サーミスタ	ポット内の水温を検出

表 2，アクチュエータ表

アクチュエータ	機能
温度表示画面	温度・設定モードを表示
水位メータ	水位センサと同数のインジケータセルと呼ばれるランプで表示
保温ランプ	保温状態を点灯
沸騰ランプ	沸騰状態を点灯
ヒータ	ポット内の水を加熱
ポンプ	ポット内の水を吸い上げて，給湯口から排出
ロックランプ	ロック状態を点灯
タイマ表示窓	タイマ残り時間を表示
ブザー	ブザーを鳴らす

4. 故障定義票のポット適用

ポットの例題で故障定義票を作成する．ポット図1のようにセンサ，アクチュエータ，制御システムの3つに分類することができる．

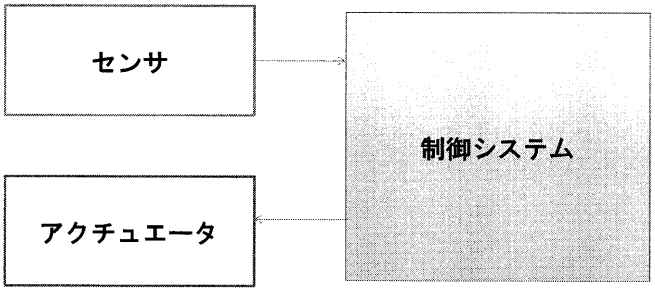

図3，センサ・アクチュエータ相関図

センサはシステム外部のデータを感知し制御システムに送り，制御システムはセンサから送られたデータをもとに動作を決定し，アクチュエータに信号を送る．アクチュエータは制御システムからの信号をもとに動作をする．

4.1. センサ

センサとはポットの制御システムにデータを送るシステムと定義する．ポットにはセンサはコンセント，蓋センサ，満水センサ，水位センサ（4個），沸騰ボタン，保温設定ボタン，給水ボタン，解除ボタン，タイマボタン，サーミスタ（温度測定）の計13個付いている．この中で水位センサを例として故障定義票を作成すると図3のようになる．

対象	故障型
水位センサ（コンポーネント）	物理故障
説明	影響
センサが物理的に故障する	センサ接続先に信号が正しく伝達できない
対策	
センサの点検	

図3，　水位センサ故障定義票

センサごとに1枚の故障定義票を作成した．故障定義票の記述項目のうち同じものは対象・故障型・説明・対策だった．定義票の記述項目で異なる内容は影響だけだった．ここではセンサにはソフトウェアが含まれていないので，対策は点検することとした，このため故障定義票の対策はすべて同じ記述になった．

4.2. アクチュエータ

アクチュエータはポットの制御システムから信号を受け取るシステムであると定義する．ポットには温度表示画面，水位メータ，保温ランプ，沸騰ランプ，ヒータ，ポンプ，ロックランプ，タイマ表示窓，ブザーの計9個のアクチュエータがある．このうち水位メータを例に故障定義票を図4のように作成した．

アクチュエータごとに1枚の故障定義票を作成した．故障定義票の記述項目のうち同じものは対象・故障型・説明・対策だった．定義票の記述項目で異なる内容は影響だけだった．

対象	故障型
水位メータ（コンポーネント）	物理故障
説明	影響
水位メータが物理的に故障する	接続元からの信号が正しく受信できない
対策	
アクチュエータを点検する	

図4，水位メータ故障定義票

5. 故障定義票の簡約可能性

故障分析票は網羅的に作成することになるので作成量が多くなるという課題がある．これに対処するためには簡約できることを定め作成量を少なくすることを考える．

5.1. 簡約できること

図2，3を見てもわかるようにコンポーネントの故障の場合，対象にかかわらずセンサの場合は制御システムに信号を送ることができなくなり，アクチュエータの場合には制御システムの信号を受信できなくなるとなることが分かる．

5.2. 簡約できないこと

コンポーネントが物理故障した場合そのコン

ポーネントがシステムに対しどのように組み込まれているかでシステムに与える影響度は変わってくる．システムに与える影響度は対象が変わると変わってくるので簡約することができない．

6. 考察

6.1. 簡約方法

これまでの方法では，故障定義票をセンサ・アクチュエータごとに定義し，個別に影響を定義していたこのため， センサｎ，アクチュエータｍに対して故障定義票の記述量は次のようになる．

センサの故障定義票：ｎ枚

アクチュエータの故障定義票：ｍ枚

これに対してセンサ全体で1枚の故障定義表を作成し，センサリストを作成する，またアクチュエータ全体で1枚の故障定義表を作成し，アクチュエータリストを作成する，またセンサとアクチュエータごとに異なる影響があるのでこれについてはリスク分析表を作成してセンサとアクチュエータごとに影響を一覧表で記述する．

この時，新しい簡約方法ではセンサｎ，アクチュエータｍに対して故障定義票の記述量は次のようになる．

センサの故障定義票：1枚

アクチュエータの故障定義票：1枚

センサリスト：1

アクチュエータリスト：1

リスク分析表：1

ここで簡約できない影響部分だけ取り除きリストにしそうでない部分はリスト・アクチュエータ各1枚の故障定義票にする．

リスク分析表の例を表3に示す．

表3，リスク分析表の例

コンポーネント名	種別	故障型	影響	頻度	システムでの対策
水位センサ	S	物理	中	低	下位の水位センサがOFFのとき上位の水位センサがONでないことを確認する
ヒータ	A	物理	大	低	動作信号に対して正常に反応していないことを確認する

リスク分析表では，コンポーネント名，センサ・アクチュエータ種別，故障型，影響，頻度，システムによる対策を記述する．たとえば表3では水位センサの種別がセンサ(S)，故障型は物理故障，影響は中，発生頻度は低，システムによる対策は下位の水位センサが OFF のとき上位の水位センサが ON でないことを確認するというものである．

6.2. 簡約方法の特徴

従来方法では利点としてコンポーネントごとに故障型，説明，影響，対策をまとめて一覧できることがあげられる．これに対して欠点としてコンポーネント全体では影響を一覧比較できないことや故障型，説明，対策で同じ記述が重複することなどがある．

6.1 で提案した簡約方法では利点としてコンポーネント全体で影響を一覧できることや故障定義票の作成量が少なくなることがあげられる．欠点としてはコンポーネントごとに故障型，説明，影響，対策をまとめて一覧できないことがある．

6.3. 限界

本方法ではコンポーネント故障しか考えておらず故障定義票の量が多くなるイベント故障，タイミング故障には使用できない．故障定義票を実際のシステムで扱うにはさらなる簡約方法が必要である．

6.4. ヒータとサーミスタの故障

サーミスタ故障の影響として，ヒータで過度に加熱してしまうリスクがある．しかしサーミスタは故障しているため，この場合は異常を検知できない．このように1つのコンポーネントが壊れることにより違うコンポーネントが正常でない動きをする複合コンポーネント間の故障の影響に関してどのよう分析するか検討する必要がある．

一方，ヒータにおいて OFF 信号を ON 信号と誤認識する故障が発生したとする．このとき，サーミスタが正常に異常温度を検知しても，ヒータに OFF 信号を送っても ON 信号と誤認識するので温度異常の状態が継続することになる．

前者は，最初のコンポーネント故障による影響の例である．後者は正常なコンポーネントで検知した異常を次のコンポーネントで制御しようとした際に，コンポーネントが故障したために発生する故障の例になっている．

このように，複数のコンポーネント間で発生する故障の影響について検討する必要がある．しかし，本稿では，この点について議論していない．

7. 関連研究

7.1. 高安全プロセスの研究

ソフトウェア高安全性開発プロセスの研究には，は安全性知識体系として①運用環境分析②システム分析③リスク識別④リスク分析⑤安全性評価確認⑥知識管理の 6 個の知識領域がある[yama11].

運用環境分析

システムの運用活動を分析するために，①運用

環境分析②ステークホルダ分析③タスク分析などを実施する.

システム分析

システムの内部構造を分析するために,①システムアーキテクチャ②コンポーネント構成③コネクタ関係④相互作用分析などを実施する.

リスク識別

ハザード,故障モードを抽出し,その妥当性,完全性を確認するために,①抽出準備②抽出活動指揮③抽出結果の文書化④抽出結果確認などを実施する.

リスク分析

リスクに対して,システムと環境への影響,重大性を分析するために,①対象要素定義②判断根拠の分析③影響分析④重大性分析⑤原因分析⑥対策定義などを実施する.

安全性評価確認

リスク対策と安全性要求との適合性を評価,安全性リスクを摘出するために,①リスク対策評価②リスク緩和策割付③組織準備判断④安全性要求判断⑤安全性評価確認などを実施する.

知識管理

システム,環境に対する故障,危険,安全管理知識を管理するために,①故障モード知識②危険要因知識③安全管理知識④安全性知識の追跡性管理などを実施する.

7.2. ソフトウェア FMEA

ソフトウェア FMEA 分析の研究としては故障木分析に類似する後ろ向き分析によって要求分析の課題を識別する方法がとられており,これにより要求分析への適用法が提案されている[2]. しかし Lutz らはイベントとデータしか考慮していない. これに対して本提案では処理とコンポーネントとイベントおよびデータの入出力の区別を扱うことができる.

7.3. プロセス記述票に基づく FMEA 分析法

プロセス記述票を用いた FMEA 分析手法が提案されている[3]. この手法では実際に運用しているシステムに適用した結果,実際に現場でのシステムを開発経験がない分析者でも容易に網羅的な故障分析を実施できることを確認している.

8. まとめ

本稿では,プロセス記述票を用いた FMEA 分析手法に対する簡約化の方法を提案した. 本手法では組み込みシステムの例として話題沸騰ポット[4]適用した結果,故障定義票の量を減らすことができた.

今後,本手法をより多くのシステムに対して適用することにより有効性を評価していく予定である. 本手法の課題としてコンポーネント故障以外の故障についての簡約方法についてと1つの故障が引き起こす複合故障の対策も考える必要がある.

文　献

[1] 山本修一郎,“ソフトウェア高安全性分析技術の現状と課題,”情報処理学会ソフトウェア工学研究会　Vol.2011-SE-172 No.9, 2011.

[2] Robyn R. Lutz and Robert M, Woodhouse Jet Propulsion Laboratory, ”Contributions of SFMEA to Requirements Analysis” . Proceedings of ICRE'96,pp.44-51,1996.

[3] 芳川大佑, 山本修一郎“プロセス記述票に基づくソフトウェア FMEA 技法の提案” 信学技報, vol. 111, no. 169, KBSE2011-12, pp. 13-18, 2011 年 7 月

[4] 特定非営利活動法人組込みソフトウェア管理者・技術者育成研究会(SESSAME)事務局“話題沸騰ポット（GOMA-1015 型）要求仕様書第 7 版”