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
SS2011-15,KBSE2011-12(2011-7)

プロセス記述票に基づくソフトウェアFMEA分析法の提案

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 ソフトウェア機能に関するプロセス記述に基づくFMEA技法を提案するとともに，人感センサ付き信号機の制御機能への適用結果について報告する

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

A Proposal on Software FMEA Method based on Process Descriptions

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 . An FMEA method is proposed based on process descriptions of software functions. We also introduce an application result on the control function of a traffic signal system with human sensor.

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

1. はじめに

近年，ソフトウェア安全性に関心が集まっている．このためプログラムコードに対するソフトウェアFMEA分析手法が提案されている．しかし上流工程におけるソフトウェアFMEA分析手法は必ずしも十分に明確になっていなかった．このため本稿ではプロセス記述票に基づいてソフトウェアの機能定義を対象にしたソフトウェアFMEA分析手法を提案する．

本稿の構成は以下の通りである．まず次節でプロセス記述票を説明する．次に3節で本稿が対象とする信号機の例題に対するプロセス記述票の具体例について述べる．4節ではソフトウェアFMEA分析法を提案する．5節ではソフトウェアFMEA分析法の具体例を示す．6節で適用結果に基づく考察を述べる．7節で関連研究との関係を明らかにする．最後に8節でまとめと今後の課題を述べる．

2. プロセス記述票

まずプロセス記述票について記述項目と具体的な構成例を示す．

[定義]プロセス記述票

入力・入力イベント・処理・出力・出力イベント・コンポーネントを明確に記述した票をプロセス記述票と呼ぶ．

2.1. 記述項目

記述項目として以下の6つの項目があげられる．

① 入力イベント

システムが、入力処理を実施する契機を記述する．

② 入力

運用手順を実施する際に，必要となる入力情報を記述する．

③ 処理

システムに対して実施すべき運用手順の内容を記述する．

④ コンポーネント

処理手順に関係する関係物を記述する．

⑤ 出力イベント

システムが、入力処理を実施する契機を記述する．

⑥ 出力

処理を実施した結果、処理対象から出力される情報を記述する．

2.2. プロセス記述票の構成例

上述したプロセス記述票は図1のように構成できる．これにより1枚のカード形式でプロセスをわかりやすく記述できる．

入力イベント	処理	出力イベント
入力	**コンポーネント**	**出力**

図 1. プロセス記述票

3. プロセス記述票の具体例

以下では実際にプロセス記述票を用いることにより信号機問題を分析する．まず信号機問題について説明する．

3.1. 信号機問題

事例として、センサ付き信号機を考える．信号機には人センサと車センサがついており、それぞれ対象を感知しているか，していないかを識別できるセンサ情報を制御システムに送る。制御システムは内部に時計を持っており、規定時間が経過したら制御システムにシグナルを送る。時計からのシグナルを受けると制御システムは信号の歩道ライトと車道ライトの赤・青を切り替える。またセンサが人（車）をとらえており車（人）をとらえていない場合、歩道（車道）が青の時に時計からシグナルが来たとしてもこれを無視し青を延長する。したがって制御システムは信号が赤の時に時計からシグナルが来ると信号を青に切り替える．信号機システムの構成図は図 2 のようになる．

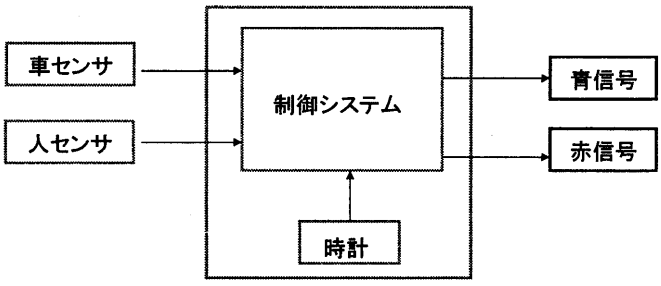

図 2, 信号機システム構成図

3.2. 信号機システムのプロセス記述票

信号機問題を扱ったプロセス記述票を付録 1 と付録 2 に記述する．付録 2 は付録 1 の処理部分である．

入力データは人・車の両センサが制御システムに送る人・車を感知しているか，いないかを示す．入力イベントは時計から送られる一定時刻経過のシグナル受信時と先ほどの入力データの変更時となる．処理は現在状態のデータと次状態の関係をイベントの遷移表で示した．またこの処理表においてセンサデータは感知している対象のみ記述し、感知していない対象は記述していない．コンポーネントは人・車センサ、時計、青信号，赤信号となる．出力は青信号，赤信号となり、出力イベントは信号の切替時となる．

4. ソフトウェア FMEA 分析法の提案

以下では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．

5. ソフトウェア FMEA 分析法の具体例

プロセス記述票を用い信号機問題をソフトウェア FMEA 分析方法で確認する。

(1) システムコンテクト定義

本例題では入力はセンサがとらえた人・車の像となり、システムは信号機制御システム、出力は歩道・車道に対する青・赤のライトの光である．システムコンテクトを図 3 に記す。

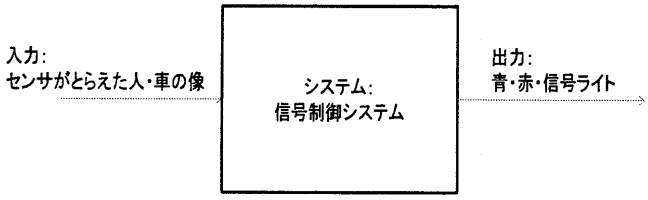

図 3, 信号機システムコンテクト図

(2) 状態遷移に基づくシステムの振る舞いの定義

システムの振る舞いを状態遷移図や状態遷移表で表現する．状態遷移では，現在状態から受理したイベントに対する次状態への遷移を定義する．

本例題ではシステムが保持しているのはセンサから送られる人や車がいるか，いないか，と歩道と車道の信号状態（青か赤か）である．

遷移イベントとしては時計から一定時間の経過のシグナルを受けた時の信号データの交代(T). ただし特定状態では遷移せず同じ状態にとどまる. そのほか現在のセンサデータと異なるセンサデータがセンサから送られたらセンサデータを変更する(C1,C2,H1,H2). ここでC1,C2,H1,H2は次のとおりである.

T:一定時刻経過
H1:人を感知
H2:人の感知がなくなる
C1:車を感知
C2:車の感知がなくなる

このとき信号機システムの状態遷移図は図3のようになる. なおこの状態遷移図は付録2で示した状態遷移表と等価である.

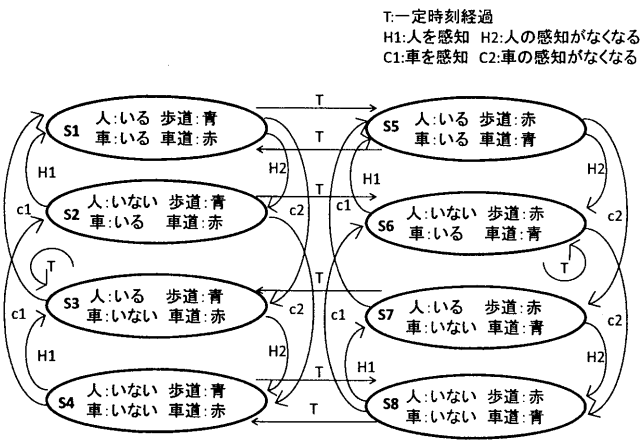

図3, 信号機状態遷移図

(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. 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. たとえば図の4で定義された故障の場合, 定期的にセンサデータをチェックすることで故障のリスクを軽減できると考える.

故障定義の例として信号機に対するセンサデータ故障とその対策を図4で示した.

対象	FM
センサデータ（データ故障）	不正データ
説明	影響
システムが保持するセンサデータが誤ったものである	制御システムが誤った信号命令を信号に送る可能性がある
対策	
定期的にセンサデータをチェックする	

図4, 信号機問題故障分析票例

6. 考察

6.1. 記述容易性

プロセス記述票を用いることで分析する項目があらかじめ定められているので, プロセス記述について分析洩れがない. また故障分析票で故障の型を定めているため熟練者でなくてもこれらを当てはめることにより容易に分析できる.

6.2. 適用上の課題

今回の適用例では, プロセス記述票が1枚. その記述項目数が合計16個である. 内訳は, 入力イベントが7個, 出力イベントが1個, 入力が2個, 出力が2個, コンポーネントが5個, 処理が1個である.

これらの記述項目ごとに故障の型の数だけの故障分析票を作成した. したがって故障分析票全体では下式のとおり54個となる.

7*4+1*4+2*4+2*4+5*1+1*1=54

ここで, コンポーネントはハード故障のみを考えた.

このように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大きくなるという課題がある. これに対処するためには重要度などを考慮して故障分析票の作成量を抑制する必要がある.

6.3. 分析プロセス

今回のソフトウェアFMEA分析で実施したプロセスを以下で説明する.

(1) 概要状態遷移図で問題を理解

まず信号機システムを大まかに理解するために簡単な状態遷移図を書いた.

(2) プロセス記述票の作成

次にプロセス記述票を書くことでシステムのプロセスを正確に定義した.

(3) 状態遷移図を再定義

さらに, 概要を分析した状態遷移図にプロセス記述票で明確にした各情報に基づいて状態遷移図を詳細化しシステム全体の振る舞いを再分析した.

(4) 状態遷移表を定義

状態遷移表を定義することにより状態遷移図の妥当性を確認した.

(5) 故障分析票の作成

これらの情報に基づいて故障分析票を作成した.

上述したことをまとめて図 5 に示す.

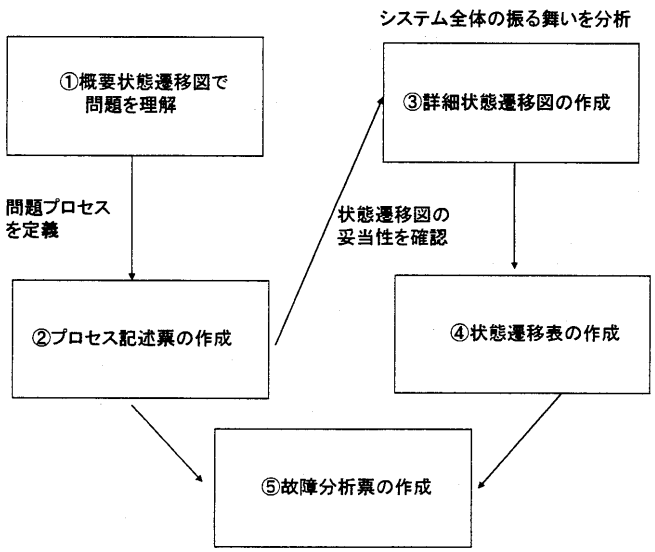

図 5, ソフトウェア FMEA 分析プロセス

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[Lutz96]. 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. 非定常系分析・障害シナリオ分析

非定常系の分析にはシステム内の情報フローをダイアグラムに表現することにより情報変化を可視化し分析することで非定常系シナリオの発生原因とシステムに与える影響を分析し, 非定常系シナリオの欠落を抑止する方法が提案されている[kame06]. またソフトウェア要求仕様定義段階での障害発生可能性を発見する手段として, 分析マトリクスと障害シナリオ分析手法が提案されている[Mise11].

本提案では非定常系シナリオや障害シナリオの発生原因となるプロセスの入出力イベントや入出力データの逸脱を網羅的に分析することができる. したがって非定常系分析や障害シナリオ分析と組み合わせることができる可能性がある.

8. おわりに

本稿では, プロセス記述票を用いた FMEA 分析手法を提案した. さらに, 本手法を実際に運用しているシステムに適用した結果, 故障の可能性と対策の必要性を確認することができた. 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た.

今後，本手法の適用結果についてさらに複雑なシステムへの適用を考えている．また本手法での課題として故障分析票の数の抑制や，故障への対策がほかのプロセスに影響する可能性がないことを確認することなどがあげられる．

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] 亀谷秀洋，新屋敷泰史，三瀬敏郎，橋本正明，鵜林尚靖，片峯恵一，中谷多哉子，“情報フロー・ダイアグラムによる組込みソフトウェア非正常系の分析手法” 電子情報通信学会技術研究報告. SS，ソフトウェアサイエンス 105(596), 1-6, 2006.

[4] 三瀬敏郎，新屋敷泰史，片峯恵一，橋本正明，中谷多哉子，鵜林尚靖，“非正常系現象に着目した組込みシステムの障害シナリオ分析手法” 電子情報通信学会技術研究報告 110(468), 19-24, 2011.

付録 1

<table>
<tr><th>入力イベント</th><th>処理</th><th>出力イベント</th></tr>
<tr><td>人を感知/
感知しなくなる</td><td rowspan="3">※</td><td rowspan="3">信号の切替</td></tr>
<tr><td>車を感知/
感知しなくなる</td></tr>
<tr><td>一定時間の経過</td></tr>
<tr><th>入力</th><th>コンポーネント</th><th>出力</th></tr>
<tr><td rowspan="2">人センサ</td><td>人センサ</td><td rowspan="2">歩道：青　車道：赤</td></tr>
<tr><td>車センサ</td></tr>
<tr><td rowspan="3">車センサ</td><td>時計</td><td rowspan="3">歩道：赤　車道：青</td></tr>
<tr><td>青信号</td></tr>
<tr><td>赤信号</td></tr>
</table>

付録 1，信号機プロセス記述票 1

付録 2

		次状態							
		人:いる 車:いる 歩道:青 車道:赤	車:いる 歩道:青 車道:赤	人:いる 歩道:青 車道:赤	歩道:青 車道:赤	人:いる 車:いる 歩道:赤 車道:青	車:いる 歩道:赤 車道:青	人:いる 歩道:赤 車道:青	歩道:赤 車道:青
現状態	人:いる 車:いる 歩道:青 車道:赤		人の感知 がなくなる	車の感知 がなくなる		一定時刻 経過			
	車:いる 歩道:青 車道:赤	人を感知			車の感知 がなくなる		一定時刻 経過		
	人:いる 歩道:青 車道:赤	車を感知		一定時刻 経過	人の感知 がなくなる				
	歩道:青 車道:赤		車を感知	人を感知					一定時刻 経過
	人:いる 車:いる 歩道:赤 車道:青	一定時刻 経過					人の感知 がなくなる	車の感知 がなくなる	
	車:いる 歩道:赤 車道:青					人を感知	一定時刻 経過		車の感知 がなくなる
	人:いる 歩道:赤 車道:青			一定時刻 経過		車を感知			人の感知 がなくなる
	歩道赤 車道:青				一定時刻 経過		車を感知	人を感知	

プロセス記述票 2 処理部分