組み込みソフトウェアの上流設計における試験表現に関する研究

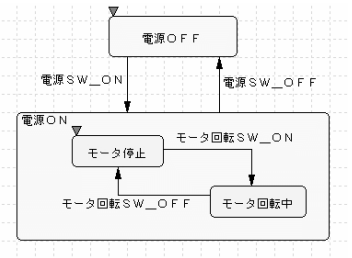
- 状態遷移モデルを基にしたモデルベース試験 -

キャッツ㈱ 山本 修二

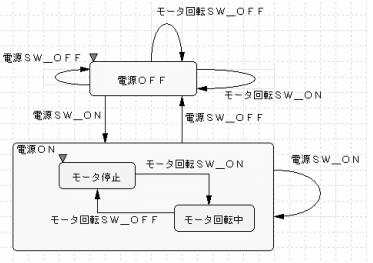
はじめに

- 近年の組み込みシステムは、複雑化を増しており、回収騒ぎなどが増加し、***メードインジャパン***の信頼性を地に落としている。
- この問題を発生させている大部分の原因は、***システム設計***と***組み込まれるソフトウェア***にある。
- 設計手法は、OOP、MDA、アジャイル などのいろいろな手法が提案され、対応するツールも徐々にそろってきているが、試験に対するアプローチも重要なポイントである。
- 組み込みソフトウェア開発では、状態遷移設計は一般的であるが、***状態遷移ベース試験は人海戦術***で行われている。
- 状態遷移試験に関する標準化を進めることで、各社ツールの連携も進展し、組み込みシステムの品質向上に貢献できる。

状態遷移設計とは？



状態遷移設計とは？



状態遷移設計とは？

□0 モータ制御	S	電源ＯＦＦ	電源ＯＮ		
				モータ停止	モータ回転中
E		0	1	2	3
電源ＳＷ＿ＯＮ	0	:)電源ＯＮ	/	/	/
電源ＳＷ＿ＯＦＦ	1	/	:)電源ＯＦＦ	/	/
モータ回転ＳＷ＿ＯＮ	2	/	/	:)電源ＯＮ:モータ回転中	/
モータ回転ＳＷ＿ＯＦＦ	3	/	/	/	:)電源ＯＮ:モータ停止

状態遷移試験

- 状態遷移抽出条件
  - 開始状態を電源OFF、終了状態を電源OFFとする。
  - 遷移する前の状態と遷移後の状態と遷移のきっかけとなるイベントが同じ組み合わせは、1つの遷移シーケンス内に 1回しか現れない。
  - イベントが発生した時、イベントが無視される場合は、遷移したと見做す。
- 状態遷移シーケンス例
  - 電源OFF - モータOFF -> 電源OFF - 電源OFF -> 電源OFF - モータON -> 電源OFF - 電源ON -> モータ停止 - 電源ON -> モータ停止 - モータOFF -> モータ停止 - モータOFF

組み込みソフトウェア試験標準化委員会」概要

- **試験関連標準化　組み込みシステム用ソフトウェア評価項目抽出ツールの開発**」（IPA情報処理振興事業協会　重点領域情報技術開発事業」）
- **組み込みソフトウェア試験標準化委員会**」(*TSCEC : Testing Standardization Committee for Embedded Software*、通称 :テセック)　設立
- 標準化内容
  1. 試験項目定義事項
     組み込みソフトウェアの試験に関する定義事項（試験項目同一性、網羅率など）
  2. 試験項目表示方法
     ユースケース図、アクティビティ図、状態遷移図（ステートチャート）、状態遷移表における試験項目の表示方法
  3. 試験項目表記方法
     抽象度の高い仕様から抽出された試験項目の表記方法

試験項目定義事項

- 試験項目の分類や試験項目が全て抽出されたかどうかの判定条件などの試験項目抽出に関連する定義事項。
  - 対応する仕様書種別
    - 試験項目を対応する仕様書種別を定義する。対応仕様書とは、状態遷移表、状態遷移図（ステートチャート）など。
  - 試験項目分類定義（例、正常、準正常、異常）
    - 試験項目の分類名、分類基準を標準化する。例えば、分類としては正常／準正常／異常で、正常とは通常イベント（タイムアウトを除いたイベント）による遷移で、イベントに対する処理が無視や禁止でないものなど。
  - 網羅率定義（評価対象項目／全項目）
    - 試験項目の全項目の定義と網羅率（カバレッジ率）の定義。
  - 試験項目の同一性定義
    - 2つの試験項目が同一であるか異なっているかの判断基準の定義。

試験項目表示方法

- 試験項目表示方法とは、本開発ソフトウェアが抽出する試験項目をコンピュータ画面上でどのように表示するかの方法である。具体的には、状態遷移図／表上やユースケース図やアクティビティー図上でどのように表示するかである。
  - 状態遷移順序（開始、経由、終了）表示方法
    - 開始／経由／終了状態と発生した状態の順序を表示する取り決めで、例えば状態遷移表上に表示する際に順序を色で表すとか番号を表示するなど。
  - 状態遷移の重複時の表示方法
    - 複数の試験項目を同じ仕様書上に表示する際に、2回以上経由した状態／イベント／処理をどのように表示するかで、例えば状態遷移表上の処理に表示する場合に、処理のセルに複数の色で分けられた箱状に表示するとか回数を右上に回数を数字で表示するというような詳細な表示方法。
  - イベント発生順序表示方法
    - 開始／経由／終了イベントと発生したイベントの順序を表示する取り決めで、例えば状態遷移表上に表示する際に順序を色で表すとか番号を表示するなど。
  - 仕様書種別毎の表示方法
    - 対応する仕様書種別の取り決めで、例としてはユースケース図、アクティビティ図、状態遷移図（ステートチャート）、状態遷移表など。

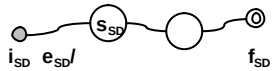
試験項目表記方法

- 試験項目表記方法とは、本開発ソフトウェアが抽出する試験項目を電子ファイルや書類上にどのような記号で記述するかである。
  - 状態表記方法
    - 状態どのような記号で表すかを標準化する。例えば、XMLで表すとすれば、タグの名称をどうするかとか、テキストで表すとすれば、半角アルファベットで"Sx"（x:番号）であるとかを細かく標準化する。
  - イベント表記方法
    - イベントをどのような記号で表すかを標準化する。例えば、XMLで表すとすれば、タグの名称をどうするかとか、テキストで表すとすれば、半角アルファベットで"EVx"（x:番号）であるとかを細かく標準化する。
  - 遷移表記方法
    - ある状態からどのイベントでどの状態に遷移した際の遷移をどのように表すかを標準化する。例えば、XMLで表すとすれば、タグの名称をどうするかとか、テキストで表すとすれば、半角アルファベットで"" -> ""であるとかを細かく標準化する。

標準案内容

1. 状態図（SD）
2. タスク状態図（TD）
3. 各種定義
4. 遷移列集合（TS）
5. 並列遷移列（CTS）

1. 状態図（SD）



- g := [ ]　..... guard
- a := < > ..... assertion
- l := string ..... label
- n := { } ..... note

- $g^{?}$ (exp, TASK)
- $a^{?}$ (exp, TASK)
- $e^{?}$ (l, m, time, pri)
- $s_{SD}^{?}$ (g, a, l, n, PROC)
- $t_{SD}^{?}$ (e, g, a, l, n, PROC, s_s,s_d)
- $SD^{?}$ (I_{SD}, F_{SD},S_{SD}, T_{SD}, f, f^{-1},E_{SD})

- Type
  - I
  - exp
  - PROC
  - task

2. タスク状態図
(タスク間関係は今後検討)

- sTD ? (g, a, l_t, n, PROC, prev)
  - **l**は**タスク名**、**prev**は**PROC**で表せるが、理解を助けるために独立させる。
  - **Temporal operator** は、**perv**と**g**,**a**で使用する。**Prev**は、**g**,**a**で書く。
- TD ? (l_{TD}, F_{TD}, S_{TD}, T_{TD}, f, f^{-1}, l_t, pri, time, E_{TD}, TYPE)
  - タスク間通信 ∈ E_{TD}

3. 各種定義

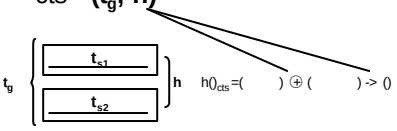
- 入力 ? イベント
- 出力 ? s × Proc out
  - 遷移先状態をsとする。
- 入出力 ? 入力×出力
- 入出力列 ? 入出力*
- Proc p
- Proc列 p*
- イベント e ∈ E
- イベント列 e*
- 状態 s
- 状態組 s×s
- 状態列 s*
- 遷移 t
- 遷移列 t*

4. 遷移列集合 (TS)

- 入出力列を決める。
- 遷移列、ts ∈ TS
- ts ? (i_{ts}, f_{ts}, T_{ts}, g)
  - $t \in T_{ts}$, t_1 -> t_2 -> …… -> t_n
  - $t_{i+1} = g(t_i)$

5. 平行遷移列 (CTS)

- ts ∈ TS , tg ⊂ TS
- cts ? **(t_g, h)**



標準化案例 (試験項目表記方法)

```
<?xml version='1.0' encoding='UTF-8' ?>
<!DOCTYPE pathGroup SYSTEM 'file: pathGroup.dtd '>
<pathGroup>
 <title>モータサンプル</title>
 <path>
  <state>
   <stateName>電源OFF</stateName>
  </state>
  <transition>
   <eventName>電源SW_ON</eventName>
   <state>
    <stateName>電源ON：モータ停止</stateName>
   </state>
  </transition>
  <transition>
   <eventName>モータ回転SW_ON</eventName>
   <state>
    <stateName>電源ON：モータ回転中</stateName>
   </state>
  </transition>
  <transition>
   <eventName>モータSW_OFF</eventName>
   <state>
    <stateName>電源ON：モータ停止</stateName>
   </state>
  </transition>
  <transition>
   <eventName>電源SW_OFF</eventName>
   <state>
    <stateName>電源OFF</stateName>
   </state>
  </transition>
 </path>
</pathGroup>
```

標準化案例 (試験項目表記方法)

```
<?xml version='1.0' encoding='UTF-8' ?>
<!ELEMENT pathGroup (title, path+) >
<!ELEMENT title (#PCDATA) >
<!ELEMENT path (state ,transition+,state ?) >
    <!ELEMENT state
    (activity?,stateName ,guard? ,assert? ,activity?,path?,activity ?)>
<!ELEMENT transition (eventName ,guard? ,op?,state ?)>
<!ELEMENT stateName (#PCDATA) >
<!ELEMENT eventName (#PCDATA) >
<!ELEMENT op (#PCDATA) >
<!ELEMENT activity (#PCDATA) >
<!ELEMENT guard (#PCDATA) >
<!ELEMENT assert (#PCDATA) >
```

状態遷移シーケンス抽出ツール プロトタイプ

組み込みソフトウェア試験標準化委員会」 連絡先

- 横浜市港北区新横浜2-11-5　キャッツ株式会社内
- 　組み込みソフトウェア試験標準化委員会」事務局
- E-mail : TSCEC@egroups.co.jp
- URL：http://www.egroups.co.jp/group/TSCEC
  - ソフトウェア事業部　山本 修ニ
  - 電話 :045(473)2816
  - FAX :045(473)2673