2019 年 5 月 15 日　第 1 版

組込みソフトの安全設計

ー基礎から二足歩行ロボットによる実践まで

付録

第５章 5.5 の補足

「5.5 トレーサビリティを活用した変更における影響範囲の特定と試験項目抽出の例」で説明した SR1-6 と SR4-2 の仕様変更に関して、誌面の都合上、その設計内容の一部が書籍に掲載できませんでした。

そこで本資料では、ソフトウェア詳細設計からソフトウェアユニット試験も含め、仕様 SR1-6 と SR4-2 に関わる設計内容を補足説明します。前と記載した部分が仕様変更前の記述で、後と記載した部分が仕様変更後の記述です。

SR1-6 に関わる設計内容

【システムの動作仕様】

- 前完了状態ではヒータオフ，LED 長周期点滅とする．(SR1-6)
- 後保温状態ではヒータ保温，LED 長周期点滅とする．(SR1-6)

【モジュールの機能と動作仕様】

システム状態制御モジュール（M1）

機能

- 現在のシステムの状態とスイッチやサーミスタ温度入力，時間経過により次のシステムの状態を決定し，ヒータ，LED 表示を制御する．

動作仕様

- スイッチ入力検知モジュールから取得したスイッチ押下確定情報やサーミスタ温度検知モジュールから取得した平均温度，時間経過によりシステムの状態を決定する．各状態において，ヒータ制御モジュールへヒータ制御状態を指示し，LED 表示制御モジュールへ LED 表示状態を指示する．詳細は電気ケトルの動作仕様通りとする（状態遷移表及び図を参照）．(SR1-1～14)

【インタフェースの抽出】

システム状態制御モジュール（M1）

入力：スイッチ押下確定情報，平均温度

出力：LED 表示状態指示，ヒータ制御状態指示

関数：システム状態制御処理ユニット（U1-1）

【ソフトウェア詳細設計】

システム状態制御モジュール（DD1）

ファイル名　　system.c

公開インタフェース system.h

関数

システム状態制御処理ユニット(DD1-1)

システム状態制御処理ユニット（DD1-1）

関数名　void system_control(void)

処理内容

- 変数定義初期化でシステム状態を待機状態とする．（DD1-1-0）

・・・

前完了状態

後保温状態

- 前完了状態ではヒータ制御状態指示をヒータオフ，LED 表示状態指示を LED 長周期点滅とする．（DD1-1-3-1）
- 後保温状態ではヒータ制御状態指示を保温，LED 表示状態指示を LED 長周期点滅とする．また，平均温度をヒータ制御モジュールに渡す．（DD1-1-3-1）

・・・

【ソースコード】

（システム状態制御処理ユニット　system.c）

```
    case  COMPLETE:                                       /* 保温状態 */
          if((u16_temperature <= TEMP_40) || (TEMP_150 <= u16_temperature)){
                e_system_state = TH_BREAKDOWN;/* サーミスタ故障であればサーミスタ故障状態へ */
          }else if(f_switch.on_off == ON){                /* スイッチが押下された場合 */
                f_switch.on_off = OFF;                    /* スイッチ押下フラグクリア */
                e_system_state = WAIT;                    /* 待機状態へ */
          }else if(TEMP_110 <= u16_temperature){
                e_system_state = OVERHEAT;            /* 110℃以上であれば空焚き状態へ */
          }
          e_heat_output = KEEP_90;                        /* ヒータ保温指示 */
          u16_temperature_h = u16_temperature;            /* 平均温度の設定 */
          e_lighting_type_oder = COMPLETION_INFORM;       /* ＬＥＤ長周期点滅 */
          break;
```

【ソフトウェアシステム試験】

- 前完了状態ではヒータオフ，LED 長周期点滅となる．（ST1-6）
- 後保温状態ではヒータ保温，LED 長周期点滅となる．（ST1-6）

【ソフトウェアユニット試験】

前完了状態

後保温状態

- 前完了状態ではヒータ制御状態指示がヒータオフ，LED 表示状態指示が LED 長周期点滅となる．（UT1-1-3-1）

・ 後保温状態では，ヒータ制御状態指示が保温，LED 表示状態指示が LED 長周期点滅となる．また，平均温度がヒータ制御モジュールに渡される．(UT1-1-3-1)

SR4-2 に関わる設計内容

【モジュールの機能と動作仕様】

ヒータ制御モジュール（M4）

機能

・ 前システム状態制御モジュールの指示に従いヒータをオン・オフし、水を加熱する。
・ 後システム状態制御モジュールの指示に従いヒータをオン・オフし、水を加熱、保温する。

動作仕様

・ マイコンリセット直後はヒータオフとする（SR4-1）
・ 前ヒータ制御状態（オン・オフ）の指示に従って、ヒータをオン・オフする。(SR4-2)
・ 後ヒータ制御状態（オン・オフ・保温）の指示に従って、ヒータをオン・オフ・保温制御する。保温温度は 90 ±2 ℃とする。

【インタフェースの抽出】

ヒータ制御モジュール（M4）

入力：前ヒータ制御状態指示（オン・オフ）
　　後ヒータ制御状態指示（オン・オフ・保温）
出力：ヒータ出力ポート初期設定値
　　ヒータオフ
関数：ヒータ制御初期化処理ユニット（U4-0）
　　ヒータ制御処理ユニット（U4-1）

【ソフトウェア詳細設計】

ヒータ制御モジュール（DD4）

ファイル名　　heater.c
公開インタフェース heater.h
　入力
　　ヒータ制御状態指示（オフ、オン、保温）
　　前 enum HEAT_OUTPUT{HEAT_OFF = 0,HEAT_ON}
　　後 enum HEAT_OUTPUT{HEAT_OFF = 0,HEAT_ON,KEEP_90}
　　enum HEAT_OUTPUT e_heat_output
　　後平均温度
　　unsigned int u16_temperature_h;

関数

ヒータ制御初期化処理ユニット(DD4-0)

ヒータ制御処理ユニット(DD4-1)

ヒータ制御初期化処理ユニット（DD4-0）

関数名 void init_heater(void)

処理内容

・ヒータ制御出力ポートをデジタル出力、出力レベルは Low とする。(DD4-0-1)

利用する外部インタフェース

出力

ヒータ出力ポート制御レジスタ

P10,PM10,PMC10

ヒータ制御処理ユニット（DD4-1）

関数名 void output_heater(void)

処理内容

・ ヒータ制御指示がオフであれば、ヒータをオフにする。(DD4-1-1)

・ ヒータ制御指示がオンであれば、ヒータをオンにする。(DD4-1-2)

・ 後ヒータ制御指示が保温であれば、平均温度が 89 ℃以下になればヒータをオンにし、91 ℃以上になればヒータをオフにする。(DD4-1-3)

利用する外部インタフェース

出力

ヒータ出力ポート　P10

提供する公開インタフェース

入力

ヒータ制御状態指示

e_heat_output;

後平均温度

u16_temperature_h;

後マクロ定数

保温しきい値下限（89 ℃）　TEMP_89

保温しきい値上限（91 ℃）　TEMP_91

【ソースコード】

（インタフェース　heat.h）平均温度を取得するインタフェース変数追加

```
enum HEAT_OUTPUT{HEAT_OFF = 0,HEAT_ON,KEEP_90};        /* ヒータ制御状態指示 */
extern enum HEAT_OUTPUT e_heat_output;
extern unsigned int u16_temperature_h;                  /* 平均温度のインタフェース */
```

（ヒータ制御処理ユニット　heater.c）保温指示の処理追加

```
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
unsigned u16_temperature_h = TEMP_20;                    /*  平均温度  */
・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
        switch(e_heat_output){                           /*  ヒータ制御指示により処理を実行する  */
        case HEAT_OFF:                                   /*  ヒータ制御指示オフの場合  */
                /*  ヒータ制御指示を異常の場合と同じ処置とするため break;  を記載せず  */
                defult:                                  /*  ヒータ制御指示が異常の場合  */
                P1_bit.no0 = 0U;                         /*  ヒータオフ  */
                break;
        case HEAT_ON:                                    /*  ヒータ制御指示オンの場合  */
                P1_bit.no0 = 1U;                         /*  ヒータオン  */
                break;
        case KEEP_90:                                    /*  ヒータ制御指示保温の場合  */
                if(u16_temperature_h >= TEMP_91){        /*  平均温度が 91℃以上の場合  */
                        P1_bit.no0 = 0U;                 /*  ヒータオフ  */
                }else if(u16_temperature_h <= TEMP_89){  /*  平均温度が  89℃以下の場合  */
                        P1_bit.no0 = 1U;                 /*  ヒータオン  */
                }else{          /*  平均温度 89℃を超え 91℃未満ではヒータ制御を以前のままとする  */
                }
                break;
    }
```

【ソフトウェアシステム試験】

ヒータ制御機能の試験（ST4）

マイコンリセット直後はヒータオフとなる。（ST4-1）

ヒータ制御状態（オン・オフ）の指示に従って、ヒータをオン・オフする。（ST4-2）

- 待機状態ではヒータオフとなる。（ST4-2-1）
- 加熱状態ではヒータオンとなる。（ST4-2-2）
- 前完了状態ではヒータオフとなる。　（ST4-2-3）
- 後保温状態では 90　±2　℃に保温される。　（ST4-2-3）
- 空焚き状態ではヒータオフとなる。（ST4-2-4）
- サーミスタ故障状態（断線）ではヒータオフとなる。（ST4-2-5）
- サーミスタ故障状態（短絡）ではヒータオフとなる。（ST4-2-6）

【ソフトウェアユニット試験】

ヒータ制御モジュール（UT4）

ヒータ出力ポート設定初期化処理ユニット（UT4-0）

- マイコンリセット直後、ヒータ出力ポートがデジタル出力、オフに設定される。（UT4-0-1）

ヒータ制御処理ユニット（UT4-1）

- ヒータ制御指示がオフであれば、ヒータをオフにする。（UT4-1-1）
- ヒータ制御指示がオンであれば、ヒータをオンにする。（UT4-1-2）

・ 後ヒータ制御指示が保温であれば、平均温度が 89 ℃以下になればヒータをオンにし、91 ℃以上になればヒータをオフにする。(UT4-1-3)

書籍の誤記修正

書籍中の誤記を修正します。青字部分が修正箇所です。

誤記

65 ～ 66 頁

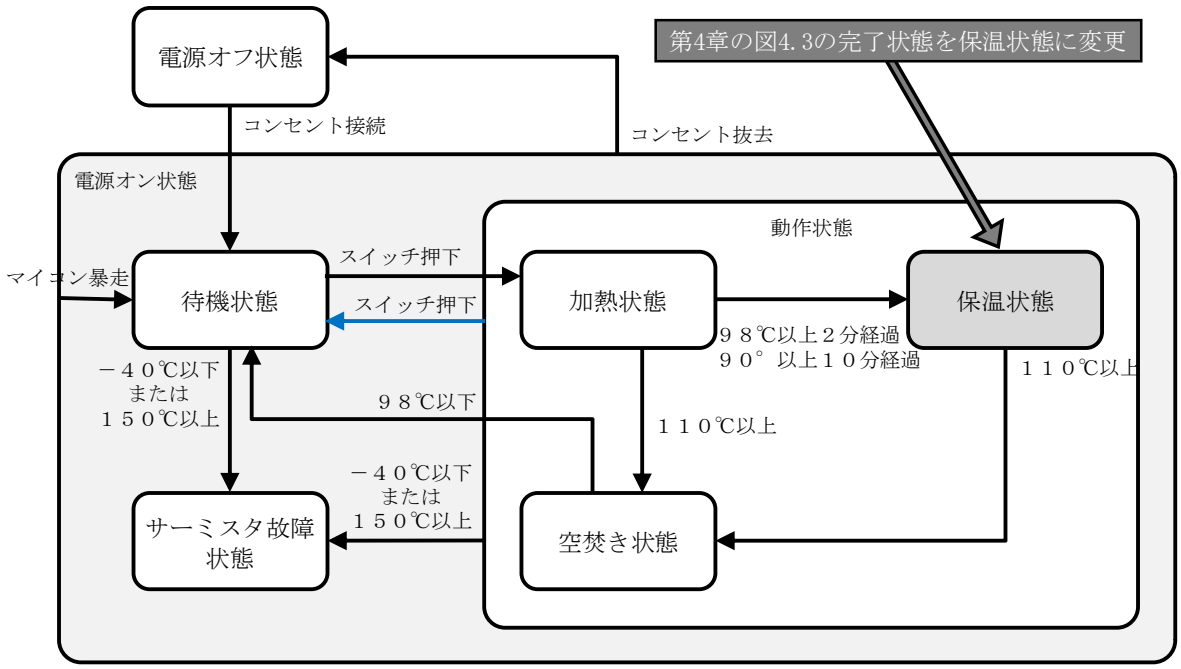
ソーソコード 4.1　電気ケトルのシステム状態を制御する関数

s16_temperature を u16_temperature に修正（13 箇所）

96 頁

図 5.5　電気ケトルの状態遷移図

加熱状態から待機状態への矢印を動作状態から待機状態への矢印に修正



97 頁

「変更後」に次の青字部分を追記

保温状態ではヒータ制御状態指示を保温,LED 表示状態指示を LED 長周期点滅とする. **また,平均温度をヒータ制御モジュールに渡す.**

98 ～ 99 頁

文書およびソースコード中

s16_temperature を u16_temperature に修正（5 箇所）

s16_temperature_h を u16_temperature_h に修正（7 箇所）

ソースコード 5.3　保温指示の場合の処理を追加（ヒータ制御処理ユニット）

0x0100U を TEMP_20 に修正

99 頁

ソースコード 5.3　下記のように、/* ヒータオフ */　を　/* ヒータオン */　に修正

```
case HEAT_ON:           /* ヒータ制御指示オンの場合 */
  P1_bit.no0 = 1U;      /* ヒータオン */
  break;
```

100 頁

次の青字部分を追記

ただし，UT1-1-3-1 のみ「保温状態では，ヒータ制御状態指示がヒータ保温，LED 表示状態指示が LED 長周期点滅になる．**また，平均温度がヒータ制御モジュールに渡される．**」と変更されます．