

セサミ電機

SozeX002 ソフトウェア仕様書

FirstRelease Sep16 2003

v1.3 Apr19 2004

東陽テクニカ 二上貴夫

本仕様書の目的と記述ルール

この仕様書は、製品企画を理解した組込みソフトウェア技術者がソフトウェアを設計するために利用することを意図している。同時にテストファーストを実現してシステムテストの品質を確保する資料でもある。

仕様書の記述原則は、デマルコの構造化分析手法に基づいている。ただし、リアルタイムシステムとしての記述に求められる問題に対してハトレーピルバイの拡張や UML を参考にしながら、次の変更を行っている。

1. コンテキスト図は、省略した。その代わりに DFD0 にターミネータを記入した。
2. プロセスの命名規則は、動詞句にはこだわらない表現をした。
3. プロセスの仕様 (PSPEC) は、文書、状態モデルなどで表現している。
4. 状態モデルで表現した部分については、
 - (ア) (当然だが) 状態のストアは表現していない。
 - (イ) 状態モデルのアクションとイベントでプロセスへの入出力フローを利用できるとみなしてモデリングしている。
 - (ウ) 最も簡単なムーアモデルを使用し、エントリアクションは存在するがアクティビティは使用しない。
5. プロセス仕様書の中で他のプロセスの起動/停止を制御している。プロセスは、全てシングルトンを想定する。OO のような多重インスタンス生成は存在しない。この制御は、ハトレーピルバイ手法と同じく文書のみで表現している。このため、明示的な制御フローと制御仕様書は用いなかった。

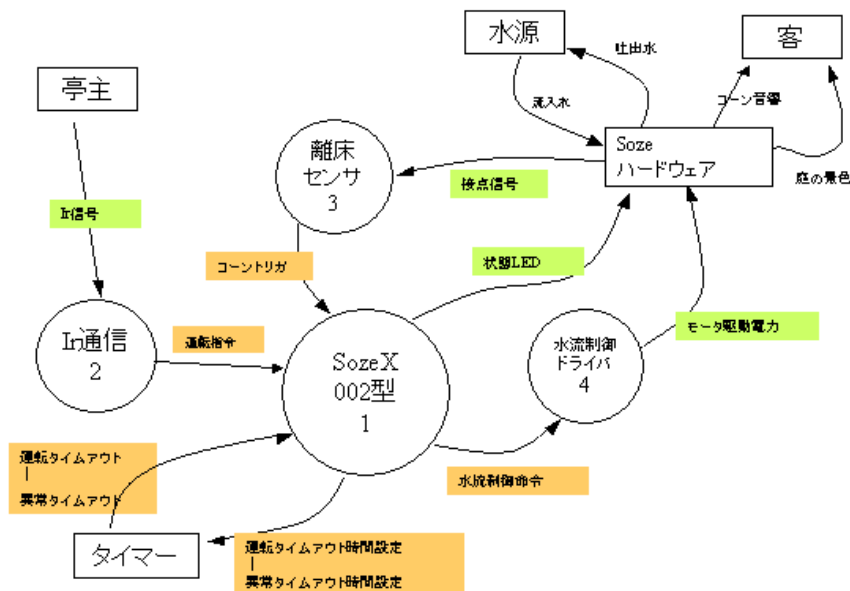
以上は、DFD モデリングと初等 UML を知っている技術者であれば解る範囲に納めてある。
(セサミ中級の受講者に期待される程度の知識と仮定する)

X002 型の概要

X002 は、X001 量産初号機に続くエコ対応機種である。竹筒が満水時に水流ポンプを一時停止して竹筒復帰中の水はねによる損失を防止する。赤外線受信は、X001 と同じく運転開始と停止の 2 命令を受け取る。

システムモデル (製品 DFD0)

X002型システムモデル



X002 型の新機能は、上図の離床センサ (3) と状態 LED フローで示されている。また、一部のデータフロー名称をより適切な名称に改訂してある。

本 DFD から動作シナリオを理解するためには、次節のイベント分析と対比して理解すること。

イベント分析

イベント 1 . 亭主が SozeX を購入した

亭主が広告や聞き伝えによって SozeX を購入する。実際の購入から納品、施工までの過程は、本仕様の範囲外であるから省略する。

刺激：電源投入 (DFD としては、明示的なフローではない。状態図の初期状態の開始に相当する)

活動：SozeX を待機状態にする

応答：状態 LED を消灯

イベント 2 . 茶会を開く

2 - 1 イベント：亭主が茶会を始める

刺激：Ir の運転開始信号

活動：SozeX の運転を開始する。

このあとは、動作不良があれば停止などの処理を全て含む

応答：水流ポンプとセンサー系で動作が行われる

結果：客は待合に通される

2 - 2 イベント：満水 / 離床

刺激：離床スイッチ = off

活動：ポンプを停止する

応答：ポンプ駆動 = off

結果：水がはねずに竹筒が復帰する

2 - 3 イベント：吐水後の復帰 / 着床

刺激：離床スイッチ = on

活動：ポンプを運転する

応答：ポンプ駆動 = on

結果：竹筒にふたたび注水される

2 - 4 茶会が終了した

2 - 4 - 1 亭主が停止操作を行う

刺激：運転命令 = “ 停止 ”

活動：システムを停止する

応答：排水し、水流ポンプが停止する

結果：亭主は、茶会と鹿威し操作性に満足する

2 - 4 - 2 亭主が停止操作を忘れた

刺激：運転タイムアウト

活動：システムを停止する

応答：排水し、水流ポンプが停止する

結果：無駄な電力、水資源を使わずに済む

ターミネータ仕様

以下は、X002 型システムモデルにあるターミネータの仕様である。

- 亭主

SozeX を含めた茶室のオーナーである。本書では、システムの施工後に行う操作は全て亭主が行うことと仮定してモデリングしている。このため、現実にはありえないが、システムの初期化など施工業者の作業も亭主の作業に含めている。要求レベルのシステムテストでは、このモデルの不完全さが問題になるだろう。テストチームによる適切なモデル改良が待たれる。

- タイマー

鹿威しのアプリケーションとして必要なタイマーとタイムアウト検知機能を表現している。よって、Ir の PPM 受信機能用タイマーは、Ir サブシステムの内部とみなしたのでこのタイマーには含めない。

タイムアウトの計測精度は、1 秒で十分である。タイムアウトを知りたい事象については、亭主の停止忘れ対策（180 分）と運転中の故障検出（数秒から数十秒）の 2 種類がある。

タイマー設定にゼロを与えると動作中のタイマーは停止する。

- SozeX ハードウェア

竹や木で作られている鹿威しの機構と装着されたセンサ、状態 LED、水流ポンプを含むハード系や庭そのものを表現している。よって、茶会に招かれた客が見て楽しむ庭の景色、聞くコーン音響なども含めている。ただし、センサアンプや水流ポンプ用の電力供給系は内部プロセスに含めている。流入水と吐出水は、大方はバランスするが、水はねによる散逸がある。この問題を解決するのが離床センサを使った X002 の目玉機能である。

プロセス詳細

DFD-1 プロセス名：SozeX002

入力：運転指令，タイムアウト，異常タイムアウト，コーントリガ

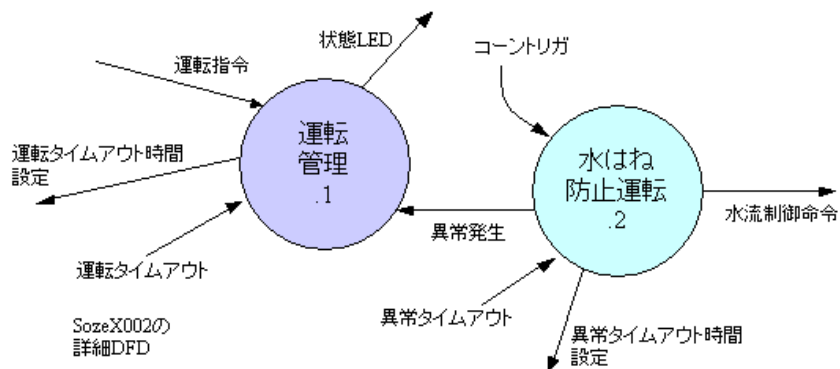
出力：タイムアウト時間，異常タイムアウト時間，水流制御命令

動作：SozeX002 プロセスは、内部で運転管理と水はね防止運転が協調動作する

水はね防止運転は、運転管理プロセスによって起動/停止される。

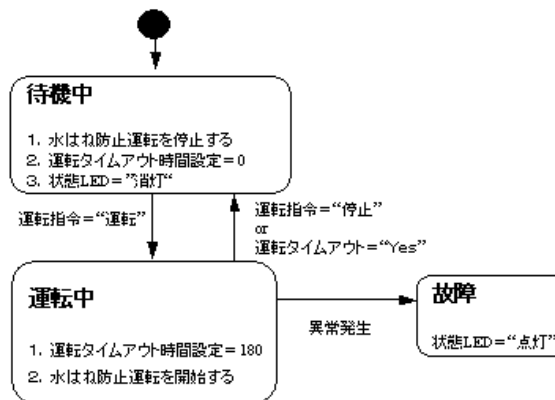
X002 の仕様では、竹筒が運転中に平衡状態に陥ってタイムアウトが生じる異常水はね防止が検出する。それを運転管理が受け取り、故障とみなす。故障の表示は、状態 LED で行う。ここで平衡状態とは、排水中や復帰中に人為や自然な理由によって竹筒の回転運動が止まってしまうことを指す。

DFD1



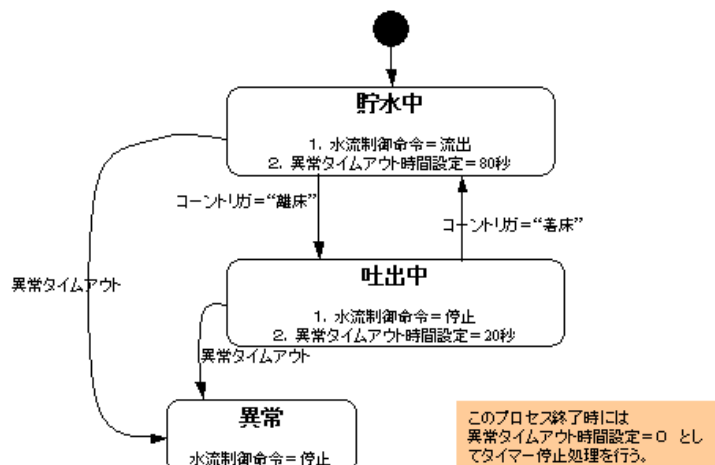
- DFD-1.1 プロセス名：運転管理
 入力：運転指令，タイムアウト，異常発生
 出力：タイムアウト時間，
 動作：下記の状態モデルを参照。なお、本プロセスは、亭主の指令に应答して水はね防止運転プロセスを制御する。異常発生と運転停止が同時に発生した場合には、運転停止を取り、異常発生は無視すること。

PSPEC1.1 運転管理の状態モデルによるプロセス仕様



- DFD-1.2 プロセス名：水はね防止運転
 入力：コントリガ，異常タイムアウト
 出力：異常発生，異常タイムアウト時間，水流制御命令
 動作：下記の状態モデルを参照のこと
 異常タイムアウトとコントリガ離床が同時に発生した場合は、コントリガを取り、異常発生は無視すること。

PSEPC1.2 水はね防止運転の状態モデルによるプロセス仕様



DFD-2 プロセス名 : Ir 通信

入力 : Ir 信号

出力 : 運転指令

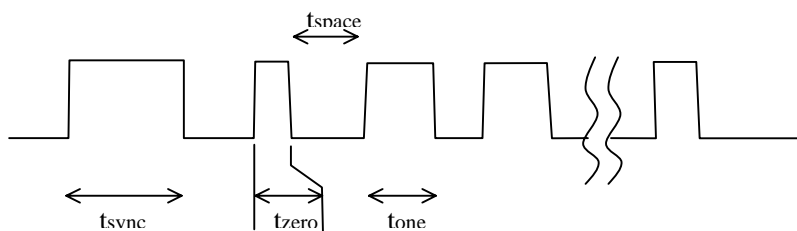
動作 :

亭主がリモコンを操作した結果特定の Ir 信号が SozeX の光トランジスタに到達する。この信号は、40 KHz のベースバンド変調がかかっている。また、外光によるトランジスタのオフセット電圧が数 Hz 以下の変動をする。これらをバンドパスフィルタにより除去して増幅し、[PPM 変調](#)の論理信号を取り出す。(この部分は、X002 ではハードウェアの Ir 検出モジュールを使用する) なお、このリモコン受信は、同期ずれなどによる信号エラーが多発する。エラー発生後は、直ちに次の受信を可能とすること。

PPM 変調の論理信号は、以下のような時系列信号としてプロセッサの論理信号入力ポートに入る。

データフォーマット :

一定時間 t_{sync} の同期信号の後、データ32ビット、CRC8ビットが続く(PIC3704は負論理出力であるから下図とは極性が反転する) この40bitの連続した信号を Ir パケットと呼ぶ。



t_{sync} : 2200 ~ 2500 μ Sec パケットの先頭を示し、同期を取るための信号

t_{space} : 約 500 μ Sec 有意信号 (t_{zero} や t_{one}) を識別するスペーシング期間

t_{zero} : 450 ~ 600 μ Sec 論理値の0を意味する

t_{one} : 1200 ~ 1400 μ Sec 論理値の1を意味する

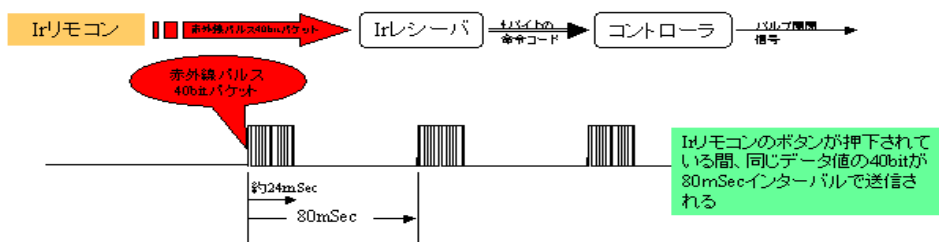
このデータ 32bit + CRC8bit の信号を受信したならば、CRC は、検査しないでよい。データ部の32bitを以下のように読み替えて1バイトの運転指令として出力すること。

なお、データ部の値は、将来変更されることを前提に設計すること。

データ部	運転指令	意味
0x536F0000	'r'	亭主が運転開始のリモコン操作を行った
0x536F0001	's'	亭主が運転停止のリモコン操作を行った

Ir パケットの始まり(下図 t_{sync} の立ち上がり)から次の Ir パケットまでは、 $80mSec \pm 10mSec$ 程度である。この時間は Ir リモコンに依存しているため、断定ができないが、最小40mSec のアイドル時間があることを前提に設計を行ってもよいこととする。

注意) Ir のデータフォーマットやタイミングはリモコンの機種によって異なるため、リモコンの機種に合わせた対応が必要となる。



DFD-3 プロセス名：離床センサ

入力：接点信号

出力：コントリガ

動作：

負論理の竹筒離床信号を検出しコントリガとして出力する。

接点信号は、竹筒が空で、そのつかが叩き石に接している時に Hi

離床したときに Lo となる負論理信号である。この論理信号は、PIO の入力端子に入力されている。接点であるから、チャタリングが発生するので、以下の条件でコントリガの出力を定める。

離床、着床の決定論理：

10mSec のインターバルで接点信号を 100mSec の期間観測する。この観測の繰り返しが連続して 10 回同じ値をとった場合に、コントリガの出力値を更新する。変化が生じている間は、出力値を更新しない。

コントリガ = 着床 10mSec インタバル 100mSec 期間での接点信号観測値が全て Hi

コントリガ = 離床 10mSec インタバル 100mSec 期間での接点信号観測値が全て Lo

この観測方法だと、接点の変化から最悪で約 100mSec の変化の確認遅延が生じる。離床時点での竹筒の角速度は、たかだか 1rad/Sec 程度であるから、この遅延は無視して構わない。

DFD-4 プロセス名：水流制御ドライバ

入力：水流制御命令

出力：モータ駆動電力

水流制御命令 = “流出” であれば、モータ駆動電力を出力する

水流制御命令 = “停止” であれば、モータ駆動電力を出力しない

モータ駆動電力の出力と抑止は、モータドライバへ接続された MPU の出力ポートへの制御信号書き込みで実現される。

現在のところは、単純な 0/1 の出力であるが、次のシリーズでは、8 ビットの DA コンバータを通じて出力電力のパターンを変えることを予定している。よって設計は、この点を考慮して行うこと。

データ辞書

本仕様書に出たデータフロー、ストア、内部データの構造と意味を示す。

データ辞書の記法は、BNF に準拠している。

- ・ 素データで定義可能なところには上限と下限の値を含めた。
- ・ 下線があるものは、ソフトウェアでは扱わないものか、物理的なフローである。

流入水 := 竹筒に流れ込む水のこと

吐出水 := 竹筒が反転した時に出て行く水のこと

庭の景色 := 客が鑑賞できる SozeX を含めた庭の景色

運転タイムアウト時間設定 := 180分くらいを想定。 今後の製品展開で変更か？

下限：1 上限：240 単位：分

運転タイムアウト := タイマが発火したことの通知

下限：5 上限：40 単位：秒

異常タイムアウト時間設定 := 状態に依存して数十秒の値をとる

異常タイムアウト := 異常設定に対してタイマが発火したことの通知

異常発生 := 水はね防止運転プロセスが異常を検出したことの通知

水流制御命令 := [“流出” | “停止”]

モータ駆動電力 := 水流ポンプの DC モータを駆動する電力 ノミナル 3V300mA

接点信号 := 物理的な接点の導通状態をとる。チャタリングあり。

コーントリガ := [“離床” | “着床”]

Ir 信号 := 赤外線リモコンからの Ir 信号だが、電灯や日光などの雑音を含むことがある

運転指令 := [“運転” | “停止”]

設計への考慮点

設計条件

開発するプログラムは、インスペクション/ピアレビューによる品質の確認を行える構造と読解性を持つように設計すること。特に MPU に固有のコードは、できる限り局所化しておき MPU 依存性チェックをその領域に限定して実施できることが望ましい。計画では欧州生産の製品には、欧州製の MPU を利用する。よって最も重要な問題は、ソースコードの移植性である。特に欧州では、ファイルの内容を一部でも書き換えた場合にリグレッションテストが要求されるため、コードを手直ししないことによるコストメリットは大きい。また、各機能は、独立して入出力テストできるように設計すること。

実装に関する情報

X002 は、MPU として M16C、実装ボードとしてオクス電子(株)の OAKS16 MINI ボードを採用することになっている。

を採用することになっている。以下に現時点で明らかになっている接続情報を示す。詳細は、ハードウェア製造仕様を参照のこと。

- M16 との接続

Ir 受信モジュール→M16

Ir 受信モジュールの TTL 出力(負論理)を M16C の p83/INT1 (ディスクリット入力)へ接続する。

接点スイッチモジュール→M16C

標準実装では、離床接点スイッチは、OAKS16 MINI ボードのトグル SW5 へ並列 OR 接続する。そのため、TTL 出力(負論理)を M16C の P80pin へ接続する。これによって離床のイベントをハードレベルで試験することができる。

トグル SW5 を別の用途で使用できるように、離床接点スイッチを P85pin へ接続することもオプション仕様として許可する。

M16→水流制御

OAKS16 MINI ボードの LED に並列出力接続する(M16C 内部のドライバ IC 出力に並列接続したことになる)。

LED2 を対象とした場合、P74=HI/LED 消灯でリレー Open、点灯で Close となる
LED3 を対象とした場合、P75=HI/LED 消灯でリレー Open、点灯で Close となる
オプション仕様として、リレーと LED の動作が逆であるものも認める。

シリアルポート 2 ↔ M16C Send,Receive,GND のみ使用

用語解説

- テストファースト

プログラムを作成する前に、作成しようとするプログラムの試験用プログラムを作成する。

作成後、その試験用プログラムを実行し、すべての試験を通過した時点で、プログラムが完成したと見なす。

- 同期と非同期通信

同期通信

●同期通信は、共通に参照できる同期クロックを使って、送信側と受信側が全く同じタイミングでデータを送信/受信する。同期クロックの立ち上がり、立下り、もしくは両方を使う場合がある。

例:

- a) 同期クロックの立ち上がりで送信がわは、データを伝送ラインにのせて電位を保持する
- b) 受信側は、同期クロックの立下りで伝送ラインの電位レベルを読み出す

非同期通信

送信側と受信側が仕様上一致するはずの同期信号をそれぞれ使って通信する。

ただし、通信の開始は、送信側から知らせる必要があるため、通信の単位(パケットとかブロックと呼ぶ)の先頭は、同期をとるための信号、ブロックとなる。

非同期通信の場合には、機器の都合で送信間隔がずれてしまう場合もある。また、送信、受信両者の電子回路の個体差で時間誤差が生じる。このような誤差を吸収するような受信方式を使用する必要がある。

- 調歩式同期通信の概念

- 送信側のタイミング仕様と受信側のタイミング仕様を合わせておく
- 誤差に関しては、一定間隔ごとにタイミングを取り直すことで誤差を吸収する

Ir 方式の場合には、

- Ir 通信の場合 ... 1 ビットごとに同期を取り直す
 - 各データは 0 で始まり 1 で終了することを利用
 - そのため、「1 から 0 に変化した時点」を各データの切れ目と見なせるので、そこで同期を取りなおすことができる

- PPM 変調方式

●各データとも LOW が space 時間継続し、次に HIGH が zero 又は tone 期間継続する。その後、LOW となって終了する。最後の LOW は、次の信号の LOW と等しい。

●「LOW のあと、HIGH が続く時間の長さ」で論理 0 か 1 かが決定する。これが PPM

