安全性を考慮した組込みソフトウェア開発に関する考察
―介護ベッドを事例に―

2014SE029 石井聖大
指導教員：沢田篤史

1　はじめに

近年，組込みシステムの多機能化や高性能化により，多数のセンサを搭載したシステムが増えている．このようなシステムでは，センサから取得した外部環境の情報をコンテキストとして，それに応じて振舞いを変化させるコンテキストアウェアで組込みシステムの動作処理を実現することが多い．コンテキストアウェアなソフトウェアの開発において，開発の効率化が求められており，多くの開発環境やソフトウェアアーキテクチャが提案されている．

このような組込みソフトウェアを開発していく上で，開発者にとって特に安全性の保証が重要とされている．安全性を考慮したソフトウェア開発の中で注意すべき点は様々あるが，それらを場当たり的に対処しているだけでは，系統的な開発が望めない．安全なソフトウェアを開発するために，議論すべき事項を明確にすることで円滑なソフトウェア開発が期待される．

本研究の目的は，安全性を考慮した組込みソフトウェアの開発支援である．本研究室で提案されている組込みソフトウェアのためのアーキテクチャ [1] を適用し，このアーキテクチャに基づいて安全な組込みソフトウェアを開発するさいに注意しなければならない点を整理する．

本研究では，組込みソフトウェアとして電動式介護ベッドの制御ソフトウェアを事例として取り上げ，現存する介護ベッドの基本的な機能を抽出し，センサと組み合わせて仕様を考察する．また安全性を考慮するために，介護ベッドの動作中に異常が発生したさいの安全を保証する機能を考察する．この介護ベッドの設計に，本研究室で提案されているアーキテクチャ [1] を適用し，安全なソフトウェアの開発に関する有効性および課題を考察する．

2　背景技術

2.1　組込みシステムのためのアスペクト指向アーキテクチャ

図 1 に組込みシステムのためのアスペクト指向アーキテクチャ [1] の概要を示す．組込みシステム全体をオブジェクト指向 (コアコンサーン) とし，コンテキストおよび非機能特性 (実時間，耐故障) を横断的コンサーンとして，これらを統一的に扱う．並行，コンテキストコンサーンは組み込みシステム全体に横断し，実時間，耐故障コンサーンは，センサ (Sensor)，アクチュエータ (Actuator)，センサアクチュエータ (SensorActuator) に横断する [1]．

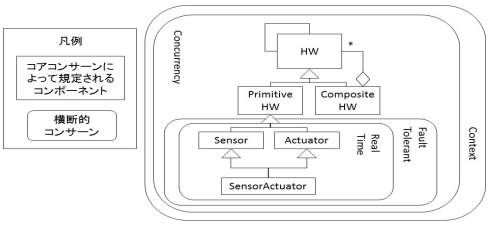

図 1　コアコンサーンと横断的コンサーンとの関係の概略

2.2　PBR パターン

本研究では，江坂らが提唱したアーキテクチャパターンである PBR パターン [1] を採用する．図 2(a)，(b) に PBR パターンの静的構造および動的振舞いの概要を示す．Object 間のメッセージを横取りし，コンテキストの変化を含むポリシー (Policy) に応じて，ファクトリ (Factory) が変化する再構成後のオブジェクト群を代表するアスペクトオブジェクト (AspectObject) のインスタンスを生成させ，このインスタンスにメッセージを送る．

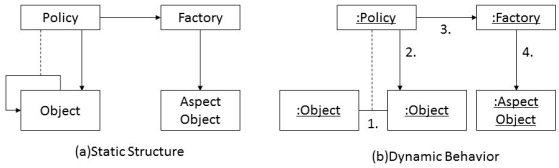

図 2　PBR パターン

3　事例

本研究では介護ベッドを事例として，提案しているアーキテクチャに基づき設計を行い，安全なソフトウェアの開発におけるアーキテクチャの有効性および課題を考察する．

3.1　介護ベッドの基本構造

介護ベッドは Web ページ [2][3] を参考にした．本研究で取り上げる介護ベッドの基本構造を図 3 に示す．

基本動作は背上げ，膝上げ，高さ調整として，各動作をするためのモーターが 1 つずつ，計 3 つのモーター群として備えられている．センサは，光センサ，人感センサ，バイタルセンサ [4]，超音波センサを用い，センサから取得した情報に応じて動作を変化させる．アクチュエータは，モーター群，フットライト [5]，スピーカーで構成し，機能に応じて稼働させる．

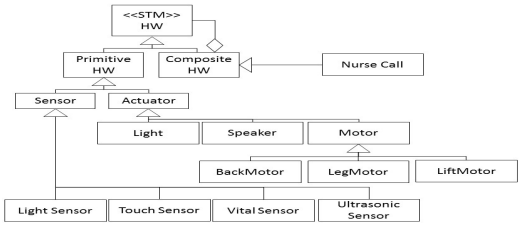

図 3 介護ベッドの基本構造 (コアコンサーン)

3.2 介護ベッドの安全性

介護ベッドの安全性として，センサから取得した情報が異常な値を検知したさいに，人体の安全を守る機能を追加する必要があると考察した．本研究では，その異常時動作を以下に示す．

- モーターの停止
- ナースコールを通じてナースセンターへの通知

3.3 PBR パターンの適用

PBR パターンを適用し，正常時動作と異常時動作の介護ベッドのコンテキストコンサーンを図 4，5 に示す．

コンテキストは人やモノ，周辺の環境の変化を表すので，センサから取得した環境の変化を表す物理量 (照度，熱量，バイタル値，距離) が考えられ，それらはポリシー (Policy) に相当する．それらのコンテキストに応じたアクションを振舞い活性化手続き (BehaviorActivator) により，STM-Family に組み合わせて，状態遷移機械 (STM) としてハードウェアを構築させる．

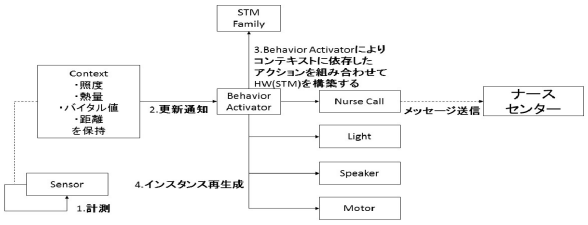

図 4 正常時動作の介護ベッドのコンテキストコンサーン

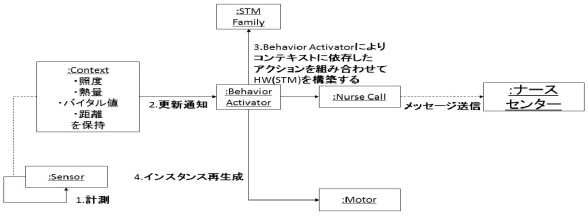

図 5 異常時動作の介護ベッドのコンテキストコンサーン

コンテキスト指向において PBR パターンを用いることで，仕様変更時にコンテキストに応じた動作をするためのコンポーネントの呼出しおよびアクション部分の記述を変更するだけでいいので，コードレベルの変更が容易である．

4 考察

4.1 安全なソフトウェア開発におけるアーキテクチャの有効性

安全なソフトウェアは正常時のときでも異常時のときでも人間や環境に危害を与えることなく動作しなければならない．仕様変更時に，万が一変更漏れ等があった場合，動作が正しく実行されない可能性が考えられるので，安全性が低下する．そこで PBR パターンを適用し，コンテキストアウェアで実現することで，変更すべき記述が規定されるので，コードが標準化され，コンテキストごとに適切に横断的コンサーンを分離し，独立して変更が容易になり，安全性を損なうソフトウェアの不具合が起きにくくなる．

4.2 安全なソフトウェア開発におけるアーキテクチャの課題

安全なソフトウェアは正しい動作だけでなく，決められた制約の範囲内で動作しなければならない．本研究の事例においては，リアルタイム性に関しては考慮していない．そのため万が一異常時動作の動作時間が長引いたり，停電時等の非常事態に陥ると，安全性が低下する恐れがあると考えられるので，安全性を保証すべき機能 (異常時動作等) はリアルタイム性と関連付けて考慮する必要がある．

5 おわりに

本研究では，介護ベッドを事例にあげ，組込みシステムのためのアスペクト指向アーキテクチャに適用，分析した結果，安全性を考慮したソフトウェア開発に関する有効性および課題を考察した．今後の課題として，他の事例を取り上げた場合の安全なソフトウェアの有効性および課題の発見が挙げられる．

参考文献

[1] 江坂篤侍，野呂昌満，沢田篤史，谷口弘一，繁田雅信，“コンテキストアウェアネスを考慮した組込みシステムのためのアスペクト指向アーキテクチャの設計，” ソフトウェア工学の基礎ワークショップ (FOSE2017) 論文集，pp.3-12，2017.

[2] パラマウントベッド株式会社，“パラマウントベッド株式会社—PARAMOUNT BED，” http://www.paramount.co.jp/，2017.

[3] フランスベッド株式会社，“フランスベッド株式会社-FRANCE BED，” http://www.francebed.co.jp/，2017.

[4] 株式会社ミオ・コーポレーション，“非接触バイタル生体センサー，” https://www.mio-corp.co.jp/sensor/，2000.

[5] 株式会社プラッツ，http://www.platz-ltd.co.jp/，2017.