ロボティックベッド®のソフトウェアレス機能安全設計・評価

Softwareless Functional Safety Design and Evaluation for Roboticbed

○久米 洋平 塚田 将平 河上 日出生 (パナソニック)

Yohei KUME, Panasonic, kume.youhei@jp.panasonic.com

Shohei TSUKADA, Panasonic.

Hideo KAWAKAMI, Panasonic

In the new ISO safety standard for personal care robots (ISO 13482), a safety related control system of a personal care robot shall be developed based on functional safety. It is very difficult to carry out such a development, especially including software system, which needs a lot of man-hours. Therefore, we have developed the prototype of the softwareless safety related control system for transfer assist robot "Roboticbed". In this paper, we introduce a summary of them.

Key Words: Personal Care Robot, Functional Safety, Performance Level

1. はじめに

生活支援ロボットの国際安全規格 ISO 13482[1]がついに発行された。生活支援ロボットの商品化には、本規格の安全要求事項への適合が求められるが、その適合に向けた最重要課題は本規格の核となる機能安全への対応である。

ISO 13482 では、制御システムを用いてリスク低減を行う場合には、ISO 13849-1[2]と IEC 62061[3]のいずれかの機能安全規格に従うことが要求されている。機能安全規格は非常に難解な規格であり、対応には多大な開発工数を必要とする。特に、安全関連部にソフトウェアを有する場合には、V 字モデルに基づく設計・検証・妥当性確認、要件のトレーサビリティ管理等、ハードウェアに比べて対応すべきボリュームが大きいため、機能安全対応の大きな負担となる。

そこで筆者らは、現在開発を進めている移乗支援ロボット「ロボティックベッド」(図 1) [4]の「ホールドツーラン機能」(車いす部の合体・分離移動動作を安全に実現するための安全機能) [5]を、ソフトウェアを用いずにハードウェアのみで構成する試み(試作・評価)(適用規格: ISO13849-1)を行なった。本稿では、その概要を報告する。

2. ホールドツーラン機能

図 1 に示すように、ロボティックベッドは、電動ケアベッドと電動車いすを融合したロボット介護機器であり、車いす部がベッド部に合体した状態では電動ケアベッドとして、車いす部がベッド部から分離した状態では電動車いすとして利用することができる。

ベッド・車いす間の合体・分離動作は、車いす部が自動で位置・姿勢を調整して行われるが、進行方向に第三者が誤って進入すると、車いす部への衝突やベッド・車いす間への挟まれ等の危害が発生する可能性がある。

そこで、このような危害の発生確率を低減させるために、ロボティックベッドでは、合体・分離動作を行うためのホールドツーラン機能(安全確認型のリスク低減手段)を搭載している[5]。すなわち、ホールドツーランスイッチ入力があるときのみ合体・分離動作を許可(動力源 ON)し、ホールドツ

Fig.1 : Prototype of Roboticbed

ーランスイッチ入力がないときは、合体・分離動作を確実に停止(動力源 OFF)する安全機能である。機能安全規格に基づく設計・評価により、高い安全性を有する(単位時間当たりの危険側故障発生率の平均確率を低く抑えた)ホールドツーラン機能を実現している。

3. ハードウェアによるホールドツーラン機能の実現

3.1 概略仕様

本稿では、従来ソフトウェアを用いて実現していたホールドツーラン機能を、ソフトウェアを用いずに、ハードウェアのみで構成する試みを行なった。従来のソフトウェアを用いて実現したホールドツーラン機能の制御ブロック図を図 2 (a)に、ソフトウェアを用いずにハードウェアのみで実現したホールドツーラン機能の制御ブロック図を図 2 (b)に示す。

今回試作したハードウェアのみによる安全機能(適用規格: ISO13849-1)では、基本機能として、ホールドツーランスイッチ入力があるときは動力源を ON (SSR を ON) し、ホールドツーランスイッチ入力がないときは、500ms 後に動力源を OFF (SSR を OFF) する機能を実装した。また、診断機能として、ホールドツーランスイッチの初期故障を検出する機能と、オフディレイタイマー(500ms)の初期故障を検出する機能を実装した。

「ロボティックベッド」および「Roboticbed」は、パナソニック株式会社の日本国内における登録商標

3.2 FMEDA

試作した安全機能の安全性能レベルを評価するに当たり、事前準備として FMEDA (Failure Modes, Effects and Diagnostic Analysis) を行った。

FMEDA では、ハードウェアの全コンポーネントに対する故障モードとその影響分析を行うと共に、全コンポーネントの単位時間当たりの故障率 λ [1/h]及び自己診断率 DC[%]等から、 λ_S (安全側故障率)・ λ_D (危険側故障率)・ λ_{DD} (自己診断により検出可能な危険側故障率)・ λ_{DU} (自己診断により検出不可可能な危険側故障率)を算出した。故障率は MIL-HDBK-217[6]の値を使用した。故障モードの比率は、IEC 62061 の Annex D に記載の値を使用し、記載のないコンポーネントの比率は等分とした。

以下、実施した FMEDA の結果を用いて、ISO 13849-1 に基づくパフォーマンスレベル評価 (安全性能レベル評価)を行った。

3.3 ISO 13849-1 に基づくパフォーマンスレベル評価

ISO 13849-1 に基づくパフォーマンスレベル評価を行った結果、試作したハードウェアのみによる安全機能は、パフォーマンスレベルは PL b (IEC 62061 の SIL1 相当) という評価結果になった。以下に、実際に評価に使用した 4 つのパラメータ (a)Category, (b)MTTFd, (c)DC_{avg}, (d)CCF) の結果を示す。
(a)Category (アーキテクチャにより、カテゴリ B, 1, 2, 3, 4 の 5 通りに分類される)

冗長度は一重系であり、基本安全原則を用いて設計したため、**カテゴリ B** となった。ただし、今回は試作のため、「製造、選択、組立に関する要求事項」は考慮していない。

(b)MTTFd (Mean Time To Dangerous Failure : 危険側故障を生じるまでの平均時間の期待値) (単位 : year)

式(1)に基づき、システム全体の MTTFd を計算した結果、MTTFd は 100[year]以上となった。MTTFd は最大 100[year]であるため、最終的には MTTFd=100[year]となった。

ISO 13849-1における MTTFd の 3つの分類 (High : 30[year] ≤ MTTFd ≤ 100[year], Medium : 10[year] ≤ MTTFd < 30[year], Low : 3[year] ≤ MTTFd < 10[year]) から、本安全機能は **MTTFd = High** となった。

$$MTTF_d = \frac{1}{1/MTTF_{d1} + 1/MTTF_{d2} + \dots + 1/MTTF_{dN}}$$

$$= \frac{1}{(\lambda_{d1} + \lambda_{d2} + \dots + \lambda_{dN}) \times 24 \times 365} \quad (1)$$

(c)DC_{avg} (Average Diagnostic Coverage : 検出される危険側故障率と全危険側故障率の間の比の平均値) (単位 : %)

カテゴリ B の場合、自己診断は要求されていないため、今回は DC_{avg} の計算は実施しなかった。DC_{avg} の計算が必要な場合は、式(2)に基づき、DC_{avg} の計算を行う。

$$DC_{avg} = \frac{DC_1 / MTTF_{d1} + DC_2 / MTTF_{d2} + \dots + DC_N / MTTF_{dN}}{1/MTTF_{d1} + 1/MTTF_{d2} + \dots + 1/MTTF_{dN}}$$

(a)With Software

(b)Without Software

Fig.2 : Control block diagram of hold-to-run function

$$= \frac{DC_1 \lambda_{d1} + DC_2 \lambda_{d2} + \dots + DC_N \lambda_{dN}}{\lambda_{d1} + \lambda_{d2} + \dots + \lambda_{dN}} \quad (2)$$

(d)CCF (Common Caused Failure : 共通原因故障)

カテゴリ B の場合、共通原因故障への考慮は要求されていないため、今回は CCF 評価は実施しなかった。共通原因故障への考慮が必要な場合は、ISO 13849-1 の Table F.1 に基づき採点を行い、65 点以上が必要となる。

3.4 考察

上述の評価結果から、ハードウェアのみで安全機能を実現する場合の指針について、カテゴリをベースに考える。

カテゴリ B の場合、“最小限の関連規格への適合”、“基本安全原則の適用”、“MTTFd=Low~Medium”が要求されているが、“診断機能なし”、“(一重系の場合) 共通原因故障 (CCF) への考慮不要”でよい。そのため、ハードウェアのみでも比較的容易に要求事項 (最大 PL b まで) を満たすことができると考える。今回試作したハードウェアのみによる安全機能もこのパターンである。

カテゴリ 1 の場合、カテゴリ B の要求事項に加えて、さらに“十分吟味されたコンポーネントの採用”、“十分吟味された安全原則の適用”、“MTTFd=High”が要求されているが、こちらも“診断機能なし”、“(一重系の場合) 共通原因故障 (CCF) への考慮不要”でよい。そのため、注意して“十分吟味されたコンポーネントの採用”、“十分吟味された安全原則の適用”を行い、信頼性の高い部品を採用すれば、ハードウェアのみでも要求事項 (最大 PL c まで) を満たすことができると考える。

一方、カテゴリ 2 の場合、カテゴリ B の要求事項に加えて、

さらに“十分吟味された安全原則の適用”、“MTTFd=Low～High”、“ DC_{avg} =Low(60[%]以上)～Medium(90[%]以上)”、“共通原因故障(CCF)への考慮”が要求されている。カテゴリ B, 1 では要求されていなかった診断機能, CCF 考慮が必要になっている。特に、“ DC_{avg} =Low～Medium”に注意が必要であり, ハードウェアのみでこれを実現するのは非常に困難であると考え(もし要求事項を満たすことができれば, 最大 PL d まで可能であるが)。

以上より, ハードウェアのみで安全機能を実現する場合は, カテゴリ B (最大 PL b まで実現可能), あるいは, カテゴリ 1 (最大 PL c まで実現可能)を目指すのが現実的であると考え。言い換えれば, 要求パフォーマンスレベル $PLr=b$, $PLr=c$ の安全機能を設計する場合は, ハードウェアのみで実現することが可能であり, その場合, ソフトウェア開発工数を大幅に削減できるものとする。

4. おわりに

本稿では, ロボティックベッドのホールドツーラン機能(安全関連制御システム)を, ソフトウェアを用いずにハードウェアのみで構成する試み(試作・評価)(適用規格:ISO13849-1)を行なった。パフォーマンスレベル評価(安全性能レベル評価)を実施した結果, PL b (IEC62061 の SIL1 相当)を実現することができた。これにより, 開発工数の大きいソフトウェア開発を不要にすることができた。

なお, この成果の一部は, 独立行政法人新エネルギー・産業技術総合開発機構(NEDO)の委託業務の結果得られたものである。

参 考 文 献

- [1] ISO13482:2014, Robots and robotic devices - Safety requirements for personal care robots
- [2] ISO 13849-1:2006, Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- [3] IEC 62061:2005, Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- [4] 久米洋平, 河上日出生, 塚田将平, 中村徹, "ロボティックベッドの開発", 自動車技術, vol.64, No.5, pp.31-34, 2010.
- [5] 久米洋平, 下田智大, 太田章博, 塚田将平, 河上日出生, 本田幸夫, "ロボティックベッドの安全技術", 日本ロボット学会誌, Vol.31, No.8, pp.797-803.
- [6] MIL-HDBK-217F Notice2 (電子機器の信頼度予測 - 米軍用ハンドブック-), (社) 関西電子工業振興センター 信頼性分科会