

組込みシステムにおける並列型状態遷移図に基づく安全分析手法

金周慧[†] 松原豊[†] 高田広章[†]

組込みシステムにおける故障の影響を、より網羅的に分析するため、我々は、状態遷移図を対象とした安全分析手法を提案している。本論文では、直交する複数の状態遷移図（並列型状態遷移図）で表現されるシステムを対象とした安全分析手法 SAPSTD (Safety Analysis method based on Parallel State Transition Diagrams) を提案する。提案手法を用いることで、直交する状態遷移図のうち、一部の状態遷移図における逸脱を分析すれば、他の状態遷移図の状態に関係なく故障の深刻度が定まる場合に、分析数を減らすことができる。小規模な組込みシステムを対象に提案手法を適用し、提案手法の有効性を明らかにする。

Safety analysis method based on parallel state transition diagram for embedded systems

ZOOHAYE KIM,[†] YUTAKA MATSUBARA[†] and HIROAKI TAKADA[†]

In order to analyze effects of failures exhaustively in safety critical embedded systems, we have studied safety analysis methods based on state transition diagrams. However, guide-words and an analytical sheet used in these methods are not suitable for analyzing parallel state transition diagrams, which represent the behavior of a system whose functions work in parallel. In the case that the severity of a deviation on a state transition diagram can be determined regardless of the other state transition diagrams, the total number of deviations to be analyzed would be reduced by using the proposed method. To clarify the effectiveness of the proposed method, we applied a conventional method and SAPSTD for analysis of specifications of a sample embedded system and compared the results of them.

1. はじめに

近年、飛行機や自動車などの組込み制御システムが複雑化の中で、従来確保してきた安全性を維持・向上することが求められている。システムの安全性を確保するためには、システムの安全性を損なう故障とその要因を抽出する安全分析が重要である。従来の組込みシステムでは、システムの安全を左右する安全関連システムにソフトウェアが含まれていない場合や、含まれていても小規模である場合が多く、その安全分析は比較的容易であった。それに対して、飛行機や自動車などの組込みシステムでは、特にソフトウェアの大規模化が顕著になっていることから、ソフトウェアに対する安全分析において、ソフトウェアの不具合と、ハードウェア故障によるソフトウェア動作への影響を、網羅的に列挙することは困難な状況にある。それにも関わらず、ソフトウェアに対する安全分析手法が十分に確立していないのが現状である。

組込みシステム開発の約 8 割のプロジェクトでは、状態遷移図や状態遷移表が用いられていることが知られている¹⁾。状態遷移図を対象にした安全分析手法を用いると、多くの組込みシステムの分析に適用できることに加えて、分析の専門家以外の技術者も安全分析に参加し易くなるという利点がある。

我々は、状態遷移図を用いてモデル化された組込みシステムの安全分析を行うため、状態遷移図に着目した安全分析手法 SASTD (Safety Analysis method based on State Transition Diagram)²⁾ を提案し、状態遷移図の逸脱を列挙するためのガイドワードを用いることで、FMEA に比べてより網羅的に分析できることを示した。また、階層型状態遷移図に基づく安全分析手法 SAHSTD (Safety Analysis method based on Hierarchical State Transition Diagram) を提案し³⁾、同一の性質をもつ状態を階層的に整理することで、SASTD に比べてより効率よく分析できることを示した。

システムは、割り込み処理やエラーチェックなど複数の処理が同時に動作するものが多い。このようなシステムは並列型状態遷移図でモデル化できる。しかし、

[†] 名古屋大学大学院情報科学研究科
Graduate School of Information Science, Nagoya University

SASTD と SAHSTD の分析シートは、並列に動作する複数の状態遷移図には向かない。本論文では、並列型状態遷移図を対象とした安全分析手法 SAPSTD を提案する。SAPSTD では、逸脱を列挙する再、並列に動作する他の状態遷移図の状況を考慮することで、システムに対する逸脱の影響を分析できる。SAPSTD の適用性を確認するため、話題沸騰ポット⁴⁾を題材に、システム仕様に対して SAPSTD を適用し、SASTD の分析結果と比較する。

2. 関連研究

HAZOP (HAZards and Operability Analysis)⁵⁾は、主に化学プラントにおける、製品の製造工程に適用され、温度や流量などが正常な範囲からずれるという逸脱を、ガイドワードを用いて列挙する。ソフトウェアに適用することは想定していないため、more, less などのガイドワードが、ソフトウェアに対する分析には向いていない。STPA (STAMP - Based Process Analysis)⁶⁾は、システム内部もしくはシステム間における情報の流れに着目して分析しており、システムの状態に対する逸脱を分析することは困難である。表 1 は、SASTD と SAPSTD の分析できる範囲を示す。例えば、並列に動作する 2 つの状態遷移図があるとする。直交している状況の部分は正しく動作する、逸脱の部分は状態または状態遷移が逸脱することを考える。ある状態遷移図の状態に対する逸脱を分析する際に、他の状態遷移図では、状態遷移が発生している状況を分析するのが困難であるという問題がある。

3. SAPSTD

SAPSTD は、並列型状態遷移図に記述された、各状態で満たすべき性質と、状態が遷移する際に実行される処理に対して、それらが正常に満たされない、もしくは実行されないという逸脱を、状態遷移図における逸脱として、ガイドワードを用いて、より網羅的に列挙する手法である。並列型状態遷移図で表現できるシステムであれば、その規模に依らず適用可能である。

3.1 対象とする階層型状態遷移図

状態遷移図には、システムの状態と、システム状態間の遷移関係が記述されている。システムの各状態で

表 1 SASTD と SAPSTD の分析できる範囲
Table 1 Analyzable range for SASTD and SAPSTD.

直交する状態遷移図の状況 逸脱の分析対象	状態		状態遷移	
	SASTD	SAPSTD	SASTD	SAPSTD
状態	○	○	×	○
状態遷移	○	○	○	○

満たさせるべき性質は、仕様もしくは設計で規定されるものとする。状態遷移に対しては、状態を遷移する条件(イベント)と、イベントが発生して状態が遷移する際に実行される処理(アクション)が規定されるものとする。本論文は、ミーリー型 (Mealy Machine)⁷⁾の並列型状態遷移図の定義に従い、システムの状態と、システム状態間の遷移関係が記述される。また、状態遷移図は正しく作成されていることを前提とする。

3.2 分析の手順

SAPSTD の分析手順は、図 1 のように行われる。まず、話題沸騰ポットで想定できるグローバル影響と深刻度を定義する。次に、状態に対する分析を行い、状態遷移に対する分析を行う。許容できない深刻度をもつ逸脱に対しては、安全対策を検討する。

3.3 並列層型状態遷移図に対する逸脱の分析

SAPSTD は、並列型状態遷移図に記述された、各状態で満たすべき性質と、状態が遷移する際に実行される処理に対して、それらが正常に満たされない、もしくは実行されないという逸脱を、ガイドワードを用いて、より網羅的に列挙する手法である。

図 2 は、図 1 の状態に対する分析(1)と状態遷移に対する分析(2)の詳細な分析手順である。一つの逸脱を分析し、現在の状況(1)(2)だけで、グローバル影響が決まったら、グローバル影響が定義されているかを確認し、深刻度を決定する。定義されていなかったら、グローバル影響と深刻度の定義に追加する。これを全ての逸脱について繰り返し行う。逸脱を分析する作業は、分析シートに従う。

ガイドワードは文献²⁾と同じである。状態に対する分析では、表 2 に示すガイドワードと属性の組み合わせから逸脱を考える。次に、状態遷移に対する分析でも、表 3 に示すガイドワードから逸脱を考える。

これらのガイドワードと属性は、より多くの状態遷移図に適用できるよう定めたが、分析対象のシステムによっては、これら以外のガイドワードを定めて分析

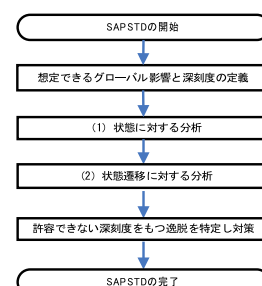


図 1 SAPSTD の分析手順

Fig. 1 Analysis flow in SAPSTD.

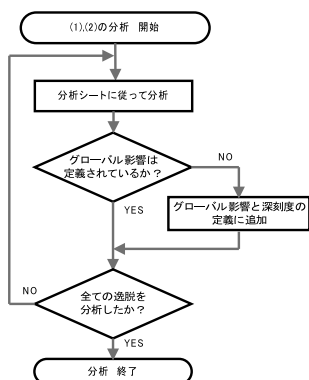


図 2 状態と状態遷移に対する分析の手順
Fig. 2 Analysis flow for states and state transitions.

する方が、より分析し易くなることもあると思われる。

3.4 逸脱に対する分析項目

図 2 で、逸脱の分析シートでは、1つの逸脱に対して、9つの項目を順番に検討する。1つ目は、逸脱を識別するための ID 番号である。2つ目は、分析対象である仕様を記述する。3つ目は、逸脱の内容を、ガイドワードと属性と共に逸脱を記述する。4つ目は、逸脱によるシステム内部動作への影響をローカル影響に記述する。5つ目は、直交する他の状態遷移図の状態/状態遷移について記述する。6つ目は、逸脱によるシステム全体、もしくはシステム利用者に対する影響を、グローバル影響に記述する。7つ目は、グローバル影響の深刻さを示す評価値を深刻度に記述する。深刻度は、安全分析の前もしくは進める中で、システムの利用状況とグローバル影響をシステムに求められる安全性、コスト制約などを踏まえてシステム開発者が決定する。8つ目は、逸脱が発生した原因を記述する。9つ目は、逸脱の発生そのものを防ぐ対策、もしくは深刻度を低減するための対策を記述する。本論文では、発生確率の大小に関わらず、すべての逸脱を列挙し、危害の発生を許容できるかどうかを判断する際には、深刻度のみを用いることにする。

4. 適用事例

SAPSTD の有効性を確認するため、架空の組込みシステムである SESSAME の話題沸騰ポット⁴⁾を対

表 2 状態に対する逸脱
Table 2 Guidewords for derivation of deviations on states.

ガイドワード	属性	解釈
Value	-	値が正しくない。
More	transition	イベントが発生していないにもかかわらず、状態が遷移する。

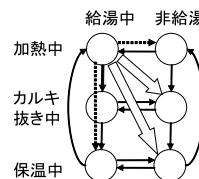


図 3 組み合わせ状態遷移図における逸脱
Fig. 3 Deviations for the combinational state transition diagram.

象に安全分析を実施した事例を述べる。同じシステムに対し組み合わせ状態遷移図でも分析を実施し、分析結果を比較する。2節の表 1 の状態遷移での逸脱を分析するときに、直交する状態遷移図の状況の状態の部分のみ分析する。直行する状態遷移図で状態遷移が発生するときの分析は、今回は逸脱の範囲を同じにするため、図 3 で、白い矢印の部分の逸脱の分析対象から除き、点線の部分のみ逸脱を考慮する。

4.1 話題沸騰ポット

話題沸騰ポットは、設定した温度まで、お湯を加熱する機能をもつ架空の機器である。ポットにお湯を入れて、温度を設定し沸騰スイッチを押すと加熱を開始する。加熱する間は沸騰ランプが点灯し、保温ランプは消灯する。加熱開始から 3 分経過すると、カルキを抜き保温する。保温したら、沸騰ランプは消灯し保温

表 3 状態遷移に対する逸脱
Table 3 Guidewords for derivation of deviations on state transitions.

ガイドワード	属性	解釈
No	transition	イベントは正しく検出できたが、状態が遷移せず、実行されるべきアクションもすべて実行されない。
Incorrect		間違った状態に遷移し、実行されるべきではないアクションが実行される。
Early		想定したタイミングより早く状態が遷移し、実行されるべきアクションが実行される。
Late		想定したタイミングより遅く状態が遷移し、実行されるべきアクションが実行される。
More	action	正しい状態に遷移し、実行されるべきアクションはすべて正常に実行されるが、余分なアクションも実行される。
Incorrect		正しい状態に遷移するが、実行されるべきアクションの代わりに、実行されるべきではないアクションも実行される。
Missing		正しい状態に遷移するが、実行されるべきアクションのうち、実行されないアクションが存在する。

ランプは点灯する．提案手法は，給湯ボタンを押せば，いつでも給湯できるように仕様を変更し，分析を行う．

話題沸騰ポットのシステム仕様を図4に示す．動作中の仕様を作成するとき，2つの案がある．案1は，並列の動作を意識した場合の仕様である．案2は，並列の動作を意識していない場合で，状態の組み合わせによって作成する仕様である．本論文では，これらのシステム仕様から，並列型状態遷移図と，組み合わせ状態遷移図を作成し，その分析結果を比較する．図5に，並列型状態遷移図を示す．上位の動作中は，内部に並列動作する状態遷移図が存在する．給湯モードでは，給湯ボタンが押されたら給湯中状態，離れたら非給湯状態になる．加熱モードでは，沸騰ボタンを押したら加熱中状態，沸点到達したらカルキ抜き中状態，沸騰完了したら保温中状態になる．案2のシステム仕様から作成した組み合わせ状態遷移図を図6に示す．

4.2 グローバル影響と深刻度の定義

話題沸騰ポットにおけるグローバル影響とその深刻度を，作業者の安全性とお湯の状態の観点から，表4のように定義した．作業者の安全性を確保するためにもっとも避けるべき状況は，ユーザが意図していないタイミングに，高温のお湯が出てしまうと，作業者が

< 上位 >

- (H.1) アイドル状態で，ユーザがポットに水を入れて，ポットの蓋を閉めると，動作中状態になる．
- (H.2) アイドル状態でエラーを検知すると，エラー状態になる．
- (H.3) 動作中状態で空焚きになると，アイドル状態になる．
- (H.4) 動作中状態でエラーを検知すると，エラー状態になる．

< 下位：動作中 >

案1：並列に動作

-加熱モードの状態遷移

- (A.1) 加熱中状態で沸点到達すると，カルキ抜き中状態になる．
- (A.2) カルキ抜き中状態で沸騰処理完了すると，保温中状態になる．
- (A.3) 保温中状態で沸騰要求すると，加熱中状態になる．

-給湯モードの状態遷移

- (B.1) 給湯中状態で非給湯要求すると，非給湯状態になる．
- (B.2) 非給湯状態で給湯要求すると，給湯中状態になる．

案2：組み合わせ

- (C.1) 給湯中の加熱中状態で沸点到達すると，給湯中のカルキ抜き中状態になる．
- (C.2) 給湯中のカルキ抜き中状態で沸騰処理完了すると，給湯中の保温中状態になる．
- (C.3) 給湯中の保温中状態で沸騰要求すると，給湯中の加熱中状態になる．
- (C.4) 非給湯の加熱中状態で沸点到達すると，非給湯のカルキ抜き中状態になる．
- (C.5) 非給湯のカルキ抜き中状態で沸騰処理完了すると，非給湯の保温中状態になる．
- (C.6) 非給湯の保温中状態で沸騰要求すると，非給湯の加熱中状態になる．

図4 話題沸騰ポットのシステム仕様

Fig. 4 System specification of the electric boiling pot.

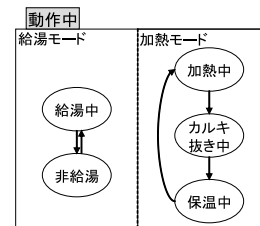


図5 話題沸騰ポットの並列型状態遷移図

Fig. 5 A parallel state transition diagram of the electric boiling pot.

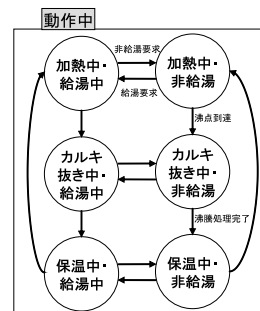


図6 組み合わせ状態遷移図

Fig. 6 A combinational state transition diagram of the electric boiling pot.

ボタンを操作する際に触れて，火傷を負う状況であると考え，このときの深刻度を最も高い9とした．設定された温度のお湯を正しく給湯できる好ましい状況の深刻度は0とした．なお今回の分析では，沸騰していないお湯の温度は，火傷をしない低温であると仮定している．深刻度の定義においては，グローバル影響の相対的な関係を明確にして，システムとして許容できる危害の範囲を明確にすることが重要である．したがって，深刻度の絶対値には特別な意味はない．

4.3 安全分析の方針

話題沸騰ポットに求められる安全性は，システムがどんな誤動作をしても作業者が火傷しないことを保障することと，作業者がボタンを押していないのに，お湯がでることを防ぐことである．そこで，システムとして許容できる深刻度は6以下であるとした．安全分析の結果，7以上の深刻度をもつ危害を発生させる逸脱に対しては，6以下に低減する対策を検討する．

本論文では，安全分析を実施するにあたり，5つの前提をおく．1つ目は，作業者の操作ミスは考慮しないことである．現実的な安全分析においては，作業者の操作ミスを考慮する必要があるが，分析の範囲を限定するため，システムの逸脱のみを分析する．2つ目は，多重故障は，発生確率が十分低いと想定して考慮しないことである．3つ目は，図5に示した情報

表 4 グローバル影響と深刻度の定義
Table 4 Definitions of global effects and severities.

グローバル影響		定義	深刻度
作業者の安全性	お湯の状態		
火傷を負う	沸騰したお湯がでる	ユーザが意図していないタイミングに、高温のお湯がでる。	9
火傷をしない	沸騰していないお湯がでる	ロック中状態で、ユーザが意図していないタイミングに、低温のお湯がでる。	8
火傷をしない	沸騰していないお湯がでる	ユーザが意図している時に、設定された温度になっていないまま、給湯する。	7
火傷をしない	沸騰されない/保温されない	沸騰したいけど、沸騰できない/保温したいけど、保温できない。	6
火傷をしない	給湯できない	ポンプが閉まっていて、給湯したいけど、給湯できない。	5
火傷をしない	沸騰されない/保温されない	逸脱を検出する(安全側故障)。	4
火傷をしない	保温される	作業者の意思で沸騰を中止する/カルキが十分に抜かれないまま保温になる。	3
火傷をしない	沸騰される/保温される	カルキ抜きが2回行われている/ランプは故障したが、沸騰と保温に影響はない。	2
火傷をしない	沸騰される/保温される	沸騰完了する。	1
火傷をしない	沸騰完了する	設定された温度のお湯を給湯できる。	0

は、全ての分析者が利用できるものとする。4つ目は、Incorrect transition は、状態遷移の方向に関係なく、遷移関係のある状態を対象に考える。5つ目は、分析の範囲を狭めるために、アクションとして複数の処理が規定される場合には、それらの実行順番が変わってもシステムとして正しく動作するものとする。

4.4 SAPSTD による分析

話題沸騰ポットの並列型状態遷移図に対して SAPSTD を適用したときの分析例として、分析の内容と分析数を数える方法についていくつか説明する。

表 5 の ID1 番は、「(A.1) 加熱中状態で、～」である。逸脱は、表 2 の No transition を適用し「カルキ抜き中状態に遷移しない」という逸脱を分析している。ローカル影響は、加熱中状態が続くと、水が蒸発して空焚きになる可能性があるが、水位センサにより、空焚きを防止する機能によって、アイドル状態に遷移する。直交する状態遷移図の状態/状態遷移は、給湯中と非給湯に分けられるが、ローカル影響の深刻度は低いので、これ以上分析を進める必要はない。このように、ローカル影響のみで、深刻度を判断できる場合は、分析数を 1 個と数える。ID7 番は、Incorrect action を適用し「加熱中状態で、～」という逸脱を分析している。ローカル影響は、2 つある。1 つ目は、ユーザが意図している時に、設定された温度になっていないまま、給湯する。直交する状態遷移図の状態は、給湯中になる。グローバル影響は、火傷をしない。深刻度は 7 になる。2 つ目は、ユーザが意図していないタイミングに、低温のお湯がでる。直交する状態遷移図の状態は、非給湯になる。グローバル影響は、沸騰されないお湯がでるので、火傷をしない。深刻度は 8 になる。この逸脱の分析は、給湯中と非給湯の分析まで行い、深刻度を定めることができる。つまり、グローバル影響が直交している他の状態に依存する給湯中と非給湯まで見ないと、深刻度を判断できないので、ID1

番の分析結果とことなり分析数を 2 個と数える。

組み合わせ状態遷移図の分析は、表 6 に示す。詳しい分析方法の説明は文献²⁾を参照する。

4.5 分析結果に関する考察

表 7 は、話題沸騰ポットに対して SAPSTD と SAPSTD による逸脱数の比較した数を示す。深刻な危害をもたらす逸脱は、一致することが確認できた。よって、組み合わせ状態遷移図の分析で分析可能な逸脱は、SAPSTD でも分析可能であることを確認した。表 7 において、組み合わせ状態遷移図の分析の「分析した逸脱数」は、実際に逸脱を分析した数を示している。状態の分析数は 36 個、状態遷移の分析数は 144 個であった。「対策が必要な分析数」は、深刻度が 7 以上の逸脱の数を示している。状態の分析数は 5 個、状態遷移の分析数は 17 個であった。組み合わせ状態遷移図の分析で「分析した逸脱数」は合計 180 個であった。SAPSTD の「分析した逸脱数」は、状態は 36 個、状態遷移は 74 個であった。「対策が必要な分析数」は、状態は 10 個、状態遷移は 8 個であった。「直交による分析数」は、逸脱の分析数から直交により減る分析数を除いた深刻度を純粋に決定した分析数である。状態は 12 個、状態遷移は 49 個であった。SAPSTD で、「分析した逸脱数」は合計 110 個で、分析した逸脱数から、直交により減る分析数を除くと直交による分析数 61 個であった。

今回の事例では、表 5 の ID1 番のように、直交する状態遷移図のうち、一部の状態遷移図における逸脱を分析すれば、他の状態遷移図の状態に関係なく故障の深刻度が定まる場合に、分析数を減らすことができた。

5. おわりに

本論文では、並列に動作するシステムに対する安全分析手法を提案し、状態遷移図を並列化する安全分析を行うことで、システムの状態が同時に動作するとき

表 5 加熱モードの状態遷移に対する SAPSTD の分析結果の一部
Table 5 A part of results of SAPSTD for deviations on state transitions in heating mode.

ID	対象	逸脱	ローカル影響	直交する状態遷移図の状態 / 状態遷移	グローバル影響	深刻度	原因	対策
1	(A.1) 加熱中状態で、沸点到達すると、カルキ抜き中状態になる。	No transition カルキ抜き中状態に遷移しない。	pot-330-13 要件で、空焚きになった時はアイドル状態になる。 逸脱を検出する。	・給湯中 (ポンプ開) ・非給湯 (ポンプ閉)	-	4	-	-
7		Incorrect action 加熱中状態で、沸点到達すると、カルキ抜き中状態 (ヒータだけ OFF という逸脱) になる。	・ユーザが意図している時に、設定された温度になっていないまま、給湯する。 ・ユーザが意図していないタイミングに、低温のお湯がでる。	・給湯中 (ポンプ開) ・非給湯 (ポンプ閉)	・火傷をしない。沸騰していないお湯がでる。 ・火傷をしない。沸騰されない。	・7 ・8	ポンプの故障。	ポンプの二重化。

表 6 組み合わせ状態遷移図の分析結果の一部
Table 6 A part of results of analysis for deviations on the combinational state transition diagrams.

ID	対象	逸脱	ローカル影響	グローバル影響	深刻度	原因	対策
56	(C.4.a) 非給湯の加熱中状態で、沸点到達すると、非給湯のカルキ抜き中状態になる。	Incorrect action 非給湯の加熱中状態で、沸点到達すると、非給湯のカルキ抜き中状態 (沸騰ランプ ON, 保温ランプ OFF, ヒータ ON は正しく動作し、ポンプだけ開くという逸脱) になる。	・ユーザが意図していないタイミングに、高温のお湯がでる。 ・ポンプが開いてる。	・火傷を負う。 ・沸騰したお湯がでる。	9	ポンプの故障。	ポンプの二重化。

表 7 SASTD と SAPSTD による逸脱数の比較
Table 7 Comparison of the number of deviations analyzed by SASTD and SAPSTD.

	SASTD による組み合わせ状態遷移図に対する分析		SAPSTD による並列型状態遷移図に対する分析		
	分析した逸脱数	対策が必要な分析数	分析した逸脱数	対策が必要な分析数	直交による分析数
状態に対する分析	36	5	36	10	12
加熱モードの状態遷移に対する分析	78	9	54	6	33
給湯モードの状態遷移に対する分析	66	8	20	2	16
合計	180	22	110	18	61

の分析ができる。さらに、適用事例において、直交する状態の影響により分析する数を削減できることを明らかにした。システムの安全分析の網羅性をより向上させるためには、SAPSTD と複数の安全分析手法を組み合わせることで適用することが望ましいと考えられる。今後は、システム内の直交ではなく、他の直交している状態遷移図、例えば、システムの状態遷移図と作業者の状態遷移図にも適用したいと考えている。

参 考 文 献

- 1) 経済産業省, 組込みソフトウェア産業実態調査: プロジェクト責任者向け調査, 2010.
- 2) 金周慧, 松原豊, 高田広章, “状態遷移図に着目した安全分析手法”, “信学論, Vol.J95-A, No.2, pp.198-209, 2012.
- 3) 金周慧, 松原豊, 高田広章, “階層型状態遷移図に基づく安全分析手法”, “組込み技術とネットワークに関するワークショップ, 2012.
- 4) SESSAME, 話題沸騰ボット (GOMA-1015 型) 要求仕様書 第 7 版, 2005.
- 5) N.G. Leveson, Hazards and Operability Analysis, Safeware: System Safety and Computers, pp.335-341, Addison-Wesley, 1995.
- 6) T. Ishimatsu, N. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, H. Nakao, “Modeling and Hazard Analysis using STPA”, “Conference of the International Association for the Advancement of Space Safety, Huntsville, Alabama, May 2010.
- 7) D. Harel, “Statecharts: A visual formalism for complex systems”, pp.231-274, The Science of Computer Programming, 1987.