Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2

階層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[†]

小規模な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ことを目的に，１つの状態遷移図に基づく安全分析手法 SASTD（Safety Analysis method based on State Transition Diagram）を提案した．大規模な組込みシステムでは，１つの状態遷移図に含まれる状態数が多くなるため, SASTD で網羅的に分析するのが困難であるという問題がある．１つの状態遷移図に含まれる状態数を減らすためには，小規模な状態遷移図に分割した階層型状態遷移図を利用するのが有効である．本論文では，SASTD を拡張した，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）を提案する．SAHSTD を話題沸騰ポットのシステム仕様に対して適用した結果，SASTD と同一の逸脱を分析できることを確認した．さらに，同一の性質をもつ状態を階層的に整理することで，分析者が本質的に分析すべき逸脱数が，SASTD に比べて，状態に対する分析では 92 個から 61 個に，状態遷移に対する分析では 284 個から 134 個に削減できることが明らかになった．

Safety analysis method based on hierarchical state transition diagram

Zoohaye KIM[†], Yutaka MATSUBARA[†], and Hiroaki TAKADA[†]

In order to analyze exhaustively affects of failures in small embedded systems, we proposed SASTD (Safety Analysis method based on State Transition Diagram). SASTD assumes that system specifications of an embedded system have been modeled as only one state transition diagram. Therefore it is difficult that we analyze exhaustively the state transition diagram including many states and state transitions by using SASTD. In many cases, a hierarchical state transition diagram is used to reduce the number of states in a state transition diagram. In this paper, we propose SAHSTD (Safety Analysis method based on Hierarchical State Transition Diagram). We applied both SASTD and SAHSTD to the system specification of an electric boiling pot, and compared the results of them. Consequently, we confirmed that all deviations derived by SASTD could be also derived by SAHSTD. Since several system states with same characteristics were integrated to hierarchical system states, the number of derived deviations that analyzer must decide its severity could be reduced from 92 to 61 in the analysis for system states, and from 284 to 134 in the analysis for system state transitions, respectively.

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する中で，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．また，組込みシステムの設計においては，80%程度に状態遷移図もしくは状態遷移表が用いられている[1]．状態遷移図や状態遷移表を対象に安全分析を実施できる手法があると，より多くの組込みシステムに適用できるだけでなく，安全分析の専門家以外の技術者も分析活動に参加し易くなると考えられる．

従来から用いられている安全分析手法として，FMEA(Failure Mode and Effect Analysis) [2]，SFMEA[3]，HAZOP（HAZards and Operability Analysis）[4]，SHARD（Software Hazard Analysis and Resolution in Design）[5]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に適用可能な安全分析手法 SASTD を提案した[6]．SASTD は，状態遷移図を対象に，状態遷移図の各状態で満たされるべき性質が満たされないという逸脱と，状態が遷移する際に実行されるべき処理が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ための手法で，FMEA に比べて，より網羅的に分析できる．しかし，大規模なシステムでは，１つの状態遷移図に含まれる状態数が多くなるため，SASTD を適用し難いという問題がある．

本論文では，SASTD を拡張し，階層型状態遷移図を対象とした安全分析手法 SAHSTD を提案する．１つの状態遷移図に含まれる状態遷数を減らすため，状態遷移図を階層構造で表現することで，１つの状態遷移図を複数の小さな状態遷移図に分割できる．１つの状態遷移図に含まれる状態数を少なくした階層型状態遷移図に対して，SAHSTD を適用することで，より容易に安全分析ができる．SAHSTD の適用性を確認するため，話題沸騰ポット[7]を題材に，システム仕様に対して SAHSTD を適用し，SASTD と分析結果を比較する．その結果，SASTD と同等の安全分析結果が得られることに加えて，同じ性質をもつ状態に対する，重複した分析を省略することにより，SASTD に比べて本質的な分析量を減らすことができることを明らかにする．

2. 関連研究

状態遷移図に適用可能な安全分析手法を紹介する．SMHA（State Machine Hazard Analysis）[8] は，状態遷移図を対象に，初期状態から遷移可能なすべてのパスを網羅的に探索することで，深刻な危害をもたらす状態に遷移するパスを見つけ出す手法である．状態遷移図に，あらゆる障害が発生した場合の状態と，その状態へ遷移するパスが網羅的に記述されていることを前提としている．このような状態遷移図を作成す

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

Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2

るためには，まず，システムの故障や逸脱を分析し，その時のシステムの振る舞いを網羅的に状態遷移図に記述することが必要となる．SpecTRM（Specification Tools and Requirements Methodology）[9]は，解析評価のための基準となる有限状態遷移モデルである．ソフトウェアの内部で規定されたモードや状態変数の遷移条件の一貫性と遷移条件の網羅性の確認は可能であるが，状態で満たすべき性質の逸脱と，状態遷移する際に起きる逸脱については考慮しておらず，状態遷移図の網羅的な分析には向いていない．複数のサブシステムで構成されるシステムに対しては，従来の分析手法だけでは不十分であるという立場から STPA（STAMP‐Based Process Analysis）[10] が提案されているが，システム内部もしくはシステム間における情報の流れのみ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．

3. SAHSTD

3.1 分析手法の概要

SAHSTD は，階層型の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．階層型状態遷移図の上位と下位に分けて分析することにより，１つの状態遷移図に対して分析する状態数が減るため，分析が容易になる．逸脱により発生する危害の深刻度を分析した結果，許容できない深刻な危害をもたらす逸脱が存在する場合には，その逸脱に対して，許容可能なレベルまで危害の深刻度を低減する対策を検討する．

3.2 階層型状態遷移図に対する逸脱の分析

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．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．SAHSTD の手順は，以下の様に行われる．

（1）想定できるグローバル影響（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）と深刻度（深刻さを示す評価値）の定義
（2）上位の状態に対する分析
（3）上位の状態遷移に対する分析
（4）下位の状態に対する分析
（5）下位の状態遷移に対する分析
（6）（2）から（5）の分析をしながら，未定義のグローバル影響を追加

SAHSTD では，上位と下位の状態遷移図に記述された，状態遷移図に対する逸脱の分析を，システム状態に対する分析と，状態遷移に対する分析の 2 段階で逸脱を分析する．分析を 2 段階に分ける理由は，システムがある状態に留まっている状況と，イベントが発生した際にシステムが取りうる振る舞いとで逸脱の性質が異なるため，異なる視点から逸脱を分析する必要があるからである．分析者が逸脱を列挙することを補助するために，表 1 と表 2 に示すガイドワードと属性を分析の各段階で使用する．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する方が，より分析し易くなることもあると思われる．

状態に対する分析では，表 1 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．ここで分析するのは，システムがある状態に留まっている間に，常に満たすべき性質からの逸脱と，状態遷移の発生するイベントが発生していないにもかかわらず状態が遷移してしまうという，状態遷移条件からの逸脱である．次に，状態遷移に対する分析では，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．ここで分析するのは，状態遷移における遷移先の状態が仕様と異なる逸脱や，状態遷移のタイミングに関する逸脱，さらに，正しい状態に遷移した後に実行されるアクション

表 1　状態に対するガイドワード
Table 1　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関わらず，状態が遷移する

表 2　状態遷移に対するガイドワード
Table 2　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が，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するが，余分なアクションも実行されてしまう
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，本来実行されないアクションが実行される
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

Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2

に関する逸脱である．

3.3 分析項目

SAHSTD では，１つの逸脱に対して８つの項目を順番に考えながら分析シートを作成する．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，もしくは設計の記述である．状態に対する分析では，状態において満たすべき性質を，状態遷移に対する分析では，状態遷移に関する仕様，もしくは設計を記述する．３つ目は，前節で述べた分析手法を適用して列挙した逸脱の内容を，ガイドワードと属性と共に記述する．４つ目のローカル影響は，逸脱によるシステム内部動作への影響を記述する．５つ目のグローバル影響は，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，ローカル影響から連鎖的に分析する．６つ目の深刻度は，グローバル影響の深刻さを示す評価値である．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考慮してシステム開発者が決定する．深刻度の決定においては，システムとして許容できるかどうかを，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定義する必要がある．７つ目の原因には，逸脱が発生した原因として，ハードウェア，ソフトウェア，もしくはその両方に関連する原因を記述する．８つ目の対策は，逸脱の発生そのものを防ぐ対策，もしくは逸脱の発生を許容してその深刻度を低減するための対策を記述する．ソフトウェアとハードウェアの両方が含まれるシステムにおいては，危害の発生確率を明確に算出することが困難である．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．また，許容できない深刻度をもつ逸脱に対してのみ，原因分析と対策検討を実施するものとする．

4. 適用事例

4.1 話題沸騰ポットの概要

話題沸騰ポットは，お湯を設定した温度まで加熱する機能をもつ架空の機器である．話題沸騰ポットの内部には，ポンプ，ヒータ，蓋センサ，水位センサなどが接続されている．話題沸騰ポットの上位と下位のシステム仕様を図 1 に示す．このシステム仕様から，図 2 で示す階層型状態遷移図を作成する．

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 3 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，お湯が入っていない状況で加熱が開始され（空焚きと呼ぶ），ポット全体が非常に高温になり，作業者がボタンを操作する際に触れて，やけど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．次に避けるべきなのは，ロ

＜上位＞	(H.1)コンセントを接続すると，アイドル状態になる． (H.2)アイドル状態で，沸騰要求（蓋センサーon）すると，沸騰行為状態になる． (H.3)沸騰行為状態で，沸騰処理完了すると，保温行為状態になる． (H.4)保温行為状態で，沸騰要求する（沸騰ボタン 100msec 以上押す）と，沸騰行為状態になる． (H.5)沸騰行為状態で，エラーを検知すると，エラー状態になる． (H.6)保温行為状態で，エラーを検知すると，エラー状態になる． (H.7)沸騰行為状態で，温度制御停止すると，アイドル状態になる． (H.8)保温行為状態で，温度制御停止すると，アイドル状態になる．	
＜下位（沸騰行為状態）＞		＜下位（保温行為状態）＞
(L.h.1)沸騰要求すると，加熱中状態になる．		(L.k.1)沸騰処理完了すると，保温中状態になる．
(L.h.2)加熱中状態で，沸点到達すると，カルキ抜き中状態になる．		(L.k.2)保温中状態で，給湯要求すると，給湯中状態になる．
(L.h.3)加熱中状態で，エラーを検知すると，エラー状態になる．		(L.k.3)給湯中状態で，給湯要求解除すると，保温中状態になる．
(L.h.4)加熱中状態で，温度制御停止すると，アイドル状態になる．		(L.k.4)保温中状態で，エラーを検知すると，エラー状態になる．
(L.h.5)カルキ抜き中状態で，エラーを検知すると，エラー状態になる．		(L.k.5)保温中状態で，温度制御停止すると，アイドル状態になる．
(L.h.6)カルキ抜き中状態で，温度制御停止するとアイドル状態になる．		(L.k.6)給湯中状態で，エラーを検知すると，エラー状態になる．
(L.h.7)カルキ抜き中状態で，沸騰処理完了すると保温行為状態になる．		(L.k.7)給湯中状態で，温度制御停止すると，アイドル状態になる．
		(L.k.8)保温中状態で，沸騰要求すると，沸騰行為状態になる．

図 1　話題沸騰ポットのシステム仕様
Figure 1　System specification of the electric boiling pot.

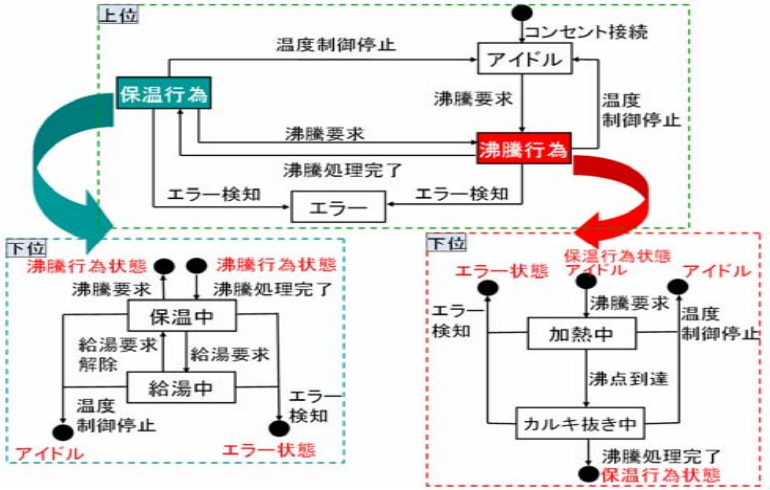


図 2　話題沸騰ポットの階層型状態遷移図
Figure 2　Hierarchical state transition diagram of the electric boiling pot.

Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2

ック中で，給湯ボタンを押していないのにも関わらず，高温のお湯が出てしまう状況で，深刻度を７とした．深刻度が６以降は，作業者の安全は確保されるが，お湯の状態に問題が発生する．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，沸騰していない場合のお湯の温度は，やけど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やけど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，お湯ができることを防ぐ機能をもつことである．そこで，システムとして許容できる深刻度は５以下であるとした．安全分析の結果，６以上の深刻度をもつ危害を発生させる逸脱に対しては，５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，３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（同時に発生する２つ以上の原因により発生する故障）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，分析する状態遷移図は，システムの仕様書と設計書から，漏れなく作成されていることである．

表 3　グローバル影響と深刻度の定義
Table 3　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		
やけどする	空焚きになる	お湯が蒸発し，サーミスタが 110℃を越える	9
やけどする	沸騰したお湯がでる	ロック中状態で，ボタンを押していないのに，高温のお湯がでる	8
やけどする	沸騰したお湯がでる	ロック解除状態で，ボタンを押していないのに，高温のお湯がでる	7
やけどしない	沸騰していないお湯がでる	ロック中とロック解除状態で，ボタンを押していないのに，低温のお湯がでる	6
やけどしない	沸騰されない	保温状態から沸騰したいけど，沸騰できない	5
やけどしない	設定された温度になったけど，給湯できない	お湯がでない	4
やけどしない	沸騰されない／保温されない	作業者の意思で沸騰／保温を中止する	3
やけどしない	沸騰されない／保温されない	お湯は入っている	2
やけどしない	沸騰される	カルキ抜きが十分に抜かれないまま保温になる	1
やけどしない	沸騰完了する	設定された温度のお湯を給湯できる	0

今回の事例では，表 2 で，Incorrect transition は，矢印の方向に関係なく線が繋がっている部分のみを考える．また，More action は，全てのアクションで，同一の装置を操作しているので考える必要はない．

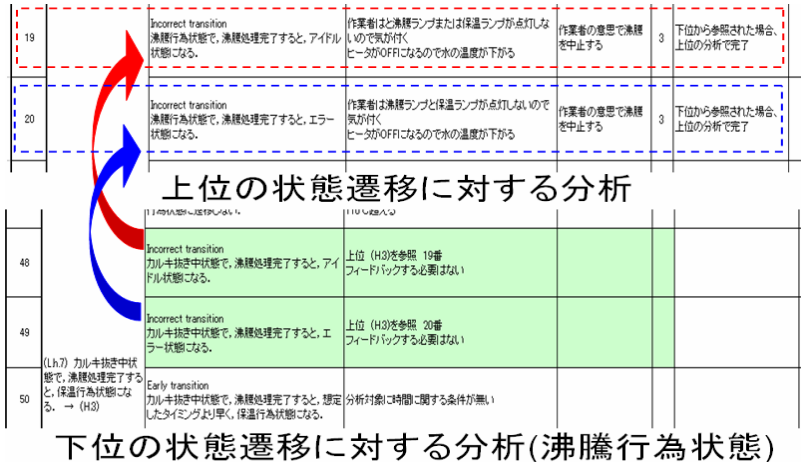
4.4 SAHSTD による分析

話題沸騰ポットのシステム仕様に対して SAHSTD を適用した結果を述べる．階層型状態遷移図における１つの逸脱に対して深刻度を決定する分析のパターンは，図 3 に示す４つに分類できる．

a の 12 番 No transition「アイドル状態で，沸騰要求したが，沸騰行為状態に遷移しない」は，上位のアイドル状態の分析だけで，深刻度を判断できる．b の 47 番 No transition「カルキ抜き中状態で，沸騰処理完了しても，保温行為状態に遷移しない」は，下位のカルキ抜き中状態の分析だけで，深刻度を判断できる．c は，上位の分析において深刻度を判断する際に，下位の分析結果を参照するパターンである．上位と下位の状態遷移に対する分析で，赤 4，5，6 番と青 15 番の点線は上位から下位の分析結果を参照する部分を示している．保温行為状態の正しい性質は「沸騰ランプ：OFF

c．上位から下位の分析結果を参照

Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2



d. 下位から上位の分析結果を参照

図 3　SAHSTD の分析パターン

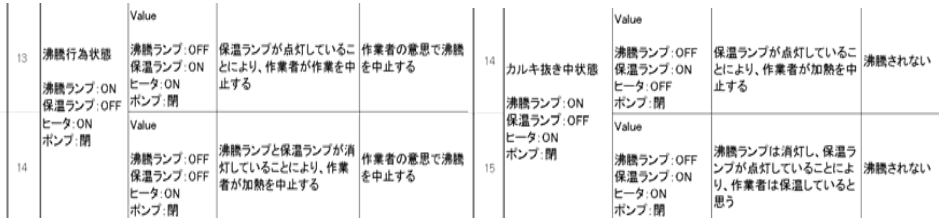
Figure 3　Analysis patterns of SAHSTD.

保温ランプ : ON，ヒータ : ON，ポンプ : 下位（保温行為）」である．ポンプの状態は，保温行為状態の下位状態に対する分析結果を参照しないと深刻度を判断することができない．赤の点線は，ポンプが閉めていて，青の点線はポンプが開いている．d は，下位の分析において深刻度を判断する際に，上位の分析結果を参照するパターンである．上位と下位の状態遷移に対する分析で，赤と青の点線は下位から上位の分析結果を参照する部分を示している．下位 48 番 Incorrect transition「カルキ抜き中状態で，沸騰処理完了すると，アイドル状態になる」では，上位 19 番「沸騰行為状態で，沸騰処理完了すると，アイドル状態になる」の分析結果を参照することで深刻度を決定できる．49 番も同様に，上位 20 番の分析結果を参照する．

図 4 は，上位の状態遷移図の沸騰行為状態に対して分析した結果と沸騰行為状態の下位の状態である加熱中状態に対して分析した結果である．どちらの分析においても同一の逸脱を分析しており，重複した分析である．どちらの状態で満たされる性質も「沸騰ランプ ON，保温ランプ OFF，ヒータ ON，ポンプ閉」という性質が共通であるため，このような場合には上位の分析だけで十分であり，下位の分析を省略しても良いと考えられる．ただし，上位と下位の状態で満たされる性質が異なる場合は，上位と下位の分析を別々に行う必要がある．

4.5 SASTD と SAHSTD の分析結果の比較

話題沸騰ポットに対して SASTD と SAHSTD を実施した結果を比較する．まず，深刻な危害をもたらす逸脱の分析結果は全て同じであることから，SASTD で分析可能な逸脱は，SAHSTD でも分析可能であることを確認した．



a. 上位の状態　　b. 下位の状態

図 4　重複した分析の例

Figure 4　An example of duplicate analysis between a higher state and a lower state.

次に，SASTD と SAHSTD の分析数を表 4 と表 5 に示す．SAHSTD の分析数は，上位の分析数と下位の分析数に分けて示している．「上位で分析済み」は，下位で分析した数のうち，上位の分析で既に同一の分析を実施している数を示している．「下位の分析を参照」は，上位（沸騰行為状態と保温行為状態）の分析において，下位の分析結果を参照することで深刻度を判断した数である．「本質的な分析数」は，全ての分析数から，「上位で分析済み」の数と「下位の分析を参照」の数を除いた，深刻度を純粋に決定した分析数である．状態に対する分析では，SASTD は 72 個，SAHSTD は全体で 92 個の分析を行ったが本質的な分析数は 61 個であった．状態遷移に対する分析では，SASTD は 215 個であるのに対して，SAHSTD は全体で 284 個の分析を行ったが，本質的な分析数は 134 個であった．

今回の事例では，SAHSTD の分析において，上位と下位で重複する分析を省略し，さらに，上位の分析において，下位の分析結果を参照することで分析の重複を防ぐことにより，SASTD よりも本質的に必要な分析数を減らすことができた．このことは，１つの状態遷移図において満たすべき性質が同じである複数の状態を，階層型状態遷移図で階層化することで，重複した分析をなくすことができることを意味する．

5. おわりに

本論文では，階層型状態遷移図に基づく安全分析手法 SAHSTD を提案した．状態遷移図を階層化することで，１つの状態遷移図に含まれる状態数を減らすことで分析の負担を軽減できる．さらに，適用事例において，上位と下位の分析で重複した分析をなくすことで，SASTD に比べて分析数を削減できることを明らかにした．従って，１つの状態遷移図を対象にする SASTD より分析が容易になったといえる．ただし，組

Vol.2012-SLDM-155 No.10
Vol.2012-EMB-24 No.10
2012/3/2

込みシステムの安全分析において，分析の網羅性をより向上させるためには，SAHSTDと複数の安全分析手法を組み合わせて適用することが望ましいと考えられる．

今後の課題としては，話題沸騰ポットに適した安全機能の検討や，並列に動作する２つの状態遷移が存在するシステムに対する安全分析手法を検討する．

表 4　状態に対する分析結果
Table 4　Analysis results for system states.

	SASTD	SAHSTD		上位で分析済み	下位の分析を参照	本質的な分析数
		上位	下位			
アイドル	8	8	—	—	—	8
エラー	7	7	—	—	—	7
沸騰行為	—	１０	—	—	1	9
保温行為	—	１０	—	—	7	3
加熱中	１０	—	１０	9	—	1
カルキ抜き中	１０	—	１０	9	—	1
保温中	１９	—	１９	3	—	１６
給湯中	１８	—	１８	2	—	１６
合計	７２	９２		２３	8	６１

表 5　状態遷移に対する分析結果
Table 5　Analysis results for state transitions of the system.

	SASTD	SAHSTD		上位で分析済み	下位の分析を参照	本質的な分析数
		上位	下位			
コンセント→アイドル	１０	１１	—	—	—	１１
アイドル→沸騰行為	—	１１	—	—	—	１１
アイドル→加熱中	１３	—	—	—	—	—
沸騰行為→保温行為	—	１２	—	—	—	１２
保温行為→沸騰行為	—	１２	—	—	—	１２
沸騰行為→エラー	—	１２	—	—	—	１２
カルキ抜き中→保温中	１３	—	—	—	—	—
保温中→加熱中	１５	—	—	—	—	—
保温行為→エラー	—	１２	—	—	１２	0
沸騰行為→アイドル	—	１２	—	—	—	１２
保温行為→アイドル	—	１２	—	—	１２	0
保温行為→加熱中	—	—	１２	7	—	5
加熱中→カルキ抜き中	１４	—	１３	0	—	１３
加熱中→アイドル	１４	—	１３	１１	—	2
カルキ抜き中→アイドル	１３	—	１３	１１	—	2
加熱中→エラー	１３	—	１３	１１	—	2
カルキ抜き中→エラー	１３	—	１３	１１	—	2
カルキ抜き中→保温行為	—	—	１３	１１	—	2
沸騰行為→保温中	—	—	１２	１１	—	1
保温中→沸騰行為	—	—	１３	１１	—	2
保温中→給湯中	１５	—	１３	0	—	１３
給湯中→保温中	１３	—	１２	0	—	１２
保温中→アイドル	１５	—	１３	１１	—	2
給湯中→アイドル	１３	—	１２	１０	—	2
保温中→エラー	１５	—	１３	１１	—	2
給湯中→エラー	１３	—	１２	１０	—	2
合計	２１５	２８４		１２６	２４	１３４

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)　N.G. Leveson, Failure Mode and Effect Analysis, Safeware: System Safety and Computers, pp.317-326, Addison-Wesley, 1995.
3)　R.Lutz and M.Woodhouse, Experience Report: Contributions of SFMEA to Requirements Analysis, IEEE International Conference on Requirements Engineering, 1999.
4)　N.G. Leveson, Hazards and Operability Analysis, Safeware: System Safety and Computers, pp.335-341, Addison-Wesley, 1995.
5)　D. J. Pumfrey, The Principled Design of Computer System Safety Analyses, PhD Thesis, York University, 1999.
6)　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，電子情報通信学会論文誌 A, Vol.J95-A,No.2, Feb 2012.
7)　SESSAME，話題沸騰ポット（GOMA-1015 型）要求仕様書 第 7 版
8)　N.G. Leveson, J.L. Stolzy, Safety Analysis Using Petri Nets, IEEE Transactions on Software Engineering, Vol. SE-13, No. 3, pp. 386-397,The Institute of Electrical and Electronics Engineers, 1987.
9)　N.G. Leveson, The SpecTRM-RL language, 1998.
10)　T. Ishimatsu, N. Leveson, J. Thomas, M. Katahira, Y. Miyamoto, H. Nakao, Modeling and Hazard Analysis using STPA , 4th IAASS Conference, 2010.