

博士学位論文

状態-作用生起順序に着目した
ハザードの同定・分析および抑制策導出手法の研究

令和3年3月

長岡技術科学大学 大学院工学研究科
情報・制御工学専攻
学籍番号 17700182
柴垣 光男

指導教員 福田 隆文

目次

第1章 序論

1.1 研究テーマ.....	5
1.2 研究の背景.....	6
1.2.1 単一の不変安全状態をもつ機械類のハザード.....	6
1.2.2 可変安全状態と相反ハザード.....	7
1.2.3 相反事象と相反ハザード.....	7
1.3 研究目的.....	9
1.4 論文の構成.....	10
1.5 用語の定義および記号.....	13

第2章 先行研究

2.1 リスクアセスメントにおける本研究と従来技法の位置付け.....	18
2.1.1 ハザードの同定技法.....	20
(1) HAZOP (Hazard and Operability) スタディーズ.....	20
(2) What-if 技法.....	21
(3) A-C モデル (The Action Changes and the action-chains Model).....	22
(a) A-C モデルおよび S-A プロセスチャートのハザード図式表現法.....	22
(b) 自律形移動ロボットのスキッドに起因するハザードと抑制策の図式表現例.....	23
2.1.2 ハザードの分析技法.....	30
(1) FTA.....	30
(2) FMEA (Failure Modes and Effects Analysis).....	31
(3) ETA (Event Tree Analysis).....	33
(4) STPA (System-Theoretic Process Analysis).....	33
2.2 S-A プロセスチャートの特徴と従来技法との比較.....	36
2.3 S-A プロセスチャートと従来技法との関係.....	38

第3章 S-A プロセスチャートの理論的枠組みと構築方法

3.1 本論文におけるハザードモデル.....	40
3.2 遷移作用と事象の関係およびその図式表現.....	42
3.3 離散事象システムモデルと S-A プロセスチャートとの関係.....	43
3.4 遷移作用の分類.....	44

3.5 S-A プロセスチャートの基本構成.....	45
3.6 ハザード同定のための S-A プロセスチャートの展開方法	46
3.7 状態遷移経路分析のための S-A プロセスチャートの展開方法	46
3.7.1 システム要素およびシステム状態の表記方法	46
(1) システム要素状態 $X_{i,j,k}$	47
(2) システム状態 S_y	47
3.7.2 遷移作用 $A_{i,j}(k,k')$ と $X_{i,j,k}$ との関係.....	47
3.7.3 状態遷移経路図.....	49
3.7.4 状態遷移経路図からの S-A プロセスチャートの導出	53
3.7.5 状態遷移経路図と遷移作用順列 P_w の関係	54
3.8 S-A プロセスチャートにおけるハザードの抑制原理および抑制概念	57
(1) 望ましくない状態遷移を無くす, または抑制するハザード抑制策.....	60
(2) 危害から遠ざかる移行制御によるハザード抑制策.....	61

第 4 章 S-A プロセスチャートを用いたハザードの同定

4.1 緒言.....	62
4.2 事例 1 : 環境試験槽の停止に起因するハザードの同定とその抑制策の導出.....	63
4.2.1 記号.....	63
4.2.2 環境試験槽の概要	64
4.2.3 ハザードの同定.....	66
4.2.4 ハザード抑制策の導出事例	70
4.3 事例 2: リチウムイオン 2 次電池の熱暴走起因のするハザードの同定とその抑制策の導出	73
4.3.1 略語.....	73
4.3.2 リチウムイオン 2 次電池の信頼性・安全性試験システムの概要	74
(1) システムの概要.....	74
(2) 各システム要素の動作条件	74
4.3.3 システム状態の定義.....	76
(1) システム要素 $X_{i,j,k}$	76
(2) 状態遷移プロセスモデル	76
(3) システム状態の定義.....	77
(4) 遷移作用 (事象) の設定	79
4.3.4 ハザードの同定.....	80
4.3.5 ハザード抑制策の導出事例	83
4.4 第 4 章のまとめ	86

第5章

多状態を持つ要素を含むシステムの S-A プロセスチャートを用いたハザードの分析

5.1 緒言.....	87
5.2 事例検証.....	87
5.2.1 記号および略語.....	87
5.2.2 事例1：溶剤乾燥器のガス爆発の分析.....	88
(1) システムの概要.....	88
(2) システム要素の状態定義.....	88
(3) 状態遷移プロセスモデル（可燃性混合気）.....	90
(4) $A_{ij}(k, k')$ を生起させる $E_{ij}(k, k')$ の設定.....	91
(5) ガス爆発のシステム状態遷移表および状態遷移経路図.....	92
(6) 状態遷移経路図からの S-A プロセスチャートの導出.....	93
(7) 遷移作用の具象化によるシステム要素挙動分析.....	93
5.2.3 事例2 後方車が前方車に追突の分析.....	98
(1) システム要素の状態定義.....	98
(2) 状態遷移プロセスモデル.....	98
(3) 後方車が前方車に追突のシステム状態遷移表および状態遷移経路図.....	99
(4) 後方車が前方車に追突の S-A プロセスチャートの導出.....	100
(5) ハザード5の抑制概念.....	101
5.3 第5章のまとめ.....	102

第6章

S-A プロセスチャートから導出される FT による事象生起順序依存ハザードの分析

6.1 緒言.....	103
6.2 S-A-FT の構造.....	104
6.2.1 S-A プロセスチャートと S-A-FT との関係.....	104
6.2.2 S-A-FT の階層構造.....	105
6.2.3 順序依存 O-PrIm 群.....	107
6.2.4 相反/排他事象を含む O-PrIm.....	107
6.3 事例“電源システム故障”の分析.....	109
6.3.1 S-A プロセスチャートの導出（電源システム故障）.....	109
(1) システムの基本動作.....	109
(2) システム要素の状態定義.....	110
(3) 状態遷移プロセスモデル.....	110

(4) $A_{ij}(k, k')$ を生起させる $E_{ij}(k, k')$ の設定	112
(5) システム状態-遷移作用-出力事象の関係	113
(6) S-A プロセスチャートの洗い出し	115
6.3.2 S-A-FT の展開とその分析	116
(1) S-A-FT の導出	116
(2) O-PrIm の導出	119
(3) 順序依存 O-PrIm 群の導出	119
6.4 第 6 章のまとめ	120

第 7 章 結言

7.1 研究成果	121
7.2 結論	126
7.3 S-A プロセスチャートの今後の展開	126
参考文献	127
謝 辞	133
付録 1 初期状態～危害に至る図 4-6 の潜在的状態遷移プロセス一覧 (No.1～No.114)	134
付録 2 FRAM (機能共鳴分析技法:Functional Resonance Analysis Method) の概要	138

第1章 序論

1.1 研究テーマ

ある事象が、ある状態では安全側事象となり、別の状態では危険側事象となる場合がある。あるハザードに関して危険状態または危害を発現させる事象を危険側事象、それらを抑制する事象を安全側事象とする。例えば、自動車の走行ではプリクラッシュシステムの故障による誤停止は追突するハザードに対して安全側であるが、追突されるハザードに対しては危険側である。ハザードが複数存在する場合、ある事象が安全または危険側事象かどうかは、どのハザードを想定するかによって変わる。また、あるハザードの抑制を目的とする機能の履行が、他のハザードでは危害を発現させる危険側事象となり得る。さらに、その危険側事象は、故障、エラー、失敗等だけでなく、システム要素の正常な要求機能の履行、修復、回復等によって行われる場合がある。このようなハザードの同定および分析にあたっては、ハザード生成過程の動的検討、すなわち危害に至る潜在的状態遷移プロセスを次々と変化する状態および事象の連鎖として把握することが必要である。特に、あるシステムとその他複数のシステムが結合し複雑化したシステムでは、互いに相反するハザード（1.2.2項参照）を考慮した分析が必要である。しかし、従来のハザードの同定・分析技法では、ハザードを動的に分析することは困難である。

このことから、本論文は、あるシステム（系）のハザード（Hazard）を体系的・系統的に洗い出し、相反ハザードの有無を識別し、その結果から合理的かつ系統的に抑制策を導出する方法について議論している。

英文表記“Hazard”は、JIS Z 8051: 2015¹⁾、JIS B 9700: 2013²⁾、JIS C 0508-4: 2012³⁾等の規格において、“ハザード”、“危険源”、“潜在危険”等と呼ばれるが、本論文は、これを“ハザード”と呼ぶ。MIL-STD-882E⁴⁾は、ハザードを、

死亡、怪我、職業疾病、機器または財産の損傷または損失、または環境への損害をもたらす不測の事象または一連の事象（すなわち事故）につながる可能性のある顕在または潜在的な状況（A real or potential condition that could lead to an unplanned event or series of events (*i.e.* mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment)

と定義している。また、JIS B 9700 (ISO 12100: 2010⁵⁾) は、ハザードを

危害を引き起こす潜在的根源（Potential Source of Harm）

と定義しているが、具体的には危害を起こし得る起源（Origin）となるものと起こり得る結

果 (Potential Consequence) との組合せによって、例えば、“重力加速度に起因して落下するハザード”、“充電部に起因する感電のハザード”のように表現する。さらに、JIS B 9700 は、危害の発現プロセスを次の①～⑥のとおり分類し、危険状態および危険事象を含めてハザードを同定することを要求している。

- ① 最初に危害を起こし得る起源となるもの (Origin) が存在し、
- ② 起源に対して何らかの事象が働いて、
- ③ 危険状態を生成し、
- ④ 危険状態において危険事象が生起し、
- ⑤ 回避に失敗、
- ⑥ 危害が発現する。

ハザードの概念に明確な境界を設定することは困難であり、分析対象によってその解釈にばらつきが生じる恐れがある。そのため本論文では、①～⑥のプロセス全体をハザードとして取り扱い、ハザードを初期状態から危害が発現するまでの一連の潜在的プロセス全体、すなわち

初期状態、中間状態、プレクリティカル状態またはクリティカル状態を経て危害に至る潜在的状態遷移プロセス

と定義し議論を展開する。

1.2 研究の背景

JIS Z 8051: 2015 は安全を”許容不可能なリスクがないこと”と定義しているが、本論文では、安全な状態を“ハザードが許容範囲に制御されており直ちには危害が発生しない状態”と定義する。安全な状態は不変安全状態 (1.5 節 (3) 参照) と可変安全状態 (1.5 節 (4) 参照) とに分類できる⁶⁾。

1.2.1 単一の不変安全状態をもつ機械類のハザード

一般的に機械安全の分野での機械により人が挟まれ、巻き込まれる等により危害が発現するハザードに関する状態には、

- ・ 安全状態
- ・ 危険状態
- ・ いずれともわからない状態

が存在し、安全状態が確認されている時にのみ運転を許可する安全確認型の安全論理が、基本原則として位置付けられている^{7)~9)}。ここでシステムの安全状態とは、次の (a) または (b) を意味する¹⁰⁾。

- (a) 機械の稼働領域に人が存在していない状態
- (b) 機械が停止している状態、すなわち ZMS (Zero Mechanical State: 機械に供給されるエネルギーを遮断し、潜在するエネルギーを消散、低下させ、作業者に障害を与えないように処置された状態)

また、機械災害抑止のための基本方策は、“安全が確認できない場合、危害が生じる前に自ら停止すること”とされる¹¹⁾。

1.2.2 可変安全状態と相反ハザード

近年普及が著しい稼働領域を人間の存在領域と共有することを前提とする搬送用、清掃用、介護用等の次世代ロボット¹²⁾において、ロボットから人の隔離は不可能であり、しばしばロボットが転倒を回避するためにバランスを制御する等、状況に応じた制御を適切に継続することが安全な状態となる。この場合、例えば、状況の変化に応じてロボットの出力増大の状態および出力減少の状態に制御されることにより安全が確保される。このように安全確保に必要な状態が変化する安全状態を可変安全状態という。

自動車の走行では追突するハザードと追突されるハザードがある。プリクラッシュシステムの故障による誤停止は追突するハザードに対して安全側であるが、追突されるハザードに対しては危険側である。これらのハザードは、誤停止に関して相反ハザードである¹³⁾。

1.2.3 相反事象と相反ハザード

アイテムの状態 A から B への変化と状態 B から A への変化の組み合わせを相反事象という。相反事象に関して相反ハザードが構成される場合がある。例えば、**図 1-1** はガス濃度を抑制する目的で換気システムを装備する溶剤乾燥器の各状態 $S_1 \sim S_3$ と事象 E_1 : 換気システム稼働状態→停止状態への変化および事象 E_2 : 換気システム停止状態→稼働状態への変化との関係を表している。 E_1 と E_2 とは相反事象である。 A_1 は E_1 によって生起する作用であり、 A_2 は E_2 によって生起する作用である。また、可燃性ガスの属性であるガス濃度は、次の 3 個の状態を持つ。

- S_1 爆発下限界以下
- S_2 爆発範囲 (爆発性雰囲気)
- S_3 爆発上限界以上

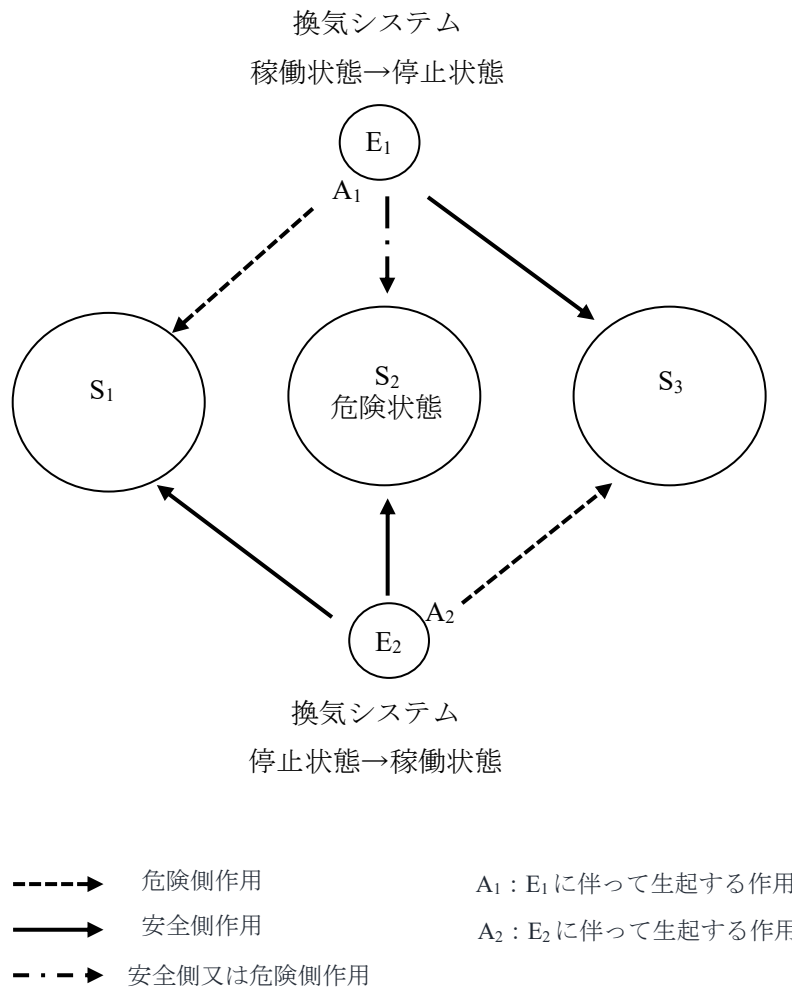


図 1-1 溶剤乾燥設備（乾燥中）の各状態と事象の関係

ガス爆発のハザードに関して S₂ は、着火エネルギーの発生によって直ちにガス爆発が生起し得る危険状態である。被乾燥物から可燃性ガスが蒸発している状態で、換気システムが停止すると乾燥器内のガス濃度は自然上昇を続ける。この場合、E₁ は、S₁ に対して S₂ を生起させる危険側事象であるが S₃ に対して S₂ への移行を抑制する安全側事象と言える。また、E₁ は S₂ に対して S₁ への移行を妨げる危険側事象であるが、S₃ に向かわせる安全側事象とも考えられ、E₁ が S₂ に対して安全側または危険側かどうかは一義的に決定できない。逆に、E₂ は、S₁ に対して S₁ を維持するための安全側事象であるが、S₃ に対して S₂ を生起させる危険側事象である。また、E₂ は S₂ に対して S₁ を生起させる安全側事象である。

これらの S₁~S₃、E₁、E₂ の関係から、ただちに次のハザードが同定される。

ハザード 1: ガス濃度が S₁ から S₂ へ上昇後、着火源の作用によりガス爆発が発生する。

ハザード 2: ガス濃度が S₃ から S₂ へ下降後、着火源の作用によりガス爆発が発生する。

ハザード1およびハザード2と事象E₁および事象E₂との関係を表1-1に示す。ハザード1に対してE₁は危険側、E₂は安全側であるが、ハザード2に対してE₁は安全側、E₂は危険側である。すなわち相反事象E₁およびE₂に関してハザード1およびハザード2は相反ハザードである。

表 1-1 相反事象と相反ハザード

ハザード	相反事象（換気システム）	
	E ₁ :稼働状態→停止状態	E ₂ :停止状態→稼働状態
ハザード1 ガス濃度がS ₁ からS ₂ へ上昇後、着火源の作用によりガス爆発が発生。	危険側	安全側
ハザード2 ガス濃度がS ₃ からS ₂ へ下降後、着火源の作用によりガス爆発が発生する。	安全側	危険側

1.3 研究目的

本研究では、1.2節の相反事象および相反事象に関して構成される相反ハザードに着目する。相反事象に関して相反ハザードを持つシステムでは、あるハザードの抑制を目的とする機能の履行（安全側事象）が、他のハザードでは危険側事象となり得る。また、故障、エラー、失敗等の無秩序状態作用（1.5節（19）および3.4節参照）だけでなく、システム要素の正常な要求機能の履行、修復、回復等による秩序状態作用（1.5節（18）および3.4節参照）が危険側事象となる可能性が存在する。例えばシステム要素のアップ状態からダウン状態¹⁴⁾への変化だけでなく、ダウン状態からアップ状態への変化（事象）が、危険側事象となり得る。秩序状態作用が危険側となり得る場合、その秩序状態作用の実行は安全側でのみ許可されるようにインターロック回路¹⁵⁾を構成する等の対策が必要である。

ハザードを同定・分析するための従来技法、例えば、HAZOP（Hazard and Operability）スタディーズ^{21)~24)}、What-if^{24),25)}、FTA（Fault Tree Analysis）^{24), 28)~33)}、ETA（Event Tree Analysis）^{24), 34), 35)}、FMEA（Failure Modes and Effects Analysis）^{24), 26),27),36)~40)}等が、自動車、ロボット、航空機、化学プラント、産業機械等の分野で幅広く適用されてきた。しかし、相反ハザードの生成は状態および事象の生起順序と強い相関がある。このため、相反ハザードの同定および分析に際しては、ハザード生成過程の動的検討、すなわち危害に至る潜在的状態遷移プロセスを次々と変化する状態および事象の連鎖として把握することが必要である。しかし、これら従来技法は、危害に至る状態遷移プロセスにおける状態と

事象との関係およびその生起順序を系統的に同定して図式化する手段を持たず、相反ハザードの分析には不十分な側面をもつ。

この課題に対して、本研究の目的は、従来技法にはない次の (a) ~ (c) の特徴をもつハザードの同定、分析、および抑制策の導出手法を確立することである。

- (a) システム状態が状態を変化させる作用を伴う事象によって次々と遷移し到達し得る危害の洗い出し、すなわちハザードの網羅的同定が可能である。
- (b) 網羅的に同定したハザード群の中から相反ハザードの識別が可能である。
- (c) 相反ハザードの抑制策の系統的かつ合理的な導出が可能である。

本研究は、まず、状態 (state) と状態を変化させる作用 (action) を伴う事象との生起順序に着目したハザードの図式表現技法、すなわち S-A プロセスチャート (State-Action Process Chart) ^{41),42)} を提案する。次に、S-A プロセスチャートを、環境試験槽の停止、ガス爆発、後方車が前方車に追突する等のハザードの同定・分析に適用し、S-A プロセスチャートの有効性を検証する。

以下、第2章～第7章で具体的に論ずる。

1.4 論文の構成

本論文の概要は次のとおりである。また、論文の構成は図 1-2 のとおりである。

第1章は、本研究の目的およびその背景と位置付けについて説明している。

第2章は、主に工学分野におけるリスク分析に広く適用されている従来技法と S-A プロセスチャートとの相違点および関連性について説明している。ここで対象とするリスクは、自動車、ロボット、航空機、化学プラント、産業機械等の機械・電気システムの人的あるいは物的損失に限定し、例えば、自然災害、環境、法務、財務、政治、外交等のリスクは対象としない。

第3章は、ハザードを図式表現するための S-A プロセスチャートの理論的枠組みと構築方法について論じている。

第4章は、温湿度試験槽の停止に起因するハザードおよび試験槽内での LIB (リチウムイオン2次電池) の熱暴走に起因するハザードの同定とその抑制策の導出に S-A プロセスチャートを適用して、(a) システムのそれぞれの状態にシステム要素の故障、エラー、正

常機能の履行に起因する遷移作用を組み合わせることで危害に至る状態遷移プロセスを系統的に追跡し、ハザードを網羅的に同定すること、(b) 図式化されたハザードの状態と遷移作用の図式構造から、ハザード抑制原理に基づきハザードの抑制策を系統的かつ合理的に導出することが可能であることを示し、その有効性を検証している。

第5章は、すでに特定された危害と初期状態とを結ぶ状態遷移経路の分析に S-A プロセスチャートを適用しその有効性について論じている。本章では、まずシステムの状態をシステム要素が持つ状態の組合せによって定義し、各システム状態の遷移可能な経路と遷移作用が、状態遷移経路図で表現されることを示している。次に、この状態遷移経路図上で初期状態と危害（最終状態）とを結ぶ経路をたどることによって、状態遷移経路が異なるハザードが網羅的・系統的に洗い出される。ここでは、2つの事例にこの技法を適用して、ある状態では抑制作用となり、別の状態では危害へと向かわせる作用をもつ事象を識別し、相反ハザード等の分析に対する S-A プロセスチャートの有効性が検証されている。

第6章は、まず S-A プロセスチャートから得られたハザードを、優先 AND 構造を持つ FT (S-A-FT) で展開する手法を提案している。次に、2冗長電源システムの故障に至るプロセスの分析に本技法を適用し、S-A-FT では S-A プロセスチャートと FTA とが互いに補完的役割を担うことによって、システム要素レベルまでのハザードのより合理的な分析が可能となることを示している。

第7章は、研究成果のまとめ、結論、提案手法の今後の展開について説明している。

論文構成は図 1-2 として要約できる。

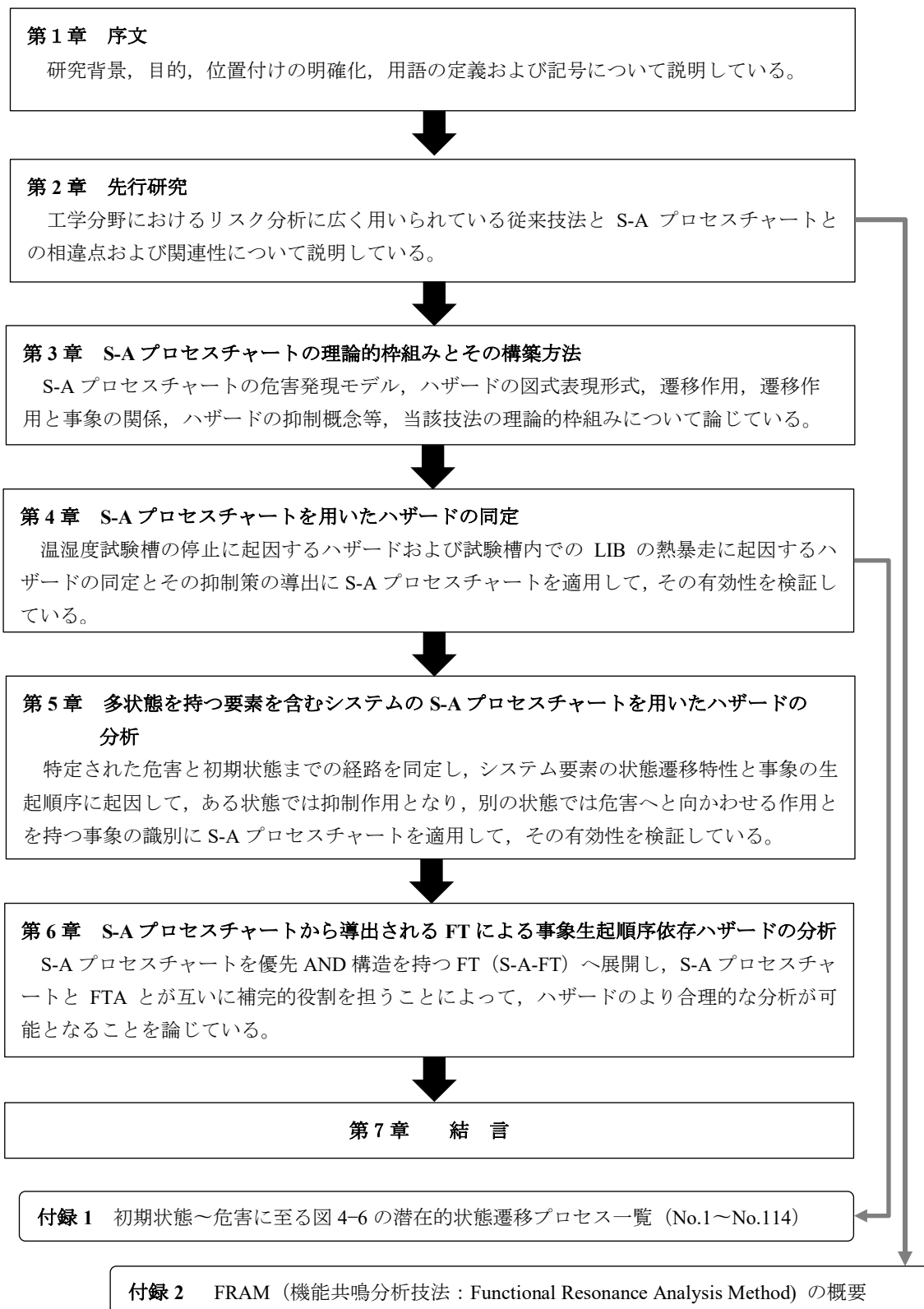


図 1-2 論文の構成

1.5 用語の定義および記号

安全に関する用語は基本的には JIS Z8051 に従うが、本論文で用いるその他の用語および記号は、次の定義に従う。

(1) 状態 (state)

ある時刻における物理量，機能，または形態等によって定まるシステムの時間幅をもつ特性

(注) 文献⁴³⁾ 3.1.2.2 に時刻を追記し修正引用

(2) 安全な状態

ハザードが許容範囲に制御されており，直ちには危害が発生しない状態

(3) 不変安全状態

単一ハザードに対してシステムの状況によって，秩序状態が安全であれば秩序状態を維持する，または無秩序状態が安全であれば無秩序状態を維持する，またはシステムを秩序状態から無秩序状態へと，または無秩序状態から秩序状態へと変化させることによって得られる最終的な安全な状態

(4) 可変安全状態

単一ハザードに対してシステムの状況によって，システムを秩序状態から無秩序状態および無秩序状態から秩序状態へと変化させることによって，またはそれらの変化を何回か繰り返すことによって得られる最終的な安全な状態

((3) および (4) に対する注)

- ・秩序状態 (activated state (ordered state))

要素間のエントロピーが相対的に低い (秩序性が相対的に高い (multiplicity が小さい)) 状態

- ・無秩序状態 (inert state (disordered state))

要素間のエントロピーが相対的に高い (秩序性が相対的に低い (multiplicity が大きい)) 状態

(5) 初期状態 (initial state)

S-A プロセスチャートの状態遷移プロセスの起点の状態

(6) 中間状態 (intermediate state)

システムの初期状態以外の正常な状態

- (7) プレクリティカル状態 (pre-critical state)
初期状態または中間状態から遷移した状態であり、システムの正常な状態から逸脱し、かつクリティカル状態に遷移する前の状態
- (8) クリティカル状態 (critical state)
ある遷移作用によって危害に遷移し得る状態
(注) システムの状態が、初期状態と危害だけの場合、初期状態はクリティカル状態でもある。
- (9) 遷移 (transition)
ある状態から別の状態への変化
(注) 時間幅の無い遷移を事象という。
- (10) 遷移作用 (transition action)
状態を変化すなわち遷移させる働き
- (11) 抑制作用 (control action)
遷移作用を抑制する働き
- (12) 抑制策 (control measure)
抑制作用を発現させるための手段
- (13) 危害 (harm)
ある状態遷移プロセスで、人、財産、または環境に対して、最終的な被害が発現している状態
(注) 文献¹⁾ 3.1 の危害が状態であることを追記し修正引用
- (14) ハザード (hazard)
初期状態、中間状態、プレクリティカル状態、またはクリティカル状態を経て危害に至る潜在的状態遷移プロセス
(注) 文献¹⁾ 3.2 を具体的にして修正引用
- (15) ハザードの同定 (hazard identification)
初期状態、中間状態、プレクリティカル状態、またはクリティカル状態を経て危害に至る潜在的状態遷移プロセスを洗い出すこと

(16) 属性変数 (attribute variable)

システム要素 i の $q_{i,j}$ 番目の属性

(17) 状態変数 (state variable)

i の属性 j の $p_{i,j,k}$ 番目の状態

(18) 秩序状態作用 (activated action)

要素間のエントロピーが相対的に低い(秩序性が相対的に高い(multiplicity が小さい))
状態におけるそれらの要素間の働き (例: エネルギー伝播, 情報伝達, 作用原因物質
転移, 供給阻害 (阻害), 存在形態形に起因する作用等)

(注) 文献⁴³⁾ 3.1.2.2 note1~note4 を要約し修正引用

(19) 無秩序状態作用 (inert action)

要素間のエントロピーが相対的に高い(秩序性が相対的に低い(multiplicity が大きい))
状態におけるそれらの要素間の働き

(注) 文献⁴³⁾ 3.1.2.2 note1~note4 を要約し修正引用

(20) 可逆遷移 (reversible transition)

アイテムの状態 A が他の状態を経由せずに状態 B に変化した後, 状態 A および状態
B 以外の状態を経由せずに状態 B から状態 A に戻ることができるアイテムの変化

(21) 不可逆遷移 (irreversible transition)

アイテムの状態 A が他の状態を経由せずに状態 B に変化した後, 状態 A および状態
B 以外の状態を経由せずに状態 B から状態 A に戻ることができないアイテムの変化

(22) 制約遷移 (restricted transition)

3 個以上の状態を持つシステム要素において, システム要素の属性がもつ物理量, 機
能等の特性に基づく制約条件に従った状態遷移プロセス (例えば, 温度が“低→中→高”
に遷移する)

(23) S-A-FTA (S-A-process-chart-based FTA)

S-A プロセスチャートから導出された遷移作用を生起させる事象群を第 1 階層に優先
AND ゲートを用いて展開する FT による分析 (図 6-3 参照)

(24) 基本事象 (Basic Event)

S-A-FT において, それ以上展開できない故障, エラー, 失敗, 修復, 回復等からなる

事象

(25) 最終状態 (Final State)

S-A-FTにおいて、頂上事象を起こすシステム属性状態の組合せ

(注) 最終事象の結果最終状態となる。

(26) 事象生起順序付きインプリカント (Ordered Implicant (O-Im))

S-A-FTにおいて、頂上事象を生起させる順序付けられた基本事象の組み合わせ

(27) 事象生起順序付きプライムインプリカント (Ordered Prime-Implicant (O-PrIm))

S-A-FTにおいて、頂上事象を生起させる最小限の順序付けられた基本事象の組み合わせ

(注) O-PrImはコヒーレントシステムにおける最小カット集合に相当する。

(28) 順序依存O-PrIm群 (Sequential O-PrIm group)

最大で $c!$ 通りの事象生起順序を持つ c 個の重複しない基本事象 E_d ($d = 1, 2, \dots, c$)

から成る O-PrIm が、頂上事象を生起させる r 通りの事象生起順序を持つとき、

$r < c!$ の場合、 E_d ($d = 1, 2, \dots, c$) は順序依存 O-PrIm 群を構成する。

$r = c!$ の場合、 E_d ($d = 1, 2, \dots, c$) は順序依存 O-PrIm 群を構成しない。

(6.2.3 項参照)

(29) 相反事象 (Reciprocal events)

アイテムの状態 A から B への変化 (事象) と状態 B から A への変化 (事象) の組み合わせ

(30) 排他事象 (Exclusive events)

同時に真とはならないアイテムの状態を生成する事象の組み合わせ

記号

$X_{i,j,k}$	システム要素 i が持つ属性 j の状態 k ($i=1,2,\dots,n$, $j=1, 2,\dots,q_{i,j}$, $k=0,1, 2,\dots,p_{i,j,k}$)
S_y	$X_{i,j,k}$ の組合せで表されたシステムの状態 ($y=1, 2,\dots,u$)
$A_{ij}(k,k')$	$X_{i,j,k}$ を $X_{i,j,k'}$ に変化させる遷移作用
$E_{ij}(k,k')$	$X_{i,j,k}$ を $X_{i,j,k'}$ に遷移させる働きを生起させる, ある要素の時間幅のない変化すなわち事象

第2章 先行研究

第2章では、主に工学分野におけるリスク分析に広く用いられている従来技法とS-Aプロセスチャートとの相違点および関連性について説明する。本研究においてリスクの概念は、JIS Z 8051:2015でのそれに準拠し、危害の発生確率およびその度合いの組合せと定義される。ただし、対象とするリスクは、自動車、ロボット、航空機、化学プラント、産業機械等の機械・電気システムにおける人的あるいは物的損失に限定し、例えば、自然災害、環境、法務、財務、政治、外交等のリスクは対象としない。

2.1 リスクアセスメントにおける本研究と従来技法の位置付け

JIS Z 8051:2015 (ISO/IEC Guide 51:2014⁴⁴⁾) において、リスクアセスメントは図 2-1 に示す①～④のプロセスで実施される。

- ① 意図される使用および合理的に予見可能な誤使用の明確化
- ② ハザードの同定
- ③ リスクの見積り
- ④ リスク評価

①～③はリスク分析の部分に相当する。当該規格においてリスク分析とは、ある使用条件でのシステムのハザードを同定し、同定されたハザードが顕在化する要因を定性的または定量的に分析し、その起こりやすさと発現結果の影響度とからリスクを見積ることである。S-A プロセスチャートによる一連の手法は、リスク分析②および③、およびリスクの低減④を支援するための手法として位置付けられる。本章では、まずハザードの同定・分析のための従来技法として広く適用されている次の (a) , (b) の概要について説明する。

- (a) ハザードの同定技法
HAZOP (Hazard and Operability) スタディーズ, What-if 技法
- (b) ハザードの分析 (定性的および定量的分析) 技法
FTA (Fault Tree Analysis) , ETA (Event Tree Analysis) , FMEA (Failure Modes and Effects Analysis)

次に、図式表現を用いたハザードの同定技法として、

- ・ A-C モデル (The Action Changes and the action-chains Model) ,
- また、ハザードの分析技法として
- ・ STPA (System-Theoretic Process Analysis)

について説明する。

他の安全分析のための図式表現手法として、レジリエンスエンジニアリングに基づく FRAM (Functional Resonance Analysis Method : 機能共鳴分析技法) があげられる^{16),17)}。FRAM は、システムの機能の組み合わせで事故の状況を展開し図式化する。FRAM の実用化のための研究¹⁸⁾が行われている。しかし、FRAM は、図的表現方法、対策案の導出方法の手順が十分に検討されていない等の課題を残している^{19),20)}。FRAM の概要を付録 2 に示す。

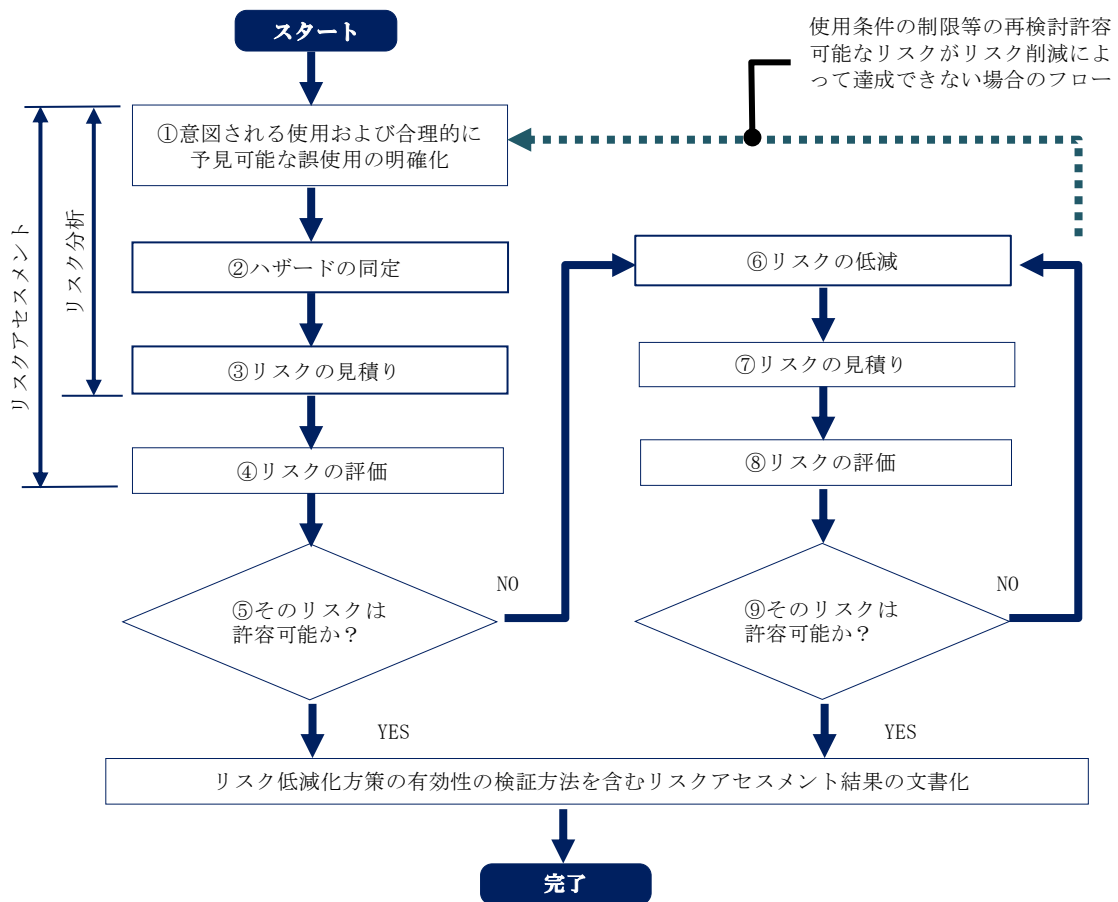


図 2-1 リスクアセスメントとリスク低減の反復プロセス
(JIS Z 8051: 2015 図 2 を修正して引用)

2.1.1 ハザードの同定技法

(1) HAZOP (Hazard and Operability) スタディーズ

HAZOP スタディーズ (以下, HAZOP という) は, 1960 年代の初めに, イギリスの ICI 社 (Imperial Chemical Industry) が自社の化学プラントの安全評価のために開発した技法である²¹⁾。HAZOP 技法に関する最初の論文は, 1974 年, H.G.Lawley によって Chemical Engineering Progress 誌に掲載された²²⁾。HAZOP は当初, 化学産業におけるプラントシステムの分析技法として開発されたが, 現在は, 鉄道, 発電, 機械システム等へ用途が拡大し, その適用方法は規格化されている²³⁾。

HAZOP は, 表 2-1 のガイドワードに基づき, 解析対象範囲におけるパラメータ (流量, 圧力, 温度, 組成等) にずれ (deviation) を与えることによって, 設計意図または動作条件からの逸脱の影響を網羅的に同定する。

表 2-1 HAZOP のガイドワード例

ガイドワードの例	内 容
No or Not	意図したことが全く起こらない。
More or less	パラメータの量的増加または減少
As well as	余分なことが起きる。(例: 不純物の混入等)
Part of	質的減少 (例: 一部の成分が減少, 不足)
Reverse	反対になる (逆になる)。
Sooner than or Later than	タイミングが早すぎる, 遅すぎる
Shorter than or Longer than	短時間すぎる, 長時間すぎる
Other	その他, 通常と異なって起きること。

表 2-2 は HAZOP ワークシートの事例である。ガイドワードから誘導される“ずれ”によって, 起こり得る結果およびその原因が考察され, 必要な対策措置が導出されている。

HAZOP は, システム要素が正常状態から逸脱し危害に至るまでの状態遷移プロセスを系統的に分析する手段を持たず, 多様なハザード, 例えば状態遷移順序に依存する, または同時に複数の要因に起因する等のハザードの分析は困難である。

表 2-2 HAZOP ワークシートの例

Guide waord	Deviation	Possible Causes	Consequence	Action required
None	No flow	Line fracture	Hydrocarbon discharged into area adjacent to public highway.	Institute regular patrolling & inspection of transfer line
More of	More temperature	High intermediate storage temperature	Higher pressure in transfer line and setting tank	Check whether there is adequate warning of high temperature at intermediate storage. If not, install.
Less of	Less temperature	Winter conditions	Water sump and drain line freeze up.	Lag water sump down to drain valve, and stream trace drain valve and drain line down stream.
Part of	High water concentration in stream
.....

(文献¹⁶⁾の Table1 : Operability study of proposed olefine dimerization unit: result for line section from intermediate storage to buffer/setting tank を修正引用)

(2) What-if 技法

What-if 技法は、HAZOP 同様、主に化学産業におけるプラントシステムの分析技法として開発され、その後用途が拡大した。ブレインストーミングにより、“もし~ならばどうなるか”、“もし~ならば何が起こるか”等の“ What-if ” 質問により起こり得る結果および推定原因が考察され、必要な対策措置が導かれる。ブレインストーミングは構造化されている場合と構造化されていない場合とがある²⁴⁾。

構造化 What-if 技法 (Structured “What-if” Technique: SWIFT) は、網羅性を高めるために、予め、“What if” または“How could” “などのフレーズで始まるプロンプトリストを準備し、構造化されたブレインストーミングを採用する²⁵⁾。

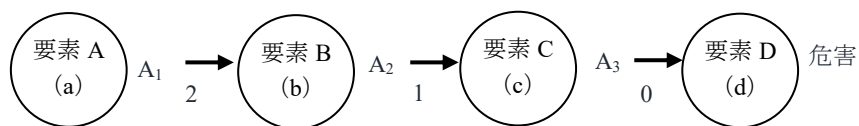
What-if 技法および SWIFT は、2.1.1 項 (1) の HAZOP と同じ理由で、状態遷移順序に依存する、または同時に複数の要因に起因する等のハザードの分析は困難である。

(3) A-C モデル (The Action Changes and the action-chains Model)

A-C モデルは、佐藤、井上、熊本によって提案されたハザードを同定・分析するための技法である^{45)~50)}。A-C モデルは、システムを構成する要素間の作用の授受と状態変化を作用連鎖図で図式化しハザードを表現する。S-A プロセスチャートは、A-C モデルの作用の概念を踏襲しており、また、ハザードの抑制のための原理を共有している⁵⁵⁾。ここでは、同一の危害に至るプロセスをそれぞれの技法で図式化し、両技法の差異について事例を用い具体的に考察する。

(a) A-C モデルおよび S-A プロセスチャートのハザード図式表現法

A-C モデルは、要素から要素への作用の伝播と状態変化を作用連鎖図で展開する。図 2-2 に A-C モデルにおけるハザードの図式現形式を示す。



No.	作用要素	被作用要素	作用	被作用要素	状態変化	
2	A (a)	から	に対して	B	の状態が	B (b)
1	B (b)			C		C (c)
0	C (c)			D		D (d)

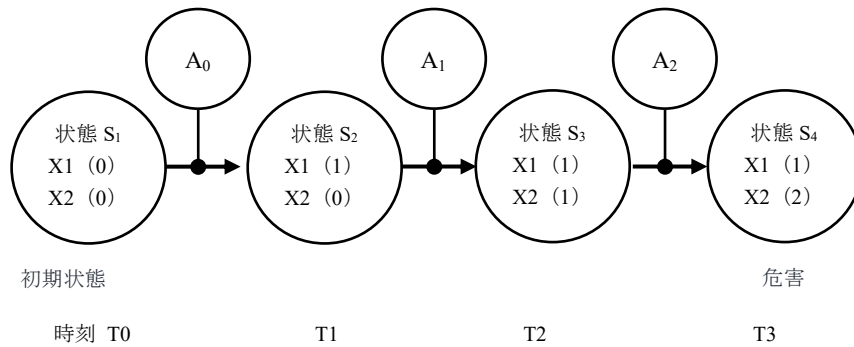
図 2-2 A-C モデルの図式表現形式

図 2-2 は、ある作用要素から被作用要素に対してある作用が行われ、被作用要素の状態が変化し、その変化がさらに作用となって次の要素に行われる一連の作用連鎖を表している。A-C モデルにおいて、作用は a) エネルギー伝播形作用、b) 情報伝達形作用、c) 作用原因物質転移形、d) 供給阻害系、e) 存在形態系、f) 機能不履行形に分類されている（詳細は 3.4 節参照）また、矢線の下値は、危害からの連鎖順序を示す。

次に、S-A プロセスチャートの図式表現形式の例を図 2-3 に示す。図 2-3 は、時刻 T0 のシステム状態 S₁ が、遷移作用 A₀ によって S₂ へ遷移、状態 S₂ が遷移作用 A₁ によって S₃ へ遷移、状態 S₃ が遷移作用 A₂ によって S₄ へ遷移するプロセスを表現している。図 2-3 において、システムの各状態は、システムを構成する要素 X1 の状態 X1 (k) 、および要素 X2 の状態 X2 (k') の組合せによって定義されている (k, k'=0,1,2,...) 。

A-C モデルはシステム要素間の作用連鎖を図式化して危害発現プロセスを展開する。そ

れに対して S-A プロセスチャートは、まずシステム状態を各システム要素の状態の組合せによって定義し、次にシステム要素の状態を変化させる遷移作用を順次組合せてシステムの状態遷移プロセスを展開し、危害に至るプロセスを同定する。



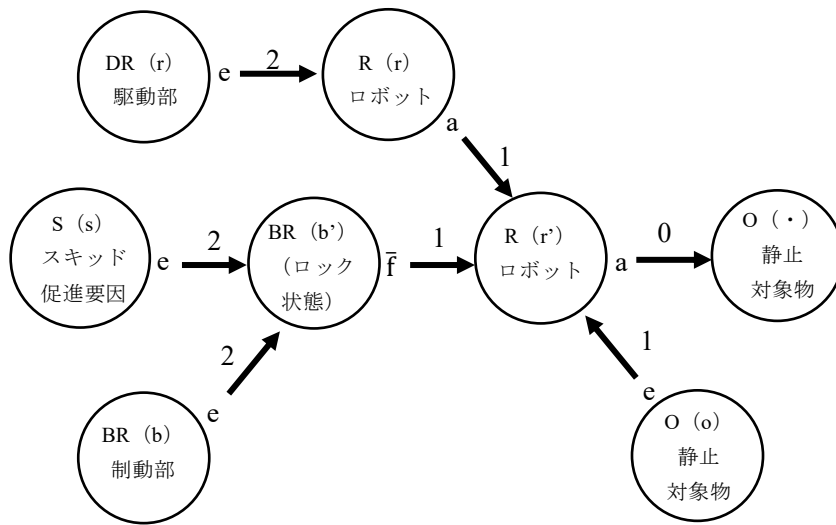
状態	遷移作用		状態
S1	が	A0: 要素 X1 の状態を 0 から 1 に変化させる作用	S2
S2		A1: 要素 X2 の状態を 0 から 1 に変化させる作用	S3
S3		A2: 要素 X2 の状態を 1 から 2 に変化させる作用	S4
		によって	に遷移する

図 2-3 S-A プロセスチャートの図式表現形式

(b) 自律形移動ロボットのスキッドに起因するハザードと抑制策の図式表現例

本項では、自律形移動ロボットのスキッドに起因するハザードを A-C モデルと S-A プロセスチャートで図式化し、2つの図式表現を具体的に比較する。

図 2-4 は、制動力“BR (b) e→”とスキッド促進要因 “S (s) e→” によって制動部 BR がロック状態“BR (b’)”に移行し、ロボット R が無制御走行状態で静止対象物 (O) と衝突するプロセスを A-C モデルを用い表している。矢線の左側に附した a, e, f は a) エネルギー伝播形作用, e) 存在形態系, f) 機能不履行形的作用を意味する。き損状態“O (•)” は、作用“O (o) e→”, “R (r) a→”, または “BR (b’) f→” のいずれかを抑制することで直接原因作用“R (r’) a→”を抑制 (解離) し、回避できる。



No.	作用要素		被作用要素	作用		被作用要素	状態変化	
2	DR (r)	が	R	駆動力	にあることで	R	R (r)	に変化する
	BR (b)		BR	制動状態		BR (b)	BR (b')	
	S (s)		BR	スキッド促進状態		BR (b)	BR (b')	
1	BR (b')	が	R	ロック状態	に対して	R	R (r')	に変化する
	O			移動経路				
	R (r)			慣性走行				
0	R (r')	から	O	運動エネルギー	が伝搬されて	O	O (・)	き損状態

図 2-4 A-C モデルによるスキッド起因のハザード (文献⁴⁵⁾, 図 6 を修正引用)

図 2-5 は、ロック状態“BR (b’)”の制御による抑制策の 1 例を表している。すなわち、滑り状態“RS (k)”をセンサ“SI”で検出し、“BR (b’) f→”に代わって制動力の ON-OFF 制御“BR (b’) a’→”を行うことによって（解離原理 P4:不履行機能の代替制御）⁴⁶⁾、R が制御停止状態“R (r’)”に変化し静止対象物との衝突を回避する。同時に、“R (r’) a→”が抑制（解離）される（解離原理 1: 作用源の制御）。

図 2-6 は、S-A プロセスチャートによる自律移動ロボットのハザード A、ハザード B、およびハザード C の図式表現例である。図 2-6 のハザード A は、図 2-4 の A-C モデルに対応している。図 2-6 は危害に至る次の潜在的状態遷移プロセスを表している。

ハザード A

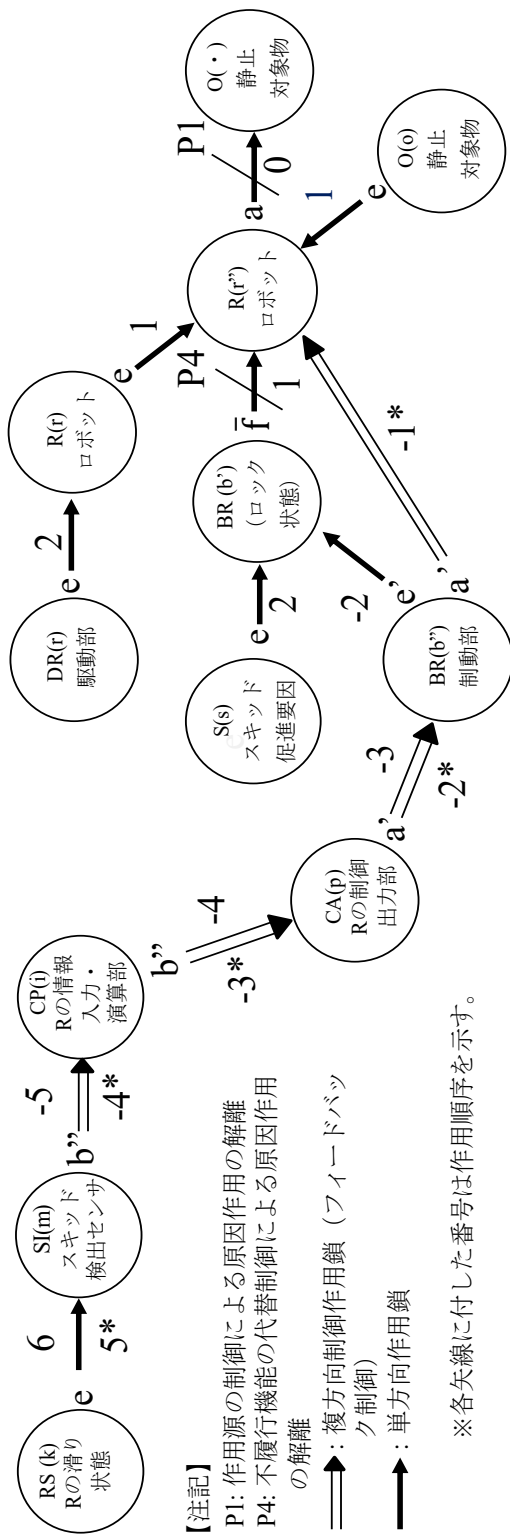
- (1) State1 が遷移作用 A1 によって State2 に遷移する。
- (2) State2 が遷移作用 A4 によって State3（走行状態）に遷移する。
- (3) State3 が遷移作用 A6 および A7 によって State4（慣性走行状態）に遷移する。
- (4) State4 が遷移作用 A2, A7 および A8 によって State5（無制御走行状態）に遷移する。
- (5) State5 が遷移作用 A9 によって State1’（衝突状態）に遷移する。
- (6) State1’ が遷移作用 A10 によってき損状態に遷移する。

ハザード B

- (1) State1 が遷移作用 A1 によって State2 に遷移する。
- (2) State2 が遷移作用 A4 によって State3（走行状態）に遷移する。
- (3) State3 が遷移作用 A8 および A7 によって State3’（滑りを伴う駆動走行状態）に遷移する。
- (4) State3’が遷移作用 A9 によって State7（衝突状態）に遷移する。
- (5) State7 が遷移作用 A10 によってき損状態に遷移する。

ハザード C

- (1) State1 が遷移作用 A1 によって State2 に遷移する。
- (2) State2 が遷移作用 A4 によって State3（走行状態）に遷移する。
- (3) State3 が遷移作用 A5 によって State8（加速状態）に遷移する。
- (4) State8 が遷移作用 9 によって State9（衝突状態）に遷移する。
- (5) State9 が遷移作用 10 によってき損状態に遷移する。



No.	作用要素		作用	被作用要素		状態変化	
	RS(k)	が		SI	が	SI(m)	検出状態
6	SI(m)	から	にあることで	SI	CP(i)	制御量演算状態	に変化する
5*	CP(i)	から	が伝達されて	CP	CA(p)	制御出力状態	
-5	CA(p)	から	が伝達されて	CA	BR(b'')	制御出力抑制状態	解離される
-4*	BR(b'')	が	があることで	BR	R(r')	正常な走行状態	
-4	BR(b'')	が	抑制された制動力	BR(b'')			
-3*	BR(b'')	が	抑制された制動力	R			
-3							
-2*							
-2							
-1*							

図 2-5 A-C モデルによる制動力の ON-OFF 制御衝突回避の図式表現例 (文献 (45), 図 7 を修正引用)

S-A プロセスチャートで表された 1 つのハザードから、遷移作用の順序を変える、または新しく遷移作用を与えることによって派生する別のハザードへの拡張が可能である。例えば、図 2-6 は、State1 (初期状態) ⇒ State2 ⇒ State3 の状態遷移プロセスの後、State3 に A6 および A7, A5 または A8 を組み合わせることによって、ハザード A から派生するハザード B およびハザード C を同定している。一方、図 2-4 の A-C モデルから、ただちに、ハザード B またはハザード C を導出することは困難である。このように、S-A プロセスチャートでは、システム状態に働く遷移作用の組み合わせを変えて、ハザードを図式的に拡張し展開することが容易である。また、S-A プロセスチャートでは、システム状態を常時明示するが、A-C モデルは、要素間の状態はわかるがシステム状態を明示しないので、システム全体の状態変化を追跡することが難しい。

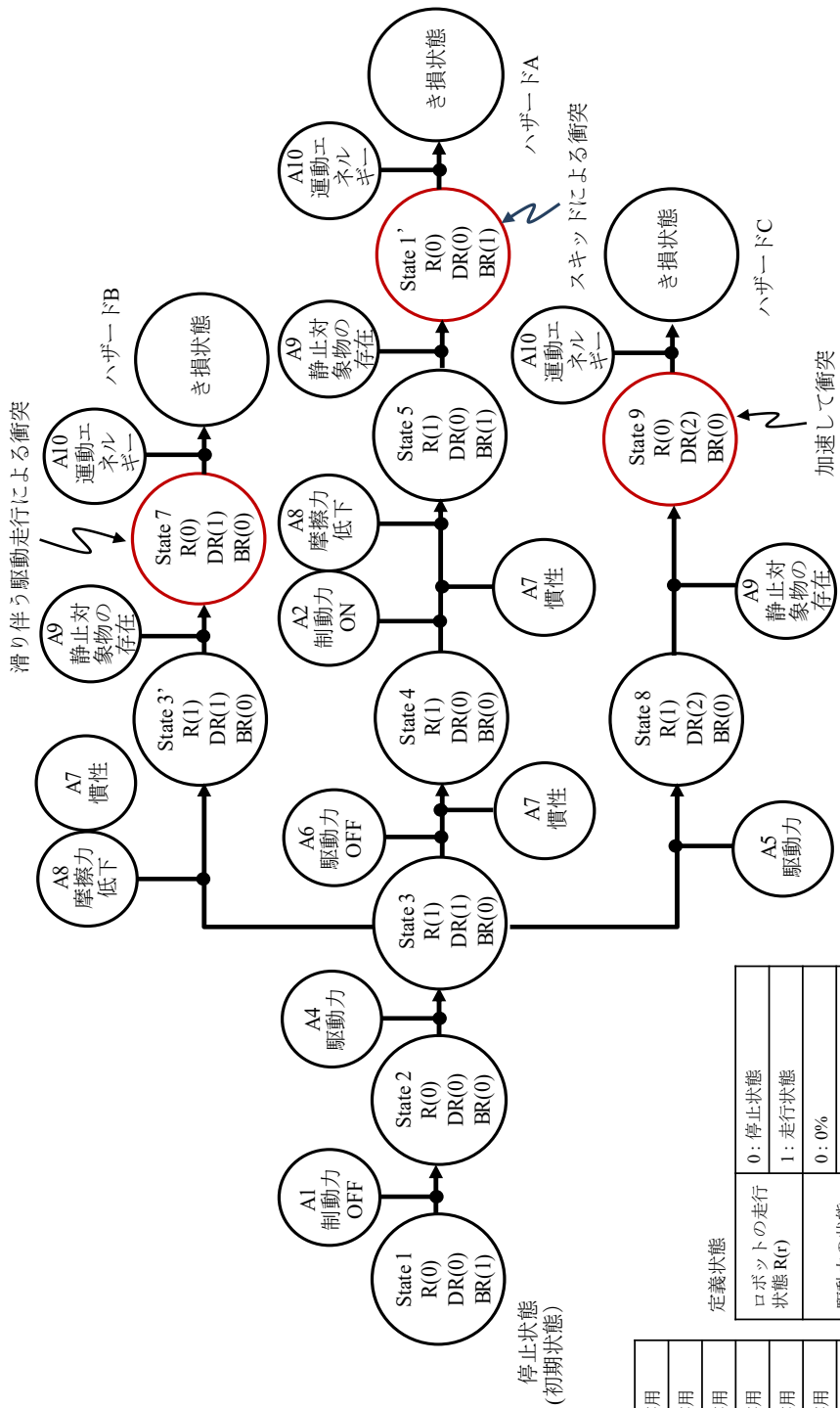
図 2-7 の S-A プロセスチャートは、ハザード A の抑制概念の図式表現である。図 2-7 は、自立移動ロボットのスキッドに起因するハザード A の次の (1) および (2) の抑制概念を表している。

- (1) 遷移作用 A2, A7, A8, A9, A10 を抑制作用 CA2, CA7, CA8, CA9, CA10 で除去または抑制する。
- (2) State5 の無制御走行状態を遷移作用 A3 および A10 で制御して State6 に遷移させる。

S-A プロセスチャートから導出される (1) および (2) のハザード抑制策と、図 2-4 の A-C モデルが示す抑制すべき作用 “BR (b) e→”, “S (s) e→”, “BR (b') f→”, “O (o) e→”, “R (r') a→” とは、次のように対応している。これは両手法が抑制概念を共有していることを示している。

- (1) “BR (b) e→” を抑制するための CA2
- (2) “S (s) e→” を抑制するための CA8
- (3) “BR (b') f→” を抑制するための CA2, A3, A7 および A11
- (4) “O (o) e→” を抑制するための CA9
- (5) “R (r') a→” を抑制するための CA10

しかし、5.2.2 項にて説明するが、ある特定のハザードでは、その抑制策の適用順序に制約が必要となる場合がある。



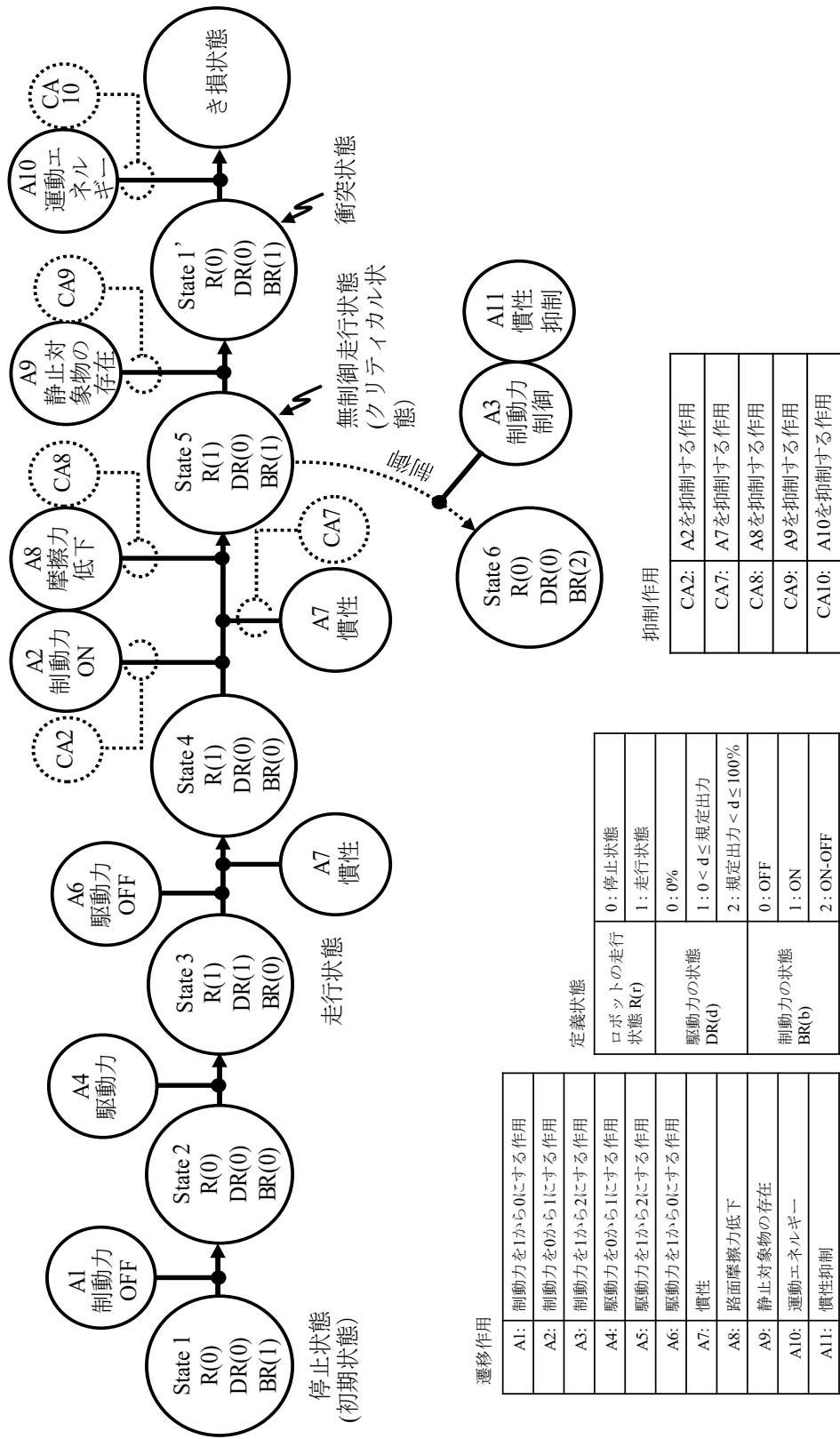
遷移作用

A1:	制動力を1から0にする作用
A2:	制動力を0から1にする作用
A3:	制動力を1から2にする作用
A4:	駆動力を0から1にする作用
A5:	駆動力を1から2にする作用
A6:	駆動力を1から0にする作用
A7:	慣性
A8:	路面摩擦係数低下
A9:	静止対象物の存在
A10:	運動エネルギー
A11:	慣性抑制

定義状態

ロボットの走行状態 R(r)	0: 停止状態 1: 走行状態
駆動力の状態 DR(d)	0: 0% 1: $0 < d \leq$ 規定出力 2: 規定出力 $< d \leq 100\%$
制動力の状態 BR(b)	0: OFF 1: ON 2: ON-OFF

図 2-6 S-A プロセスチャートによるスキッド起因のハザード



遷移作用	
A1: 制動力を1から0にする作用	
A2: 制動力を0から1にする作用	
A3: 制動力を1から2にする作用	
A4: 駆動力を0から1にする作用	
A5: 駆動力を1から2にする作用	
A6: 駆動力を1から0にする作用	
A7: 慣性	
A8: 路面摩擦力低下	
A9: 静止対象物の存在	
A10: 運動エネルギー	
A11: 慣性抑制	

定義状態	
ロボットの走行状態 R(c)	0: 停止状態 1: 走行状態
駆動力の状態 DR(d)	0: 0% 1: 0 < d ≤ 規定出力 2: 規定出力 < d ≤ 100%
制動力の状態 BR(b)	0: OFF 1: ON 2: ON-OFF

抑制作用	
CA2: A2を抑制する作用	
CA7: A7を抑制する作用	
CA8: A8を抑制する作用	
CA9: A9を抑制する作用	
CA10: A10を抑制する作用	

図 2-7 スキッド起因のハザード A の抑制概念

2.1.2 ハザードの分析技法

(1) FTA

FTA は、1961 年に米国国防省がベル電話研究所の技術者グレープの協力を得て、ミニットマンミサイルの発射制御システムの安全分析に用いられた^{27)~29)}。現在では航空、宇宙産業のみならず、原子力システム、民需産業等広範囲にわたる分野で用いられ、その適用方法は規格化されている^{30),31)}。FTA はシステムやシステム要素の望ましくない事象(頂上事象)と原因となり得る事象とを論理記号で展開し、ハザードの定性的および/または定量的分析を行う^{32),33)}。

可燃性ガス爆発を頂上事象とする FT の例を図 2-8 に示す。図 2-8 より次の分析が可能である。

頂上事象が生起するカットセット K_i は、

$$K_1 = \{S1.0, E1.1, E1.2\}$$

$$K_2 = \{S1.0, E1.1, E1.3\}$$

一方、頂上事象が生起しない最小の集合、パスセット P_j は、

$$P_1 = \{\overline{S1.0}\}$$

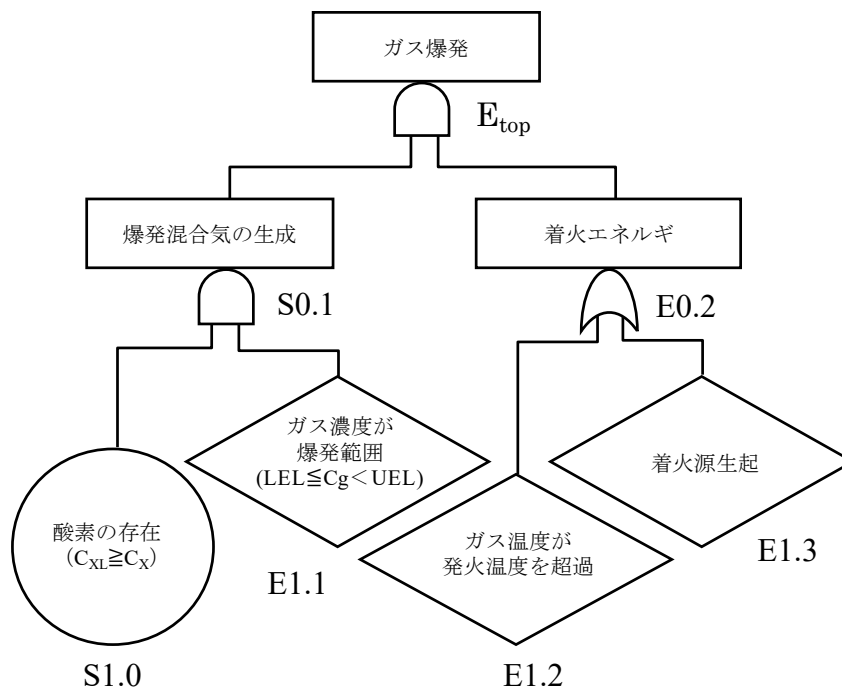
$$P_2 = \{\overline{E1.1}\}$$

$$P_3 = \{\overline{E1.2}, \overline{E1.3}\}$$

したがって、 $\overline{S1.0}$ 、 $\overline{E1.1}$ 、または $\overline{E1.2}$ および $\overline{E1.3}$ のいずれかが生起すれば、ガス爆発は発生しない(ここで、 $\overline{\quad}$ は否定論理記号を意味する)。

また、中間事象である E1.1, E1.2, E1.3 をさらに基本事象まで展開し、必要最小限の基本事象の組み合わせ(最小カットセット)を求め、基本事象の発生確率より各最小カットセットの発生確率を算出する。すべての最小カットセットの発生確率を求め合計すると頂上事象の発生確率が求められる。また、各最小カットセットを構成する事象の 1 つを発生率(1/時間)とし、他の事象を確率で与えた場合、頂上事象は発生率として求められる。

第 6 章にて論じるが、システム要求機能の失敗を頂上事象とする FT は主に 2 状態システムを前提とする。一方、危害を頂上事象とするハザード分析のための FT は、多状態システムを前提とする必要がある。



- UEL : 爆発上限界濃度 (vol %)
- LEL : 爆発下限界濃度 (vol %)
- C_g : 可燃性ガス濃度 (vol %)
- C_X : 乾燥設備内の酸素濃度 (vol %)
- C_{XL} : 爆発限界酸素濃度 (vol %)
- ∩ : AND ゲート
- ∪ : OR ゲート

図 2-8 可燃性ガス爆発の発生原理

(2) FMEA (Failure Modes and Effects Analysis)

FMEA^{24), 26), 27), 36)~40)} は信頼性分析技法として米国で開発され、その起源は 1949 年制定の米軍規格 MIL-P-1629 にあるとされている⁵⁶⁾。FMEA は、システムを構成するサブシステム、部品、要素の故障モードを洗い出し、下位システム要素の単独故障モードの影響が上位システムへ伝搬し最終的に全体システムに起りうる危険事象、失敗、危害等を特定する。また FMECA (Failure Mode, Effects and Criticality Analysis) は、FMEA を拡張してリスク尺度の 1 つである致命度解析を行う。FMEA は単独故障モードによるシステムの影響を評価し、他の故障モードが組み合わさった場合の分析が困難である。また、故障モード

の影響が、システム外に波及してどのような危害に至るかについての系統的な分析手段は持たない。FMEA ワークシートのフォーマットは多数あり、その 1 例を表 2-3 に示す。

表 2-3 FMEA ワークシートのフォーマット例
(IEC 60812:2018²⁶⁾ の Table F.12 より抜粋引用)

Name	Component	Function	Failure rate [FIT]	Failure mode	Failure mode ratio	Effect	Behaviour effect S: Safty D: Dangerous	Diagnostic coverage
F50	Fuse	Short-circuit protection at the input	25	Fail to open	50 %	None in normal operation	No effect	—
				Premature open	10 %	Outputs deenergized	S	—
				Slow to open	40 %	No effect on safety function	No effect	—
D12	Suppressor diode	Over voltage protection (EMC)	7	Short	95 %	F50 blows	S	—
				Open circuit	5 %	No effect on safety function	No effect	—
R100	Resistor, SMD	Current limitation, EMC	0.2	Short	5 %	No current limitation – failure	D	60 %
				Open	65 %	Outputs deenergized	S	—
				Parameter change	30 %	Function still given	No effect	—
C13	Capacitor ceramic, HDC / MDC	EMC	2	Short	50 %	F50 blows	S	—
				Open	30 %	None in normal operation (no protection)	No effect	—
				Change in value	20 %	Function still given	No effect	—
D25	Small signal diode, < 0,1 W	Bridge rectifier	1	Short	50 %	F50 blows	S	—
				Open	35 %	No correct rectification in case of AC supply	S	—
				Parameter change	15 %	Function still given	No effect	—

(3) ETA (Event Tree Analysis)

ETA^{24), 34), 35)}は、システム全体を分析する技法ではなく、システム内で生じたトリガーとなる起回事象を出発点として、システムが持ついくつかの防護層が失敗する場合と成功する場合に分けてイベントツリーを展開する。図 2-9 のイベントツリーは、起回事象から到達し得る結果とそのプロセスを危害発現シナリオとして表現している³⁴⁾。各事象に対して FTA を行ない、各事象の発生頻度、発生確率等をあらかじめ算出しておけば、各結果の定量的分析が可能である。

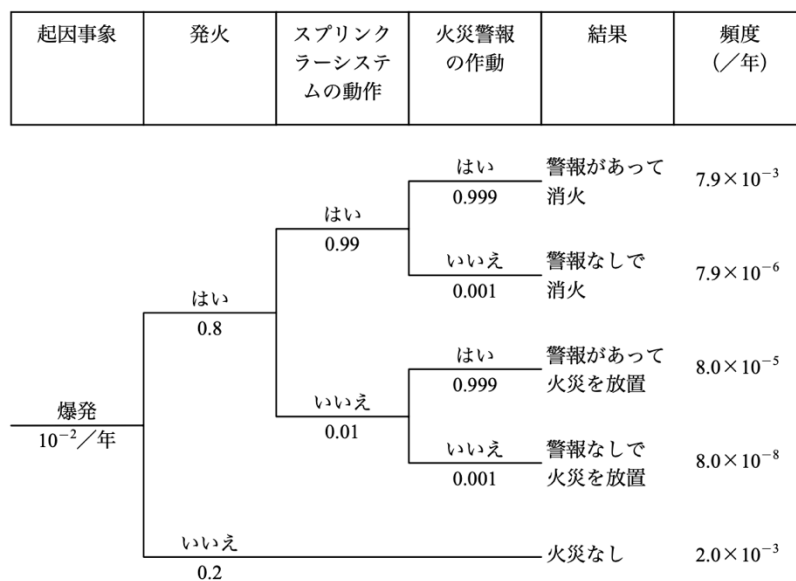


図 2-9 イベントツリーの例 (JIS Q 31010 : 2012 図 B.3 より抜粋引用)

(4) STPA (System-Theoretic Process Analysis)

STPA は、STAMP (Systems-Theoretic Accident Model and Processes) に基づき Nancy G. Leveson によって提案されたハザードの分析技法である⁵¹⁾⁻⁵³⁾。STPA は、システム要素間の相互作用に注目して、システムの要素間の不適切な相互作用によって引き起こされる損失を分析する。STPA は、ハザードを、

損失を引き起こすシステムの状態、すなわち特定の最悪の環境条件を伴うシステム条件の集合

(A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss)

また、損失を、

損失には利害関係者にとって価値のあるものが含まれる。損失には、人命のまたは人的傷害の損失、物的損害、環境汚染、任務の損失、評判の損失、機密情報の損失または漏洩、またはその他の利害関係者に受け入れられない損失が含まれる。(A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders)

と定義している⁵¹⁾。

STPA のハザードの定義は、JIS Z 8051 , JIS B 9700 等の安全規格とは異なる定義であることに留意する必要がある⁵⁴⁾。STPA は、システムをコントロールアクションおよびフィードバックを行うシステム要素でモデル化し、あるコンテキストにおけるコントロールアクションのずれによって起こり得る望ましくないシナリオを導出する。

STPA は、次の手順でハザードを分析する。

第1ステップ

- ・損失を特定する。
- ・損失を引き起こす危険状態、すなわちハザードを特定する。

第2ステップ

- ・システム（コントロールストラクチャー）を定義する（図 2-10 参照）。

第3ステップ

- ・要素間に働く非安全なコントロールアクション（UCA）を特定する。UCA とは、ある特定のコンテキストと最悪の環境下でハザードにつながるコントロールアクション（CA）である。UCA は CA に対して、次の a) ～d) に示す 4 種類のガイドワードを与え導出する。

- (a) CA（コントロールアクション）が与えられない（Not providing）
- (b) CA が与えられる（providing causes hazards）
- (c) 早すぎる、遅すぎる、順序が間違っている（incorrect timing, order causes hazards）
- (d) 早すぎる停止、長すぎる適用（stopped too soon / applied too long）

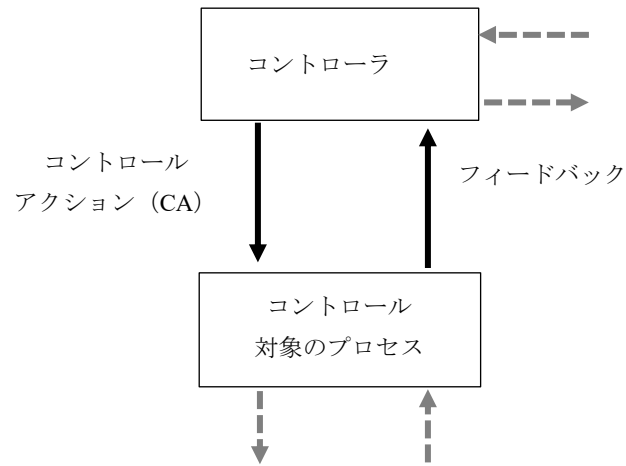


図 2-10 コントロールストラクチャーの例 (文献⁴³⁾を修正引用)

UCA は、図 2-11 のように構成する。図 2-11 の例は、走行中の自動車における UCA であり、損失は“停止に失敗して追突”，ハザードは“タイヤのロック状態”を想定している。コンテキスト (Context) とは、ハザードが起こる特定の状況、条件等を意味しており、損失が起こるための必要条件として位置付けられる。

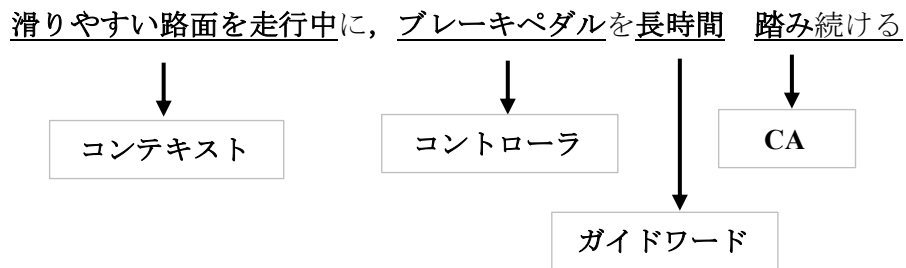


図 2-11 非安全なコントロールアクション (UCA) の例

第4ステップ

- ・ 非安全なコントロールアクション（UCA）毎に，安全要件または制約（SRC：Safety Requirement or Constraint）を設定する。安全要件または制約とは，例えば図 2-11 のUCAを禁止する安全要求事項“滑りやすい路面を走行中に，ブレーキペダルを長時間踏み続けない”を設けることである。
- ・ UCA 毎に，UCA が起こるシナリオおよびその原因を考察する。
- ・ UCA が起こるシナリオ毎に，その軽減措置（Mitigating Measure）を検討する。

STPA は，HAZOP 同様，あるコンテキストにおいて起こる CA のずれに着目する定性的技法である。STPA では，ある状況（コンテキスト）では安全側事象（CA のずれによるフィードバックの変化）が，別の状態では危険側事象となり得る。ただし，STPA は，発現し得る損失およびその発現プロセスを網羅的に同定する技法ではなく，すでに特定された損失に基づき事故シナリオを導出し，抑制策を考察する。

STPA はシステム制御モデルを用いた動作仕様の検証技法を拡張し安全分析技法として体系化したものと考えられる。ハザードをより詳細に分析するためには，システムレベルの事象および状態だけでなく，これを生成させるシステムの要素レベルの変化との関係を明らかにする必要がある，FTA 等の分析技法と組み合わせて用いることが望ましい。

2.2 S-A プロセスチャートの特徴と従来技法との比較

S-A プロセスチャートは，状態と作用の生起順序に着目したハザードの動的解析技法であり，ハザードを次々と変化する状態および事象の連鎖として把握し可視化する。この特徴によって，相反するハザード，可変する安全状態等の多様なハザードの識別が可能となる。この観点から S-A プロセスチャートと従来技法との特徴を比較したものが表 2-4 である。S-A プロセスチャートは自身の目的を達成するために不可欠な特徴，すなわち，

- ハザード同定の網羅性
- ハザードの可視化（図式化）
- 事象生起順序依存型ハザードの特定
- 安全方策の系統的展開

において，他の技法に対して適用可能性が高い。

表 2-4 ハザード同定・分析技法の特徴比較

項目	S-A プロセスチャート	HAZOP	What-if	A-Cモデル	ETA	FTA	FMEA	STPA
手 段	S-Aプロセス チャート	ワークシート	ワークシート	作用連鎖図	イベントツリー	フォールトツリー	ワークシート	コントロール ストラクチャ
ハザード同定の 解 説 性	○ システムの初期状態に 遷移作用を組合せて状 態遷移を展開し到達し 得る危害を特定する。	△～○ ガイドワードに基づき ずれを設定して、意図 した状態から逸脱した 望ましくない状態を特 定する。	△ 望ましくない事象を What-if質問で展開し起 りうる危害を特定する 。	△～○ システム要素又はシス テムに働きうる作用を 設定して作用連鎖図を 展開し起りうる危害を 特定する。	× 適用不可	× 適用不可	△ 下位システム要素の単 独故障モードの影響が 上位システムへ伝搬し 最終的にシステム全体 に起りうる危害を特定 する。ただしシステム 内の単独故障に起因す る危害に限定	× 適用不可
ハザードの可視化(危 害発現プロセスのわか りやすさ)	○ 初期状態から危害発現 までの一連のプロセス が図式化される。	× 適用不可	× 適用不可	△～○ 危害発現プロセスが作 用連鎖図で図式化され る。ただし、システム 全体の状態遷移の流れ がわかりにくい。	△ 限定的：起因事象から 危害までのシクエン スが図式化される	△ 限定的：頂上事象を展 開し、優先AND構造を 用いることによって事 象の進行が左から右へ 表現可能となる。	△ 限定的：あるシステム 要素の故障モードによ る影響の伝搬経路を追 跡し、起り得る危害 がワークシートで展開 される。	△ システム間のコント ロールのずれ等によっ て生起する望ましくな い(非安全な)シナリ オを記述する。
事象生起順序依存型 ハザードの識別	○ システムレベルで 適用可能	× 適用不可	× 適用不可	△ 適用可能	× 適用不可	△ 適用可能	× 適用不可	△ 適用可能
危害発生原因の 特定	△ システムレベルで 分析可能	△ システムレベルで 分析可能	△ システムレベルで 分析可能	△ システム要素 及びシステムレベルで 分析可能	× 適用不可	○ システム要素 及びシステムレベルで 分析可能	× 適用不可	△ システムレベルで 分析可能
危害発生 定量的分析	× 適用不可	× 適用不可	× 適用不可	× 適用不可	△ 限定的：危険状態発生 ～危害までの発生確率 を算出	○ システム要素 及びシステムレベルで 広範囲に分析可能	× 適用不可	× 適用不可
安全対策の 系統的展開 (安全対策導出までの 仕組みはあるか?)	○ ハザードの抑制原理を 用い系統的かつ適用順 序を考慮した安全対策 の展開が可能	△ 危害発現シナリオ毎に その軽減措置を検討す る。	△ 危害発現シナリオ毎に その軽減措置を検討す る。	○ ハザードの抑制原理を 用い系統的に安全対策 の展開が可能	△ 多重防護の妥当性の検 証が可能	△ 最小カット集合を求め 危害を発生させる重要 度の高い事象を特定し それを抑制する。	△ システム全体に及ぼ す影響度の高いシステ ム要素を抽出し重点的 に対策する。	△～○ 安全要件又は制約を設 定し、シナリオ毎に その軽減措置を検討す る。

○：十分に適用可能 △：適用可能 ×：適用不可

2.3 S-A プロセスチャートと従来技法との関係

S-A プロセスチャートは、システム要素レベルの分析に適しておらず、また、危害の定量分析にも適用できない。しかし、**図 2-12** に示す従来技法との関係に基づきその弱点を補うことが可能である。

図 2-12 は S-A プロセスチャートを用い、後方車が前方車に追突する危害発現プロセス①～⑥とそれを抑制するための抑制作用 CA1, CA2, CA3, 制御 1, 制御 2 の危害抑制プロセス①～④を表している。また、S-A プロセスチャートと A-C モデル, ETA, FTA との相互関係を表している。

図 2-12 の危害発現プロセスおよび危害抑制プロセスは次のとおりである。

【危害発現プロセス】

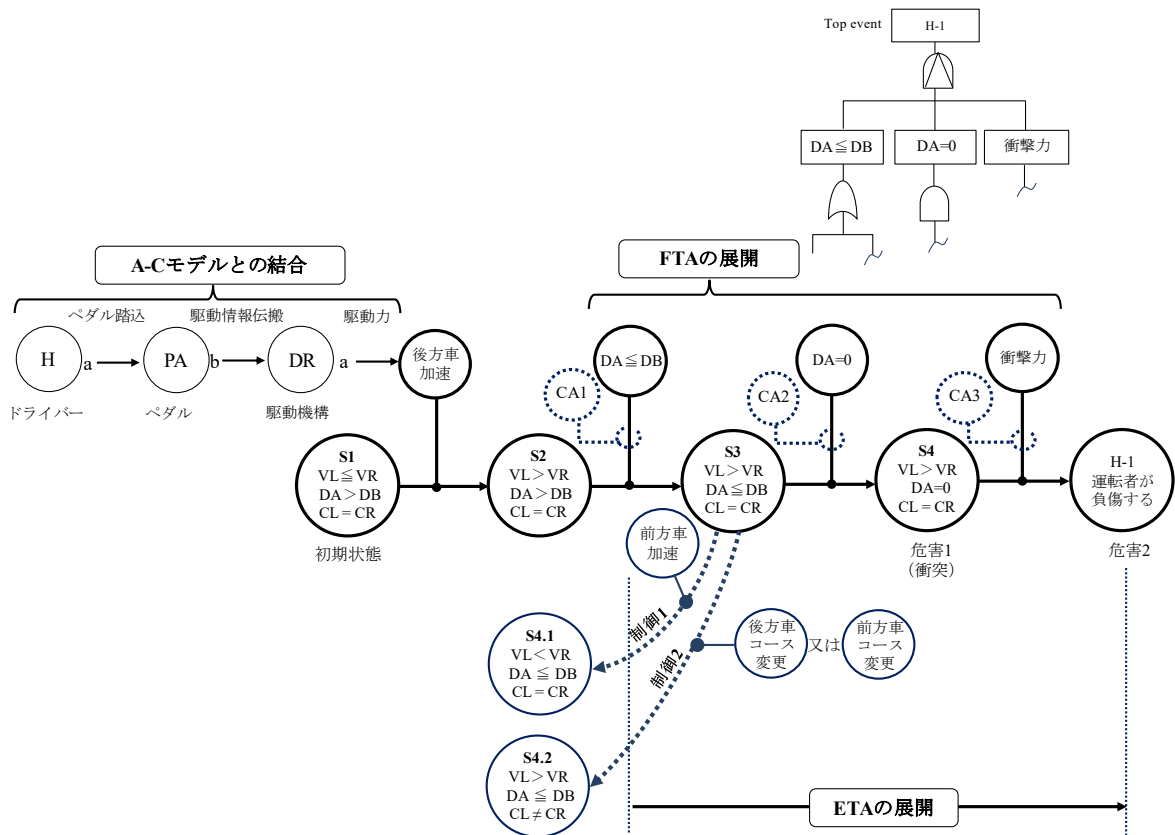
- ① 後方車が前方車と同じまたは低速 ($V_L \leq V_R$) で十分な車間距離 ($DA > DB$) を保ちながら同一コース ($CL = CR$) を走行している (状態 S_1)。
- ② 後方車が加速する。
- ③ 後方車の速度が前方車の速度を超える ($V_L > V_R$)。(状態 S_2)
- ④ 車間距離が縮小し危険距離 ($DA \leq DB$) となる。(状態 S_3)
- ⑤ 後方車が前方車に衝突 ($DA=0$) する (状態 S_4)。
- ⑥ 衝撃力によって運転者が負傷する (H-1)。

【危害抑制プロセス】

- ① 遷移作用 “ $DA \leq DB$ ” を抑制作用 CA1 で抑制する。
- ② 制御 1 または制御 2 によって状態 S_3 からより安全な状態に遷移する。
- ③ 遷移作用 “ $DA = 0$ ” を抑制作用 CA2 で抑制する (急ブレーキ等)。
- ④ 遷移作用 “衝撃力” を抑制作用 CA3 で抑制する (エアバッグ等)。

S-A プロセスチャートによる危害発現プロセスおよび危害抑制プロセスの同定・分析結果と A-C モデル, ETA および FTA との次の相互補完①～③が可能である。

- ① 遷移作用の起源を A-C モデルで遡る。
- ② 危害の方向へと進む遷移作用を AND 優先ゲートを用い FTA に変換し、システム要素レベルまで分析を展開する (第 6 章)。
- ③ ある危険事象を起点として各抑制プロセスを経由して危害に至る危害発現シナリオを ETA で分析する。



起回事象	制御1	制御2	CA2	CA3	結果	確率 (近似)
DA ≤ DB (車間距離不十分) P_A	成功				衝突回避	P_A
	P_B 失敗	成功			衝突回避	$P_A \times P_B$
	P_B 失敗	P_C 失敗	成功		衝突・軽傷	$P_A \times P_B \times P_C$
	P_B 失敗	P_C 失敗	P_D 失敗	成功	衝突・軽傷	$P_A \times P_B \times P_C \times P_D$
	P_B 失敗	P_C 失敗	P_D 失敗	P_E 失敗	衝突・重症	$P_A \times P_B \times P_C \times P_D \times P_E$

【記号】

VL：後方車速度

VR：前方車速度

DA：進行方向に対する車間距離

DB：ブレーキ制動距離（ブレーキ作動後、停止するまでの距離）

CL：後方車進行コース

CR：前方車進行コース

図 2-12 S-A プロセスチャートと従来技法との関係

第3章 S-A プロセスチャートの理論的枠組みと構築方法

第3章では、潜在的危険発現プロセス（ハザード）を図式表現するためのS-A プロセスチャートの理論的枠組みと構築方法について論じる。

3.1 本論文におけるハザードモデル

ハザードは次々と変化する状態および事象の連鎖として表現することが可能である。例えばあるシステムが、 a 個の異なる状態を持つシステム要素 X_e ($e=0,1,2,\dots,a$)、 b 個の異なる状態を持つシステム要素 Y_g ($g=0, 1, 2,\dots,b$)、 c 個の異なる状態を持つシステム要素 Z_f ($f=0,1,2,\dots,c$) で構成されているものとする。すると、システム状態 S_y ($y=1, 2, \dots,u$) は、各システム要素の組合せによって、 $S_1=\{X_0, Y_0, Z_0\}$ 、 $S_2=\{X_1, Y_0, Z_0\}$ のように表せる。次に、各システム要素の状態を変化させる作用（以下、遷移作用） A_m ($m=0, 1, 2,\dots,r$) を組み合わせて、システムの状態遷移を、**図 3-1** のように表すことができる。**図 3-1** は、あるシステムの状態 S_1 が遷移作用 A_0 によって S_2 に遷移するプロセスを図式化している。

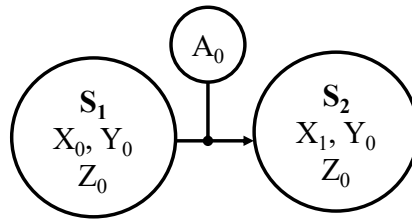


図 3-1 システム状態遷移の図式表現例

図 3-2 は、初期状態 S_1 から危害に至る潜在的状態遷移プロセス、すなわちハザードの概念を表している。**図 3-1** の状態 S_1 および S_2 に、さらに遷移作用 A_1, A_2, \dots, A_m が働くことによってシステム状態が次々と遷移し、状態 $S_y\{X_e, Y_g, Z_f\}$ 、状態 $S_y''\{X_e, Y_g', Z_f'\}$ において何らかの危害が発現したとき、 S_1 から危害 1、危害 2 を生起させる最終状態 S_y, S_y'' に至る状態遷移プロセス 1, 3, 4 は、あるハザードを表している。状態遷移プロセス 1 と 3 とは、最終状態は同じだが異なるプロセスを持つため異なるハザードとみなされる。一方、 S_1 から危害が発現しない最終状態 $S_y'\{X_e, Y_g', Z_f\}$ に至る状態遷移プロセス 2 はハザードではない。

本論文では、システム状態、状態を変化させる遷移作用、およびある状態と次の状態をつなぐ矢線を用い左から右へ時系列的に表された**図 3-2** の様な状態遷移連鎖図を S-A プロセスチャート（State-Action Process chart）と呼ぶ。

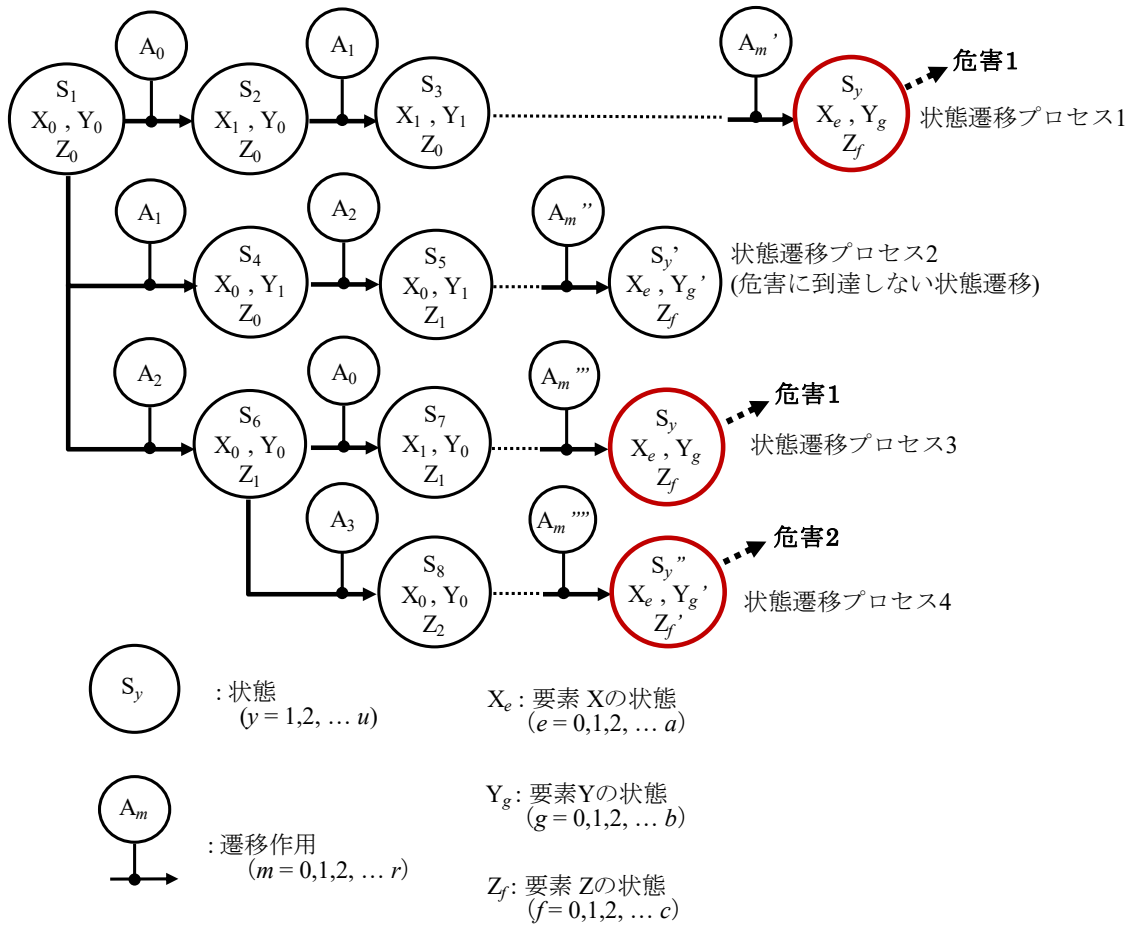


図 3-2 ハザード（潜在的危険発現プロセス）モデル

3.2 遷移作用と事象の関係およびその図式表現

S-A プロセスチャートにおける遷移作用は、システム内部または外部の要素の状態変化、すなわち事象に伴って生起する。図 3-1 は、厳密には図 3-3 のように表すことができる。図 3-3 は、次の①～③の状態遷移を表している。

- ① 要素 1 の状態変化 $a \rightarrow a'$ (事象 1) によって遷移作用 A_0 が生起する。
- ② 要素 X_0 が遷移作用 A_0 によって X_1 に変化する。
- ③ 要素 X_0 が X_1 に変化すると同時にシステム状態 S_1 が S_2 に変化する。

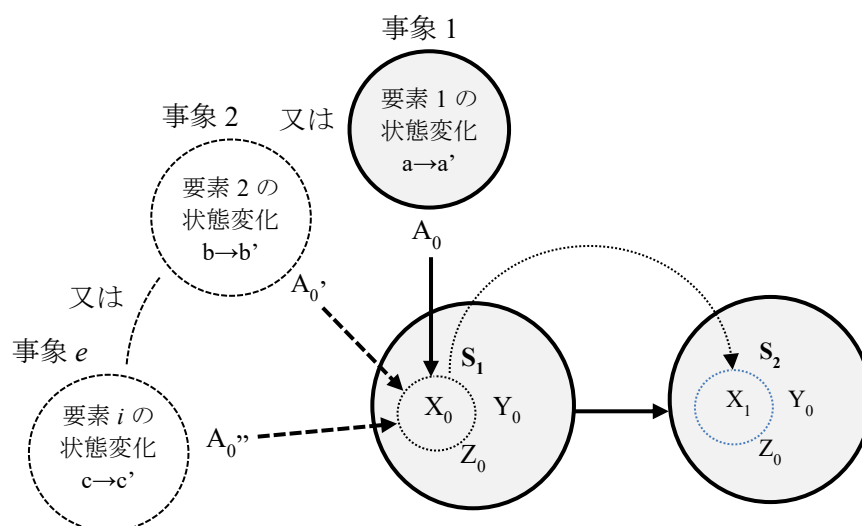


図 3-3 遷移作用と事象との関係

ある A_0 に対して、 A_0 と同様の作用を生起させる事象は 1 個に限定されず、事象 2, ... 事象 e が A_0' , A_0'' を生起させ得る。例えば、遷移作用“熱エネルギー”を生起させる事象は、ヒータ ON, 摺動運動の開始, 高温表面が接触, 等が存在する。このような S-A プロセスチャートにおける事象と遷移作用との関係は、A-C モデルにおける作用連鎖の概念に準拠している。(図 2-2 A-C モデルの図式表現形式参照)

A_0 を 1 個に特定せず S-A プロセスチャートを展開する場合は、3.5.2 項に示す方法で遷移作用を $A_{ij}(k, k')$ のように抽象化して表す。

A_0 を生起させる事象を特定して表す場合は、遷移作用を”ヒータ ON”，“熱分解反応の開始”，”高温表面に接触”等の具体的な事象表記に置き換えて図 3-4 のように S-A プロセスチャートを展開する（第 4 章参照）。

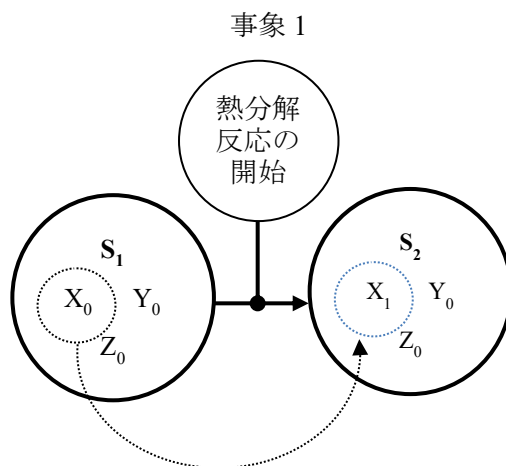


図 3-4 作用の事象表記による遷移作用の表現例

3.3 離散事象システムモデルと S-A プロセスチャートとの関係

S-A プロセスチャートは、システムの状態が内部および外部からの作用によって次々と変化して危害に至るプロセス、すなわちハザードを可視化するための図式表現形式である。S-A プロセスチャートは、システムの初期状態から危害に至る状態遷移プロセスをシステム状態、状態を変化させる遷移作用およびある状態と次の状態をつなぐ矢線を用い表し、システム状態の遷移を左から右へたどりながらハザードを解析する（図 3-5）。離散値を持つシステム要素の組合せによって表されるシステム状態は、事象生起に伴って生起する遷移作用によって次の状態へと遷移する。事象は時間幅を持たず瞬間的かつ不規則な時間間隔で生起する。システム制御分野では、状態が離散値をもつシステムを離散状態システムと呼ぶ^{57), 58)}。また 事象の生起により状態が遷移するシステムを事象駆動 (Event-Driven) であるといい、事象駆動の離散状態システムを離散事象システム (Discrete Event System) という。離散事象システムの代表的な図式表現形式であるペトリネット^{59), 60)}、オートマトン⁶¹⁾等は、システムの制御仕様を表すための論理モデルとして広く用いられる。対象とするシステムは人工システムであり、状態遷移はシステム内で所定の論理関係が成立したときに成立する。これらの論理モデルは、システムの論理的動作およびその検証等に用いられる。また、不適切な制御に起因して生起する危険状態の洗い出しにも適用される^{39), 62)~64)}。

S-A プロセスチャートもまた離散事象システムの図式表現であるが、その主目的は潜在的危険発現プロセスの洗い出し、すなわち、ハザードの同定・分析とその抑制策の導出である。対象とするシステムは人工システムに限定されず、外圍環境、人等を含む。状態遷移プロセスはシステム内での所定の論理関係に制限されず、システム内部または外部の故障、エラー、失敗、修復、回復、その他物理法則に従う事象に伴って生起する遷移作用（第3章参照）によって行われる。S-A プロセスチャートは、未知の遷移作用を設定して状態遷移プロセスを展開し、さらにFTA（Fault Tree Analysis）と関連付けて状態遷移の原因となる事象群の洗い出し、および分析をシステム要素レベルまで行うことが可能である（第6章参照）。

3.4 遷移作用の分類

S-A プロセスチャートでは、A-C モデルに準拠して遷移作用を分類する。A-C モデルは、潜在危険制御系の安全要求機能達成のために同定された制御連鎖において、制御連鎖を抑制作用および解離作用でモデル化し、作用を次の秩序状態作用と無秩序状態作用とに分類している^{43), 50), 65), 66)}。

(1) 秩序状態作用

(a) エネルギー伝播形作用

力学的（運動、位置）熱的、機械的、電氣的、放射等のエネルギーによる作用。エネルギーが伝播された要素には、エネルギー変換による変化が生ずる。

(b) 情報伝達形作用

情報伝達による作用。情報が伝達された要素には、その制御系等の状態に変化が生ずる。

(c) 作用原因物質転移形

(a)、(b) 以外の物質として認識可能な物質（化学物質、重量物、高温物質、放射性、腐食性物質、病原体等）の転移による作用。作用原因物質が転移された要素には、化学変化、ポテンシャルエネルギー、濃度の増大等の変化が生じる。

(d) 供給障害系

ある要素に、(a)～(c)の必需があつて、それに対する供給を妨害することによる働きかけ。供給障害作用を受けた要素には、例えば人間ならば窒息、装置ならば運転停止等の変化が生ずる。

(e) 存在形態系

(a)～(d)、(f)を伴わない要素の形状、形態、質量、条件、状態等による働きかけである。

(2) 無秩序状態作用

(f) 機能不履行形

(a) ~ (e) が発現しないことによる作用（機能不履行形作用）

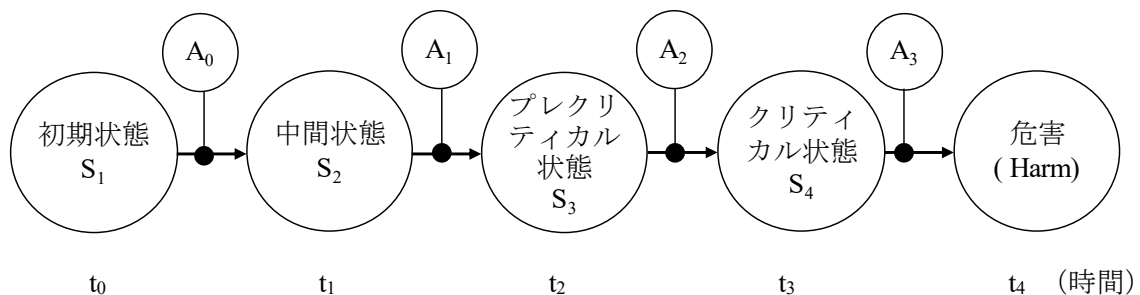
秩序状態はシステムのアップ状態に相当し、無秩序状態はダウン状態に相当する。例えば、電気回路が設計図とおりであるアップ状態は1つであるが、断線や短絡が存在するダウン状態は、無数に起こり得る。秩序状態作用はシステム要素間の秩序状態における相互作用である。無秩序状態作用は、システム要素間の無秩序状態における相互作用である。無秩序状態作用は、秩序状態作用の不履行により生ずる。

3.5 S-A プロセスチャートの基本構成

S-A プロセスチャートは、次の (a) ~ (h) の規則に従って状態と遷移作用とを識別しハザードを同定する。

(a) 図 3-5 の状態遷移プロセス①~④は、S-A プロセスチャートの基本構成を表している。

- ① 時刻 t_0 において、初期状態 S_1 が遷移作用 A_0 によって中間状態 S_2 に遷移する。
- ② 時刻 t_1 において、 S_2 が遷移作用 A_1 によってプレクリティカル状態 S_3 に遷移する。
- ③ 時刻 t_2 において、 S_3 が遷移作用 A_2 によってクリティカル状態 S_4 に遷移する。
- ④ 時刻 t_3 において、 S_4 が遷移作用 A_3 によって危害に遷移する（時刻 t_4 ）。



- ・初期状態 (initial state) : S-A プロセスチャートの起点の状態
- ・中間状態 (intermediate state) : システムの初期状態以外の正常な状態
- ・プレクリティカル状態 (pre-critical state) : 初期状態、または中間状態から遷移した状態であり、システムの正常な状態から逸脱し、かつクリティカル状態に遷移する前の状態
- ・クリティカル状態 (critical state) : ある遷移作用によって危害に遷移し得る状態

図 3-5 S-A プロセスチャートの基本構成

- (b) 状態は、初期状態、中間状態、プレクリティカル状態、クリティカル状態および危害（状態）に分類される。
- (c) S-A プロセスチャートでは、単一または複数のクリティカル状態が存在する。
- (d) S-A プロセスチャートでは、単一または複数の中間状態が存在する場合、または中間状態が存在しない場合がある。
- (e) S-A プロセスチャートでは、単一または複数のプレクリティカル状態が存在する場合、またはプレクリティカル状態が存在しない場合がある。
- (f) 状態遷移は、単一または複数の遷移作用によって起こる。
- (g) 遷移作用は時間幅を持たず瞬間的かつ不規則な時間間隔で生起する。
- (h) 危害は状態が矢印の方向、すなわち左から右へ遷移することにより発現する。

3.6 ハザード同定のための S-A プロセスチャートの展開方法

ハザードの同定は、①～③に示す手順（図 7-1 参照）で行う。

- ① システムの初期状態および遷移作用を設定する。
- ② システムの初期状態に各遷移作用を組合せる。
- ③ システム状態遷移プロセスを展開し到達し得る危害を同定する。

遷移作用は、“温度が上昇する”，“扉を開ける”，“人の存在 “のように、実際のシステムに変化を与える具体的な事象を想定し設定する。3.4 節の遷移作用の分類は、遷移作用を想定するための重要なヒントを与える。状態遷移プロセスは、遷移作用の順序を変える、または新たに遷移作用を追加することによって拡張される（第 4 章参照）。この技法は、あるシステムに関連して発現し得るシステム内部および外部の危害発現シナリオを洗い出す。

3.7 状態遷移経路分析のための S-A プロセスチャートの展開方法

S-A プロセスチャートでは、ある特定された危害に関して各システム要素が持つ状態遷移プロセス特性を定義することによって、システム状態の遷移可能な状態とその経路が、一義的に導出可能である（第 5 章参照）。遷移可能なシステム状態に、危害（状態）が含まれる場合、初期状態から危害へ至る潜在的状態遷移プロセスはハザードを意味する。本節では、状態遷移経路分析のための S-A プロセスチャートの展開方法について説明する。

3.7.1 システム要素およびシステム状態の表記方法

状態経路分析を行う場合、次の（1）および（2）に従ってシステム要素の状態の組合せ

によって表す。

(1) システム要素状態 $X_{i,j,k}$

システム要素状態は、システム要素 i が持つ属性 j の状態 k ($i=1,2,\dots,n, j=1, 2,\dots,q_{ij}, k=0,1, 2,\dots,p_{i,j,k}$) , すなわち $X_{i,j,k}$ で表す。システム要素の属性とは、システム要素が持つ温度、濃度、質量等の物理量、機能、形態等を意味する。

(2) システム状態 S_y

システム状態 S_y を各システム要素状態 $X_{i,j,k}$ の組合せにより次のように表す。

$$S_1 = \{X_{i_1'}, j_1', k_1', X_{i_1''}, j_1'', k_1'', \dots, X_{i_1'''}, j_1''', k_1'''\}$$

$$S_2 = \{X_{i_2'}, j_2', k_2', X_{i_2''}, j_2'', k_2'', \dots, X_{i_2'''}, j_2''', k_2'''\}$$

$$\vdots \quad \quad \quad \vdots \quad \quad \quad \vdots$$

$$S_u = \{X_{i_u'}, j_u', k_u', X_{i_u''}, j_u'', k_u'', \dots, X_{i_u'''}, j_u''', k_u'''\}$$

ここで、システム要素状態 $X_{i_y'}, j_y', k_y'$ ($y=1, 2,\dots, u$) は、システム状態 S_y が m_y 個 ($m_y=1, 2,\dots,d$) のシステム要素状態から構成されているときの第一番目のシステム要素状態、 $X_{i_y''}, j_y'', k_y''$ は第二番目のシステム要素状態、また $X_{i_y'''}, j_y''', k_y'''$ は第 m_y 番目のシステム要素状態を意味する。 u 個の S_y の少なくとも一つに、ある危害が生起するためのすべての必要条件を満たす $X_{i,j,k}$ の組合せが含まれる。危害に至る経路は、危害が生起していない任意の初期状態 $S_{y'}$ から危害が生起している $S_{y''}$ を最終状態として同定される。

3.7.2 遷移作用 $A_{ij}(k,k')$ と $X_{i,j,k}$ との関係

遷移作用は、 $X_{i,j,k}$ を $X_{i,j,k'}$ に変化させる作用であり $A_{ij}(k,k')$ で表す。 $A_{ij}(k,k')$ および $X_{i,j,k}$ に次の前提条件 (a) ~ (c) を設定しても不自然ではない。

- (a) $A_{ij}(k,k')$ は、互いに独立しており、1つの状態に、同時に複数の $A_{ij}(k,k')$ が作用しない。
- (b) $X_{i,j,k}$ の可逆遷移または不可逆遷移は制約遷移によって行われ、 $A_{ij}(k,k')$ もまた、 $X_{i,j,k}$ の制約遷移に従って行われる。
- (c) 制約遷移は、温度、濃度、距離等の連続した物理量を、低、中、高 (大、中、小) の区分からなる状態とした場合、低から中、中から低、中から高、および/または高から中のいずれかの遷移である。

(a) ~ (c) の前提条件から導かれる $A_{ij}(k,k')$ と $X_{i,j,k}$ との相互関係を **図 3-6** に示す。

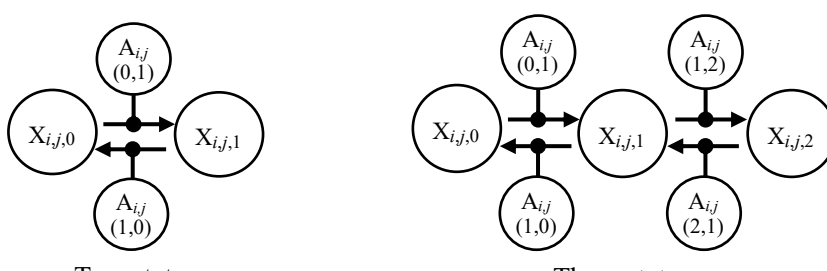
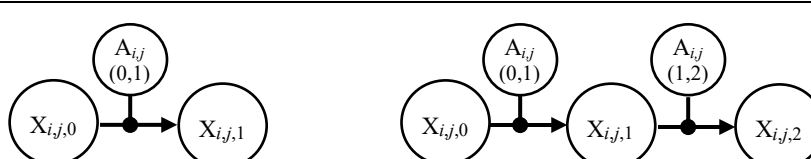
図 3-6 は、2 状態または 3 状態を持つ $X_{i,j,k}$ と $A_{ij}(k,k')$ との関係を次のようにモデル化している。

I 型: 可逆遷移を行う $A_{ij}(k, k')$

$X_{ij,k}$ が 2 状態の場合, $A_{ij}(k, k')$ は $A_{ij}(0,1)$ および $A_{ij}(1,0)$ の 2 個である。 $X_{ij,k}$ が 3 状態の場合, $A_{ij}(k, k')$ は $A_{ij}(0,1)$, $A_{ij}(1,2)$, $A_{ij}(2,1)$, $A_{ij}(1,0)$ の 4 個である。

II 型: 不可逆遷移を行う $A_{ij}(k, k')$

$X_{ij,k}$ が 2 状態の場合, $A_{ij}(k, k')$ は $A_{ij}(0,1)$ のみである。 $X_{ij,k}$ が 3 状態の場合, $A_{ij}(k, k')$ は $A_{ij}(0,1)$, $A_{ij}(1,2)$ の 2 個である。

Type	The states transition model of system element
I	 <p>Two states</p> <p>Three states</p> <p>Reversible transitions or reversible and restricted transitions, for examples:</p> <ul style="list-style-type: none"> • Item starts or stops. • Repairable item changes to up state or down state. • Concentration of flammable gas with explosion limit changes. • Operating frequency of the item with resonance frequency changes.
II	 <p>Two states</p> <p>Three states</p> <p>Irreversible transitions or irreversible and restricted transitions, for examples:</p> <ul style="list-style-type: none"> • Non-repairable item changes from up state to down state. • Material degrades with age. • Catastrophic damage occurs.

Notes

→ : Transition direction

図 3-6 システム要素の状態遷移プロセスモデルの例

3.7.3 状態遷移経路図

$X_{i,j,k}$, S_y , 状態遷移プロセスモデルおよび $A_{ij}(k,k')$ が決まると, S_y の遷移可能な経路が決まる。図 3.7 は, 次の条件 (a0) ~ (d0) に基づき, システムの各定義状態がもつ遷移可能なすべての経路と $A_{ij}(k,k')$ との組合せを示している。本論文では, 図 3-7 の様な図式表現を状態遷移経路図という。

- (a0) $X_{i,j,k}$ の状態遷移は, I型の状態遷移プロセスモデルに従う。
- (b0) システム要素 i ($i=1$) は 2 つの属性変数 $q_{1,1}$ および $q_{1,2}$ を持つ。
- (c0) $q_{1,1}$ は, 3 個の状態変数 $p_{1,1,0}$, $p_{1,1,1}$, $p_{1,1,2}$ をもつ。
- (d0) $q_{1,2}$ は, 2 個の状態変数 $p_{1,2,0}$, $p_{1,2,1}$ を持つ。

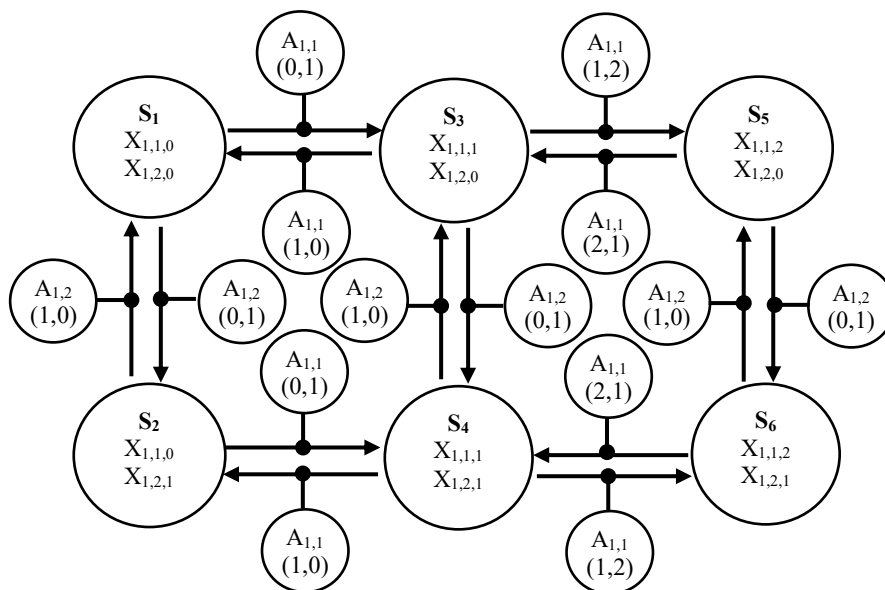


図 3-7 状態遷移経路図

図 3-7 は次のとおり求める。

① 条件 (a₀) , (b₀) , (c₀) より, X_{1,1,k} は (3.1) 式のとおり表される。

$$X_{1,1,k} = \begin{cases} X_{1,1,0} \\ X_{1,1,1} \\ X_{1,1,2} \end{cases} \quad (3.1)$$

② 条件 (a₀) , (b₀) , (d₀) より, X_{1,2,k} は (3.2) 式のとおり表される。

$$X_{1,2,k} = \begin{cases} X_{1,2,0} \\ X_{1,2,1} \end{cases} \quad (3.2)$$

③ X_{1,1,k} と X_{1,2,k} を組合せて 6 個のシステム状態 S_y (y=1, 2,...6) を定義する。

$$\begin{aligned} S_1 &= \{X_{1,1,0}, X_{1,2,0}\} \\ S_2 &= \{X_{1,1,0}, X_{1,2,1}\} \\ S_3 &= \{X_{1,1,1}, X_{1,2,0}\} \\ S_4 &= \{X_{1,1,1}, X_{1,2,1}\} \\ S_5 &= \{X_{1,1,2}, X_{1,2,0}\} \\ S_6 &= \{X_{1,1,2}, X_{1,2,1}\} \end{aligned} \quad (3.3)$$

④ 条件 (a₀) , (b₀) , (c₀) , (d₀) より, 次の A_{ij} (k,k') が存在する。

$$\begin{aligned} &A_{1,1} (0,1) \\ &A_{1,1} (1,0) \\ &A_{1,1} (1,2) \\ &A_{1,1} (2,1) \\ &A_{1,2} (0,1) \\ &A_{1,2} (1,0) \end{aligned} \quad (3.4)$$

⑤ ①～④より, 表 3-1 の状態遷移表を求める。表 3-1 は, 前提条件 (a₀) ～ (d₀) に基づき

- (a) 現在のシステム状態 S_y,
- (b) S_y に作用し得る遷移作用 A_{ij} (k,k')

(c) 遷移作用の結果生起し得る別の状態 S_y ’

の関係を表す。例えば S_1 は $A_{1,1}$ (0,1) によって S_3 へ、または、 $A_{1,2}$ (1,0) によって S_2 へ遷移する。“ n_t ”は、遷移が存在しないことを意味する。

表 3-1 前提条件 (a₀) ~ (d₀) によるシステム状態遷移表

遷移作用 \ システム状態	$A_{1,1}$ (0,1)	$A_{1,1}$ (1,0)	$A_{1,1}$ (1,2)	$A_{1,1}$ (2,1)	$A_{1,2}$ (0,1)	$A_{1,2}$ (1,0)
$S_1 = \{X_{1,1,0}, X_{1,2,0}\}$	S_3	n_t	n_t	n_t	S_2	n_t
$S_2 = \{X_{1,1,0}, X_{1,2,1}\}$	S_4	n_t	n_t	n_t	n_t	S_1
$S_3 = \{X_{1,1,1}, X_{1,2,0}\}$	n_t	S_1	S_5	n_t	S_4	n_t
$S_4 = \{X_{1,1,1}, X_{1,2,1}\}$	n_t	S_2	S_6	n_t	n_t	S_3
$S_5 = \{X_{1,1,2}, X_{1,2,0}\}$	n_t	n_t	n_t	S_3	S_6	n_t
$S_6 = \{X_{1,1,2}, X_{1,2,1}\}$	n_t	n_t	n_t	S_4	n_t	S_5

⑥ 表 3-1 を、次の手順で図式化する。

- (i) 表 3-1 より各システム状態 $S_1 \sim S_6$ が持つ隣り合う遷移可能な状態を洗い出す。
 図 3-8 の (3-a) ~ (3-f) は、各システム状態 $S_1 \sim S_6$ が持つ隣り合う遷移可能な状態を示している。
- (ii) 図 3-9 に示す手順で、各システム状態 $S_1 \sim S_6$ が持つ隣り合う互いに遷移可能な状態を結合する。まず、(3-a) および (3-b) が持つ互いに遷移可能な状態 S_1 および S_3 を組合せて (3-a) and (3-b) を得る。次に、(3-a) and (3-b) および (3-c) が持つ互いに遷移可能な状態 S_3 および S_5 を組合せて (3-a) , (3-b) and (3-c) を得る。同様にして、(3-d) , (3-e) , (3-f) を組合せ、(3-a) , (3-b) , (3-c) , (3-d) , (3-e) and (3-f) の状態遷移経路図 (図 3-7) が完成する。

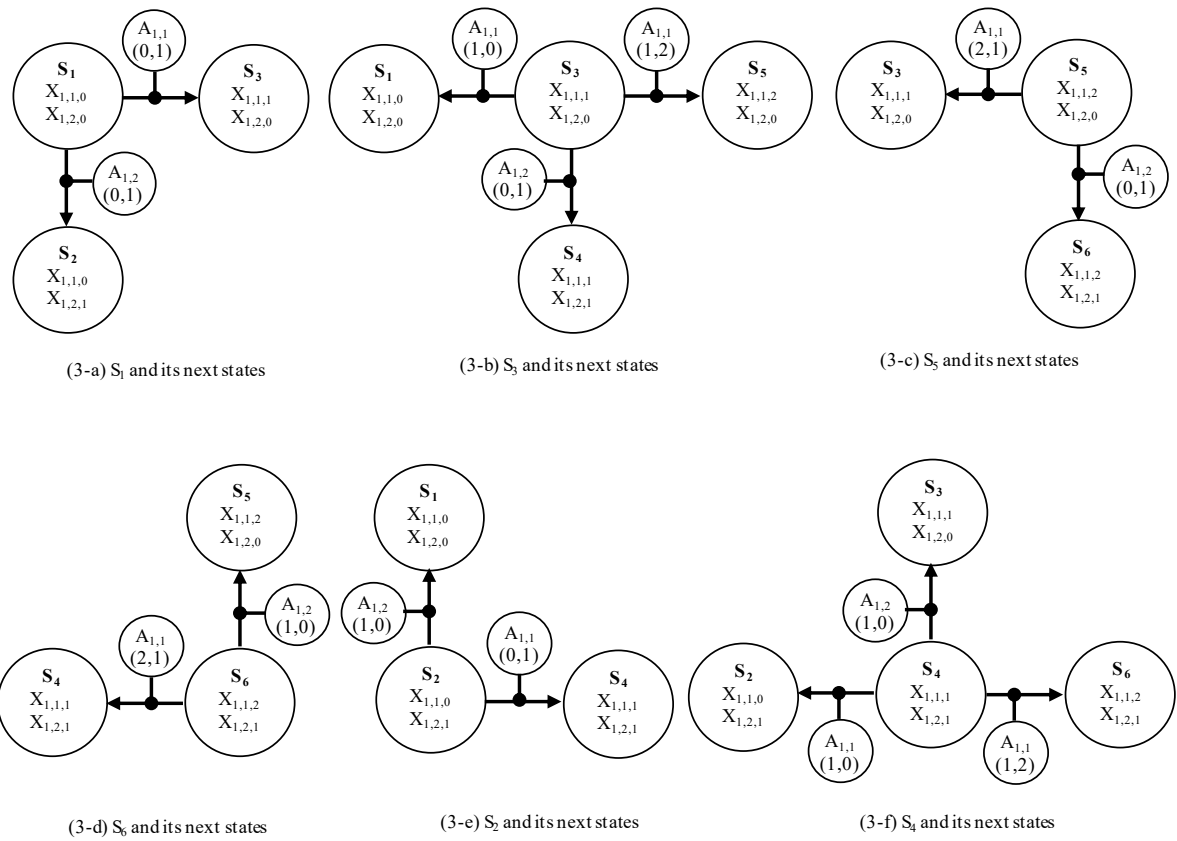


図 3-8 各状態の隣り合う遷移可能な状態

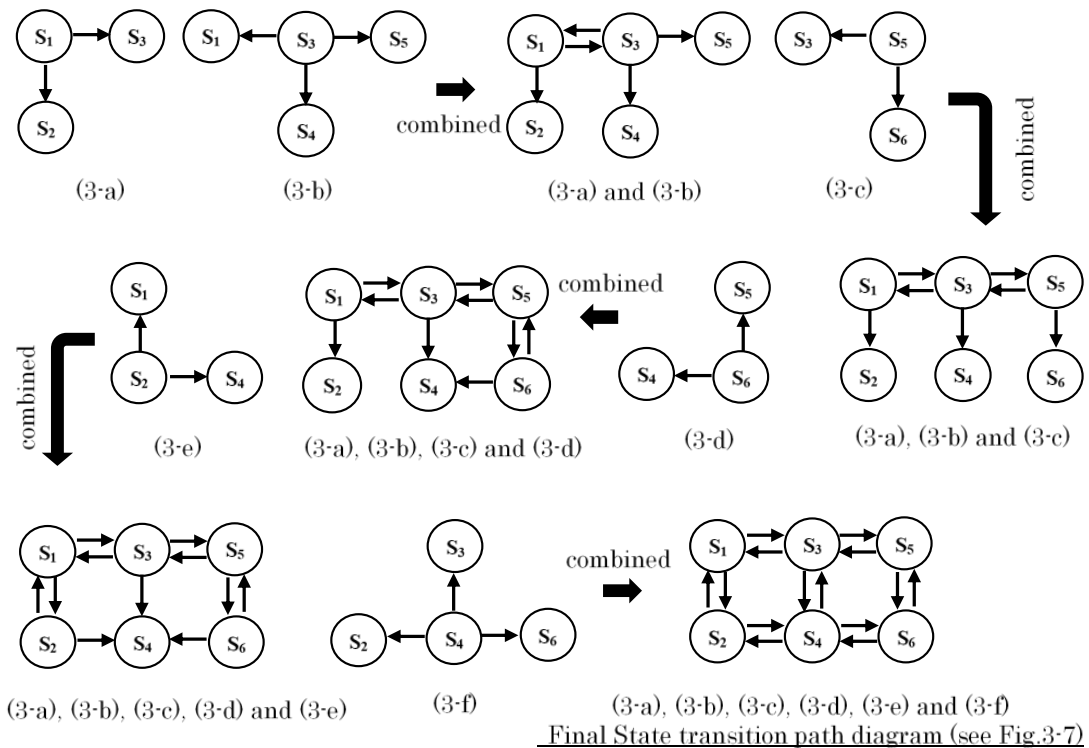


図 3-9 状態遷移経路図の組立て手順

3.7.4 状態遷移経路図からの S-A プロセスチャートの導出

図 3-7 の状態遷移経路上のある状態から別の状態へ遷移する経路は、可逆的な遷移作用によって状態間を無制限に往復する経路を生成し確定することができない。しかし、図 3-7 に対して次の S-A プロセスチャートを導出するための条件（以下、導出条件） $C_{r1} \sim C_{r7}$ を適用することによって初期状態から最終状態（危害）に至る経路が確定する。図 3-10 は $S_{ys} = S_1$, $S_{ye} = S_4$ とした場合の S-A プロセスチャートの例である。

- C_{r1} 初期状態 S_{ys}
- C_{r2} 最終状態 S_{ye}
- C_{r3} S_{ys} は繰り返し出現しない。
- C_{r4} S_{ye} は繰り返し出現しない（最終状態が発現した場合、状態遷移は完了する）。
- C_{r5} 1つの経路は、同じ $A_{ij} (k, k')$ を含まない。
- C_{r6} 1つの経路は、同じ状態を含み得る。
- C_{r7} 各クリティカル状態を経由する少なくとも各 1 個の経路が存在する。

往復する状態遷移プロセス $S_y \rightarrow S_{y'} \rightarrow S_y$ を何度繰り返しても遷移作用の効果および遷移作用の働きによる結果は変化しないという条件では、ハザードの分析という観点におい

て、 $S_y \rightarrow S_{y'} \rightarrow S_y$ の 2 回以上の繰り返しは省くことが可能であり、導出条件 $C_{r5} \sim C_{r6}$ によって繰り返し回数は、1 回に制限されている。

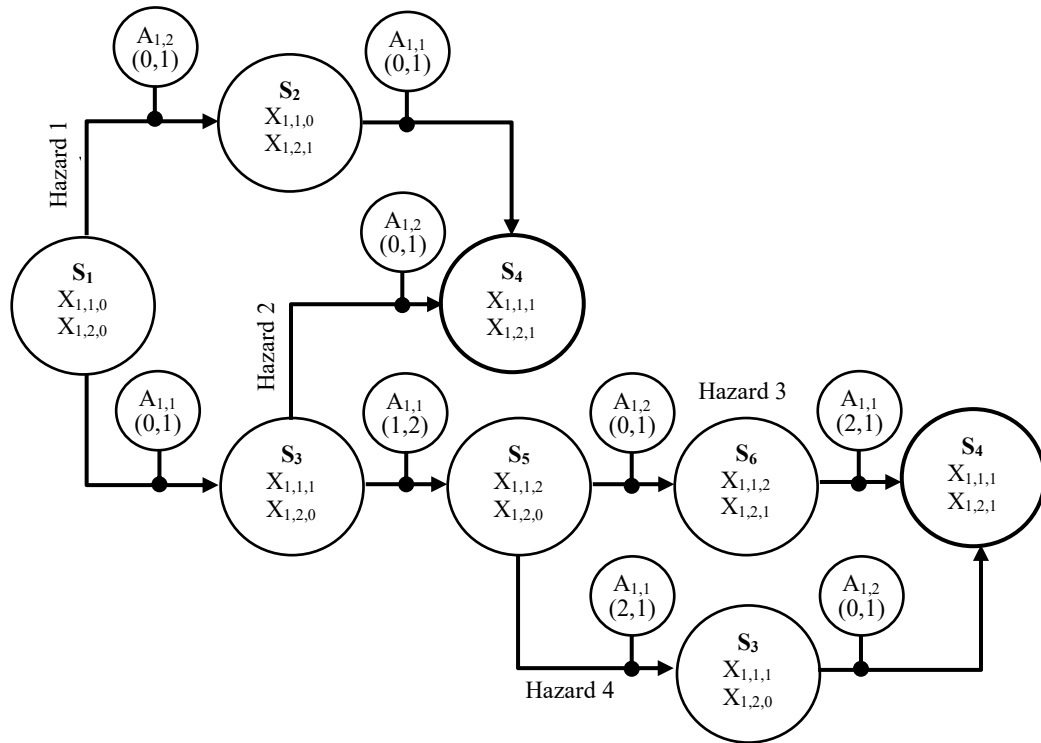


図 3-10 導出条件 $C_{r1} \sim C_{r7}$ を図 3-7 に適用して求められた S-A プロセスチャート ($S_{ys} = S_1$, $S_{ye} = S_4$ の場合)

3.7.5 状態遷移経路図と遷移作用順列 Pw の関係

導出条件 $C_{r1} \sim C_{r7}$ の網羅性に関する妥当性は、次のように説明できる。図 3-7 が持つ重複しない 6 個の遷移作用 $A_{1,1}(0,1)$, $A_{1,1}(1,0)$, $A_{1,1}(1,2)$, $A_{1,1}(2,1)$, $A_{1,2}(0,1)$, $A_{1,2}(1,0)$ から成る順列は $6!$ ($=720$) 通り存在する。720 通りの順列を初期状態 S_1 に与えることによってシステムに起こり得る潜在的状態遷移プロセスを網羅的に導出できる。ただし、図 3-6 の I 型状態遷移プロセスモデルに基づき、適用可能な順列は限定される。例えば、状態 $S_1 = \{X_{1,1,0}, X_{1,2,0}\}$ に作用可能な 1 番目の遷移作用は $A_{1,1}(0,1)$ または $A_{1,2}(0,1)$ の 2 つであり、1 番目に $A_{1,1}(1,0)$, $A_{1,1}(1,2)$, $A_{1,1}(2,1)$, $A_{1,2}(1,0)$ を持つ順列 ($5! \times 4 = 480$ 通り) は除外される。次に作用可能な 2 番目の遷移作用は $A_{1,2}(0,1)$, $A_{1,2}(1,0)$, $A_{1,1}(1,2)$, $A_{1,1}(1,0)$ または $A_{1,1}(0,1)$ の 5 つであり、2 番目に $A_{1,1}(2,1)$ を持つ順列 ($5! \times 1 = 120$ 通り) は除外される。同様にして、3 番目～6 番目に対して作用できない $A_{i,j}(k,k')$ を持つ

順列を除外すると、表 3-2 に示す 15 通りの順列 ($P_1 \sim P_{15}$) が決まる。 $P_1 \sim P_{15}$ を S_1 に組合せると危害に至るプロセスと危害に至らないプロセスが混在する 15 個の S-A プロセスチャートが完成する (図 3-11)。

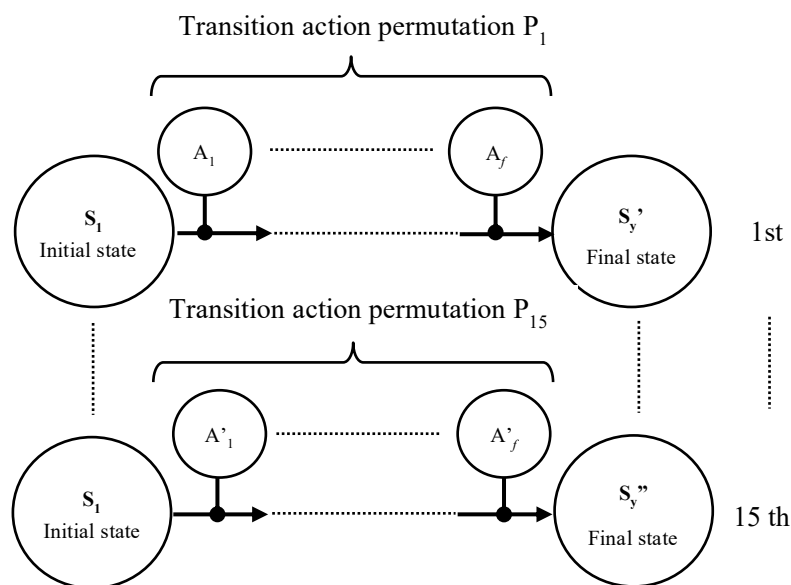


図 3-11 S_1 に遷移作用順列を組合せて求められた S-A プロセスチャート

表 3-2 の順列 $P_1 \sim P_4$, および $P_{12} \sim P_{15}$ では、1 番目の遷移作用 (A_1) および 2 番目の遷移作用 (A_2) が行われることで S_4 が発現する。順列 $P_6 \sim P_9$ では、 $A_1 \sim A_4$ が行われることで S_4 が発現する。順列 P_5, P_{10}, P_{11} では、 $A_1 \sim A_6$ が行われることで危害が発現せず S_1 に戻る。従って、危害 S_4 が発現する順列は、次の 4 個である。

$$P'_1 = \{A_{1,1} (0,1), A_{1,2} (0,1)\}$$

$$P'_{12} = \{A_{1,2} (0,1), A_{1,1} (0,1)\}$$

$$P'_6 = \{A_{1,1} (0,1), A_{1,1} (1,2), A_{1,1} (2,1), A_{1,2} (0,1)\}$$

$$P'_8 = \{A_{1,1} (0,1), A_{1,1} (1,2), A_{1,2} (0,1), A_{1,1} (2,1)\}$$

これらの順列を、 S_1 に順次組合せると、図 3-10 と同じ S-A プロセスチャートが導出される。これは、S-A プロセスチャートを状態遷移経路図 (図 3-7) に 3.7.4 項の $C_{r1} \sim C_{r7}$ を適用して導出した場合と、初期状態に表 3-2 に示す順列を組合せて導出した場合とが等価であることを示している。

表 3-2 初期状態に適用可能な遷移作用順列とその最終状態

NO.	初期状態	遷移作用順列						最終状態
		A ₁ (1 番目)	A ₂	A ₃	A ₄	A ₅	A ₆ (6 番目)	
P ₁	State1	A _{1,1} (0,1)	A _{1,2} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	A _{1,2} (1,0)	State4
P ₂		A _{1,1} (0,1)	A _{1,2} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,2} (1,0)	A _{1,1} (1,0)	State4
P ₃		A _{1,1} (0,1)	A _{1,2} (0,1)	A _{1,1} (1,2)	A _{1,2} (1,0)	A _{1,1} (2,1)	A _{1,1} (1,0)	State4
P ₄		A _{1,1} (0,1)	A _{1,2} (0,1)	A _{1,2} (1,0)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	State4
P ₅		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	A _{1,2} (0,1)	A _{1,2} (1,0)	State1
P ₆		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,2} (0,1)	A _{1,1} (1,0)	A _{1,2} (1,0)	State4
P ₇		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,2} (0,1)	A _{1,2} (1,0)	A _{1,1} (1,0)	State4
P ₈		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,2} (0,1)	A _{1,1} (2,1)	A _{1,1} (1,0)	A _{1,2} (1,0)	State4
P ₉		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,2} (0,1)	A _{1,1} (2,1)	A _{1,2} (1,0)	A _{1,1} (1,0)	State4
P ₁₀		A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,2} (0,1)	A _{1,2} (1,0)	A _{1,1} (2,1)	A _{1,1} (1,0)	State1
P ₁₁		A _{1,2} (0,1)	A _{1,2} (1,0)	A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	State1
P ₁₂		A _{1,2} (0,1)	A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	A _{1,2} (1,0)	State4
P ₁₃		A _{1,2} (0,1)	A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,2} (1,0)	A _{1,1} (1,0)	State4
P ₁₄		A _{1,2} (0,1)	A _{1,1} (0,1)	A _{1,1} (1,2)	A _{1,2} (1,0)	A _{1,1} (2,1)	A _{1,1} (1,0)	State4
P ₁₅		A _{1,2} (0,1)	A _{1,1} (0,1)	A _{1,2} (1,0)	A _{1,1} (1,2)	A _{1,1} (2,1)	A _{1,1} (1,0)	State4

3.8 S-A プロセスチャートにおけるハザードの抑制原理および抑制概念

望ましくない作用連鎖の抑制という観点から、ハザード抑制原理（以下、抑制原理）が次の (a) ～ (c) として分類されている^{41), 46), 67), 68)}。

- **抑制原理 (a)**

作用源（危険源）または被作用要素の排除・隔離（ハザードの除去），例えば，望ましくない作用を行う要素をシステムから排除・隔離し，またはその状態や性質等を作用源とならない状態に限定して使用する。

- **抑制原理 (b)**

要素の望ましくない状態変化（異常，エラー，故障等）の抑制，例えば，品質管理による故障の低減，教育訓練によるヒューマンエラーの防止，フルプルーフ構造の採用等。

- **抑制原理 (c)**

作用源の制御または作用経路の制御，例えば，(1) 要素の望ましくない状態変化が起こった条件下で，安全な状態の維持，または安全な状態への遷移（フェールオペラブル，フェールセーフ構造），(2) 作動する機械と人の分離による安全状態の維持（柵，踏切遮断機等）

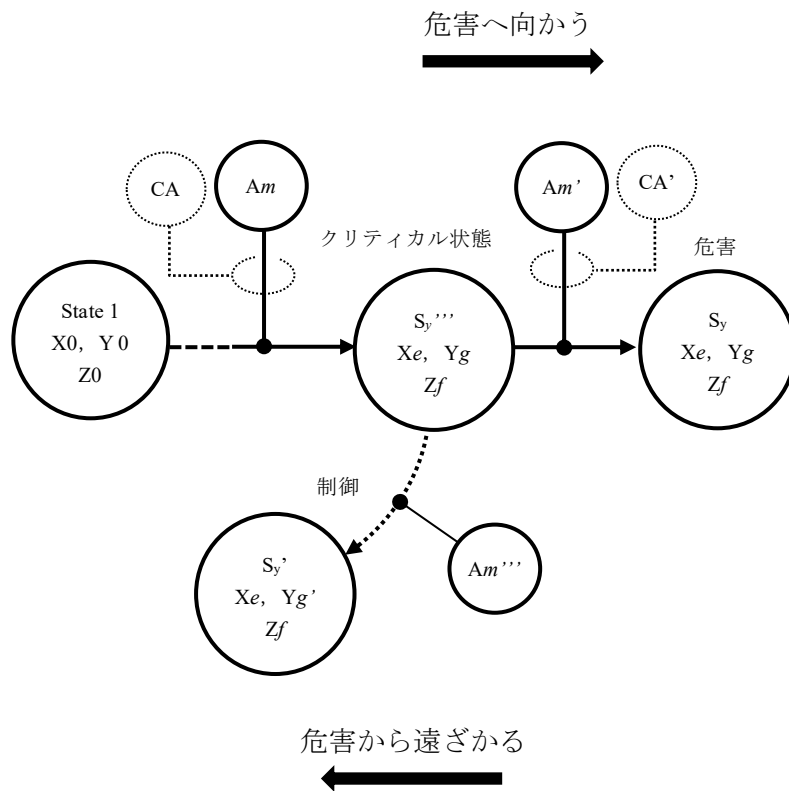
図 3-12 は，あるシステムが危害に至るハザードとその抑制概念を表している。このハザードは，遷移作用 A_m によってクリティカル状態 S_y'' が生起し，さらに遷移作用 A_m' によって危害が顕在化する。危害は，状態が矢印の方向，すなわち左から右へ順次遷移することにより発現する。図 3-12 の S-A プロセスチャートにおいて，ハザードの抑制原理 (a) ～ (c) が，次のように適用されている。

- (1) **抑制原理 (a) または (b)**

抑制作用 CA および CA' で遷移作用 A_m および A_m' を無くす，または抑制する。

- (2) **抑制原理 (c)**

遷移作用の抑制に失敗した場合は，危害が発現する前に，遷移作用 A_m'' を用い状態 S_y'' を危害からより離れた S_y' へ遷移させてハザードを抑制する。



【記号】

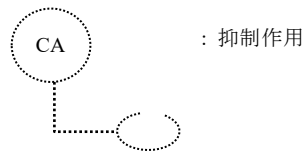
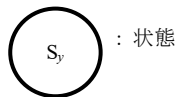
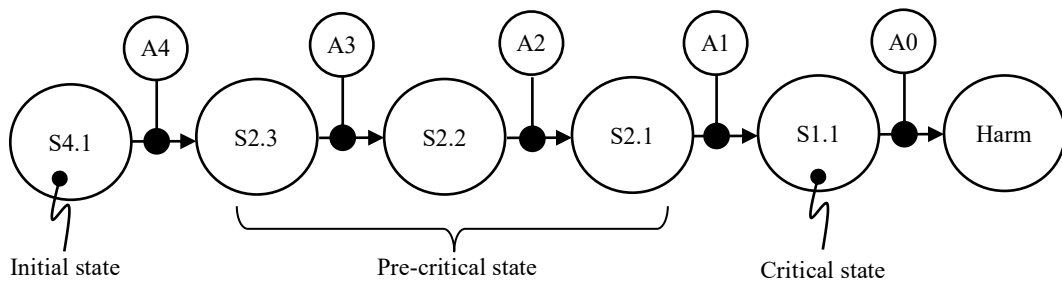


図 3-12 ハザードの抑制概念とその図式表現

各抑制原理は次のように適用する。図 3-13 は、危害発現機構および状態遷移プロセスを次のとおり表現している。ここで、システム状態は、離散値を持つシステム要素の組合せではなく記述的に表現されている。

- ① 乾燥工程にある乾燥器内部の状態 $S_{4.1}$ が、遷移作用 ”換気システム停止の作用 (A_4) ” によって、爆発性混合気生成状態 ($S_{2.3}$) に遷移する。
- ② 状態 $S_{2.3}$ が、遷移作用 ”着火エネルギーの作用 (A_3) ” によって、ガス爆発発生状態 ($S_{2.2}$) に遷移する。

- ③ 状態 S2.2 が、遷移作用 ”爆発エネルギーの作用 (A2) ” によって、乾燥器圧力上昇状態 (S2.1) に遷移する。
- ④ 状態 S2.1 が、遷移作用 ”圧力>乾燥器許容圧力 (A1) ” によって、乾燥器破壊および破片飛散状態 (S1.1) に遷移する。
- ⑤ 状態 S1.1 が、遷移作用 ”人の存在 (A0) “ によって、飛散破片による人体損傷 (Harm) に遷移する。



State

S4.1	Inside of drying oven is under the process of paint drying.
S2.3	Flammable gas concentration reaches to the gas explosion range in drying oven.
S2.2	Gas explosion occurs.
S2.1	Overpressure in drying oven.
S1.1	Drying oven fractured and debris fly in all directions.
Harm	Persons injured by flying debris.

Transition action

A4	Suspending of ventilation system
A3	Generating of ignition energy
A2	Exploding energy in confined drying oven
A1	Pressure rising higher than mechanically allowable pressure of the drying oven.
A0	Staying of persons near.

図 3-13 塗料乾燥工程中のガス爆発によって放出される飛散物衝突のハザード

図 3-13 に示した S-A プロセスチャートの例では、システムの状態を危害に近づける危険側の遷移作用によって状態が矢印の方向、すなわち左から右へ順次遷移することにより危害が発現する。そこで、S-A プロセスチャートでは、次の抑制原理 (a) ~ (c) を実現するハザード抑制策の検討が可能である。

(1) 望ましくない状態遷移を無くす、または抑制するハザード抑制策

サブクリティカル状態とクリティカル状態への遷移は、抑制すべき状態遷移である。例えば図 3-13 において、初期状態から、プレクリティカル状態、クリティカル状態を経て危害に向かう状態遷移プロセスは、図 3-14 において遷移作用 A4, A3, A2, A1, A0 に対する抑制作用 CA4, CA3, CA2, CA1, CA0 で抑制できる。ただし、単一の遷移作用の抑制に対して複数の抑制策が必要な場合もある。抑制作用 CA4, CA3, CA2, CA1, CA0 を実現するハザード抑制策の抑制原理 (a) ~ (c) との関係を次の①~⑤に示す。

① 抑制作用 CA4

遷移作用“換気システム停止 (A4)”を、“換気システムの信頼性向上”によって抑制する。この方策は、抑制原理 (b) における“望ましくない状態変化の抑制”に該当する。

② 抑制作用 CA3

遷移作用“着火エネルギーの作用 (A3)”を、“静電気除去”によって抑制する。この方策は、抑制原理 (b) における“望ましくない状態変化の抑制”に該当する。

③ 抑制作用 CA2

遷移作用“爆発エネルギーの作用 (A2)”は抑制の対象外とする。

④ 抑制作用 CA1

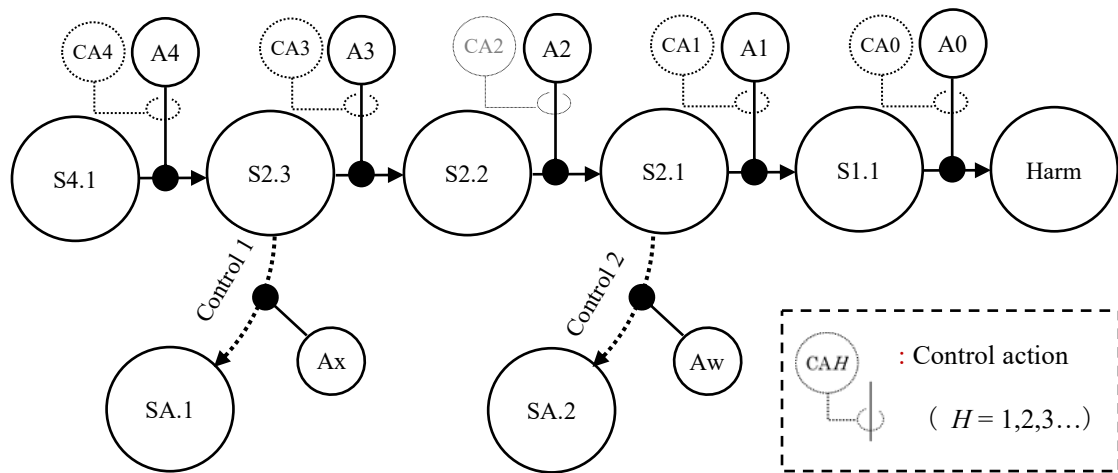
遷移作用“圧力>乾燥器許容圧力 (A1)”を、“乾燥器の耐圧強度向上”によって抑制する。この方策は、ハザード抑制原理 (a) における“ハザードの除去”に該当する。または、遷移作用“圧力>乾燥器許容圧力 (A1)”を“ガス爆発圧力放出”によって抑制する。この方策は、要素“乾燥器”の望ましくない圧力上昇の抑制という観点から、抑制原理 (b) に該当する。一方、この抑制策は、要素“乾燥器内空間”にガス爆発 (S2.2) が起こった条件下での遷移作用“ガス爆発圧力放出”による安全な状態の維持と見なすことが可能であり、この観点からは抑制原理 (c) に該当するとも考えられる。

⑤ 抑制作用 CA0

遷移作用“人の存在 (A0)”を、“作業区域における人の存在を制限する”によって抑制する。この方策は、ハザード抑制原理 (a) における“被作用要素の排除”に該当する。

(2) 危害から遠ざかる移行制御によるハザード抑制策

遷移作用の抑制に失敗し、望ましくない状態遷移が発生した場合は、状態移行のための制御によって危害からより離れる状態すなわち安全な状態へ状態遷移させてハザードを抑制する。図 3-14 において、これらの状態遷移プロセスは、点線の矢線と状態遷移を促す遷移作用“予備換気システム起動 (Ax)”による状態 SA.1 への移行制御および“ガス爆発圧力放出 (爆発圧力放散口作動) (Aw)”による状態 SA.2 への移行制御によって表されている。



State	
SA.1	Flammable gas concentration under the gas explosion lower limit.
SA.2	Depressurization in drying oven.
Transition action	
Ax	Starting up the working of second ventilation system.
Aw	Releasing explosion pressure (Activating explosion pressure release vent) .
Control action	
CA4	Improvement of reliability of ventilation system
CA3	Electrostatic discharge
(CA2	CA2 is excluded from consideration)
CA1	Improvement of pressure resistance of drying oven or releasing of explosion pressure
CA0	Reducing existence probability of persons at working area

図 3-14 ハザード抑制原理に基づく図 3-13 のハザード抑制策の例

第4章 S-A プロセスチャートを用いたハザードの同定

第4章では、環境試験槽の停止に起因する、および試験槽内での LIB の熱暴走に起因するハザードの同定とその抑制策の導出に S-A プロセスチャートを適用し、その有効性を検証する。

4.1 緒言

本章では、2つの事例を用い、主に S-A プロセスチャートが持つハザード同定の網羅性および抑制策導出手順について検証する。

まず、事例1では、システムの停止に関するハザードについて論じる⁶⁹⁾。システムを停止または再起動させると、その時の状態によって、システムは危険または安全な状態に遷移し得る。システムの停止に起因するハザードを同定するためには、システムの状態、状態遷移を引き起こす作用、および状態遷移の生起順序等を時系列上で詳細に検討する必要がある。第2章で説明したが、ハザードを同定する一般的な技法としては、A-C モデル、HAZOP スタディーズ、What-if 等がある。また、分析技法として FTA、FMEA 等が用いられている。A-C モデルは、ハザードすなわち危害発生プロセスをシステム構成要素間の①作用の授受、②要素の変化を検討することにより体系的かつ系統的に同定する。HAZOP スタディーズは、システム要素のパラメータとガイドワードを組み合わせ、正常状態からの逸脱（ずれ）を想定してハザードを同定する。同技法を用いて起動または停止に起因するハザードを分析するために、化学プラント分野では、非定常 HAZOP^{70), 71)}が研究されている。しかし、いずれもシステムの状態、作用および状態遷移の生起順序等を時系列上で詳細に分析するための技法ではない。

停止に起因するハザードの抑制策は、機械安全および機能安全分野では、電動機制御の標準化が進んでいる^{72), 73)}。それらは、主に電動機の減速失敗、または停止位置を維持できない等、運動エネルギーに由来する危害を想定している。一方、高温、低温、圧力等の熱力学的エネルギーに由来する危害を想定し、かつ停止に起因するハザードの抑制策の系統的導出技法については、化学プラント分野を除き、あまり研究されていない。

次に事例2では、リチウムイオン2次電池の熱暴走ハザードについて論じる。リチウムイオン2次電池（以下 LIB という）は、機械的、電氣的、または熱的ストレスに起因して熱暴走による破裂（Explosion）、開裂（Rupture）および発火等のハザードがある。LIB 内部に何らかの異常が発生し熱分解反応が進行すると、次に LIB は熱暴走状態に移行し、内部エネルギーを消費するまで発煙・発火状態を継続し、途中でこれを抑制または停止させることは困難である。本事例では LIB の信頼性・安全性試験^{77), 78)}において、密閉した試験槽内で LIB の熱暴走が発生したときのハザードを同定し、その抑制策を導出する。

これら2つの事例に S-A プロセスチャートを適用し、次の (a) および (b) が可能であ

ることを示し、その有効性を検証する。

- (a) システムのそれぞれの状態にシステム要素の故障，エラー（無秩序状態作用），正常機能の履行（秩序状態作用）に起因する遷移作用を組み合わせることで危害に至る状態遷移プロセスを系統的に追跡し，ハザードを網羅的に同定する。
- (b) ハザード抑制原理に基づき，ハザードの抑制策を系統的かつ合理的に導出する。

4.2 事例1：環境試験槽の停止に起因するハザードの同定とその抑制策の導出

4.2.1 記号

事例1で使用する各記号は、次のとおりである。

(1) 試験槽の状態

- a_i ：試験槽の制御状態である。“温湿度制御状態（operational state）”，または“温湿度制御停止状態（stopped state）”で表される2つの状態がある。
- b_i ：試験槽内の温度状態であり，槽内温度 t_a （°C）によって表す。
- c_i ：試験槽内の湿度状態であり，相対湿度 hd （%）によって表す。
- d_i ：試験槽内各部の表面温度であり， t_c （°C）によって表す。 $t_c < Dp1$ ，または扉開時，外気に触れて $t_c < Dp2$ が成立すると，試験槽内表面に結露水が発生する。
- e_i ：扉の状態：試験槽の扉の開閉状態。“Close”，または“Open”で表される2つの状態がある。
- f_i ：供試品の電圧印加状態であり，印加中 “On”，または印加停止中 “Off” で表される2つの状態がある。
- g_i ：供試品の表面温度であり， t_g （°C）で表す。 $t_g < Dp1$ ，または扉開時，外気に触れて $t_g < Dp2$ が成立すると，供試品表面に結露水が発生する。
- h_i ：試験槽周囲の温湿度条件における露点温度（Dp2）の状態である。本事例では，試験槽周囲の温湿度は，23°C，65%一定とする。
- i ：ある時刻から t_i 時間後の試験槽の状態を表す変数（ $i=0,1,2\dots$ ）（ $t_0 < t_1 < t_2\dots$ ）
- t_a ：試験槽内温度（°C）
- hd ：試験槽内の相対湿度（%）
- Dp1：試験槽内の温湿度が t_a （°C）， hd （%）のときの露点温度。
- t_p ：供試品の耐熱温度（°C）であり，供試品が耐熱温度を超えると，発煙，発火，変形，または破損する。
- t_{p1} ：供試品の発熱部近傍温度（°C）
- Dp2：試験槽周囲が温湿度条件 23°C，65%における露点温度。（=16.6°C）

(2) 遷移作用および抑制作用

AS1 : -40°C温度制御開始

AS2 : 85°C, 85%温湿度制御開始

A0 : 温湿度制御再開

A1 : 温湿度制御停止

A2 : 扉を開けず気密状態を維持 (緩やかな熱平衡作用)

A3 : 供試品電源 On

A4 : 供試品電源 Off

A5 : 扉を閉める

A6 : 扉を開ける

A7 : 温湿度制御設定変更

A8 : $t_{p1} > t_p$

A9 : 充電部に結露水が侵入

A10 : 供試品に結露水が滴下

A11 : 過電流発生

A12 : 人の存在

A13 : 許容応力超過

A14 : 供試品自己加熱

C A_m : 遷移作用 A_m の抑制作用。

(3) 危害


E1 : 供試品が変形, 破損または焼損 (自己加熱)

E2 : 供試品が焼損 (短絡)

E3 : 供試品が変形, または破損 (熱応力)

E4 : 環境試験結果の再現性喪失 (供試品の故障モード, または劣化特性が変化)

(4) その他

 : S-A 作用プロセスチャートにおいて, 状態遷移の転移を示す。 ($n = 1, 2, 3, \dots$)

4.2.2 環境試験槽の概要

環境試験は, 工業製品が, 実際に曝されるかもしれない環境条件において, その品質性能が要求基準に適合していることを評価し検証するために行われる⁷⁴⁾。図 4-1 に示す環境試験槽 (以下, 単に試験槽という) は, 温湿度制御器 (Temperature and humidity controller) を備え, 槽内温度センサ (Temperature sensor) および湿度センサ (Humidity sensor) から得られる試験槽内の温湿度入力情報に基づき演算した制御量をヒータ回路 (Heater) および冷却装置 (Refrigerator unit) に出力する。循環ファン (Convection fan) は, 温湿度制御

器と独立して、試験槽が制御状態にあるときは常時、運転状態にある。試験槽内には、供試品 (Specimen) である小型電子部品が設置されており、直流電圧が印加されているものとする。試験槽の試験条件は、低温試験⁷⁵⁾と高温高湿試験⁷⁶⁾を想定し、次の①または②の場合について考察する。

① 温度：-40℃，相対湿度：不飽和状態（100%未満）

② 温度：85℃，相対湿度：85%

また、試験槽の設置場所の温度・湿度は、23℃ 65%に維持されているものとする。

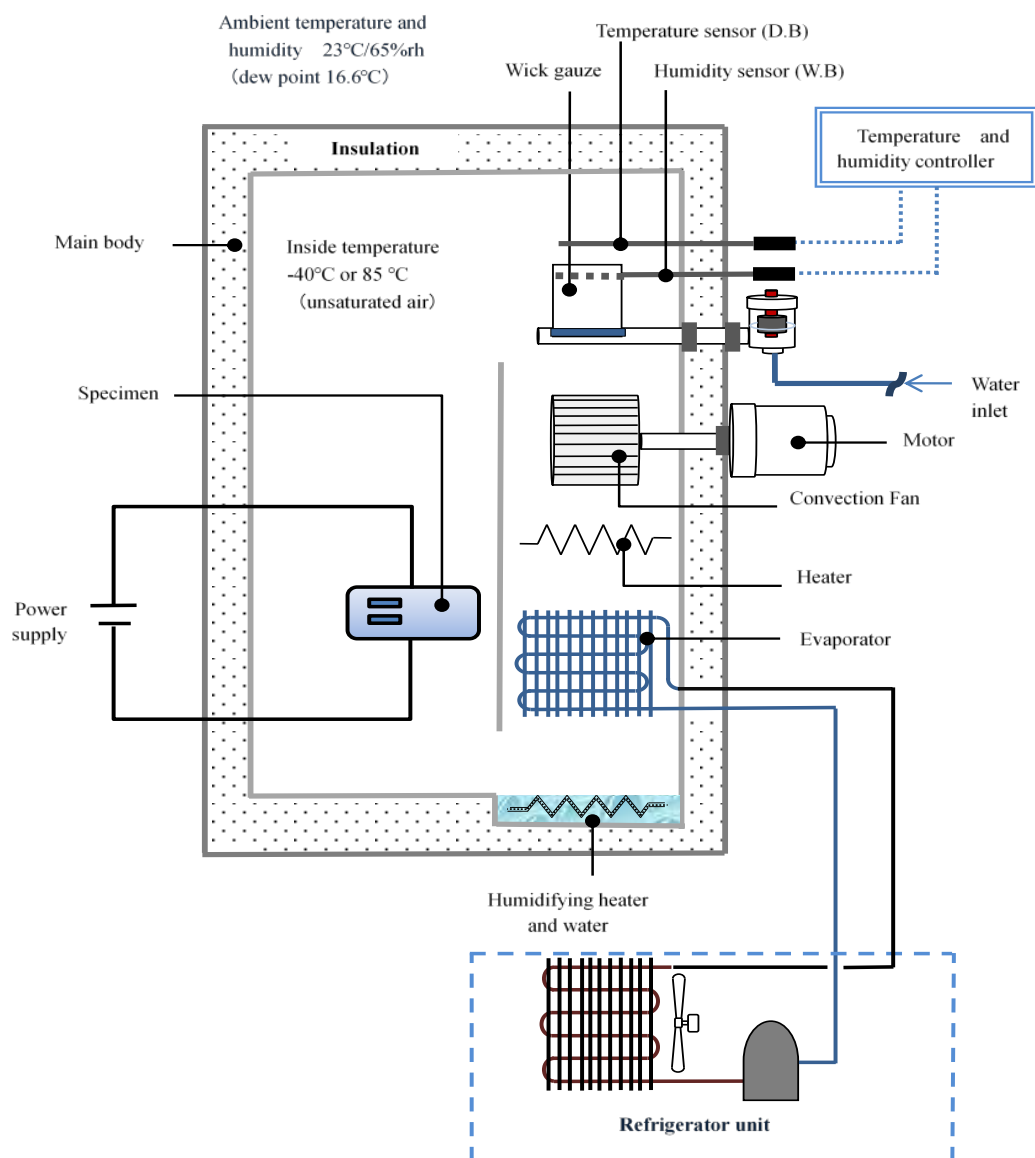


図 4-1 温湿度試験槽の概略図

4.2.3 ハザードの同定

ハザードの同定に際して、最初に、S-A プロセスチャートの初期状態を決定する。その後、順次、状態と遷移作用を組合せて、危害に至るプロセスを時系列に追跡する。

① 時刻 T における初期状態の設定

時刻 T における、**図 4-1** に示す停止中の試験槽の初期状態 S4.1 を、 $a_0, b_0, c_0, \dots, h_0$ のパラメータによって表す (**表 4-1**)。

② 時刻 $T+t_1$ における状態を推定

S4.1 は、 A_{S1}, A_{S2}, A_3 , または A_5 により、S3.1~S3.2 へ遷移する (**表 4-2**)。

③ 時刻 $T+t_2$ における状態を推定

S3.1~S3.2 は A_1, A_4 , または A_6 によって、S2.1~S2.4 へ遷移する (**表 4-3**)。

④ 時刻 $T+t_3$ における状態を推定

状態 S2.1~S2.2 は、 A_2, A_6 , または A_{14} により、S1.1~S1.4 へ遷移する。S2.3~S2.4 は、 $A_9, A_{11} \sim A_{13}$ によって、危害 E2, E3, または E5 に遷移する (**表 4-4**)。

⑤ 時刻 $T+t_4$ における状態を推定

S1.1~S1.4 は、 $A_6, A_8 \sim A_{13}$ によって、危害 E1~E5 に遷移する。

危害に至る潜在的状態遷移プロセスを S-A プロセスチャートを用い**図 4-2** に示す。

表 4-1 時刻 T における初期状態

S4.m	a_0	b_0 (°C)	c_0 (%)	d_0 (°C)	e_0	f_0	g_0 (°C)	h_0 (°C)
S4.1	stopped state	$t_a \approx 23$	hd = 65	$t_c > Dp1$	Open	Off	$t_g > Dp1$	$Dp2 = 16.6$

表 4-2 時刻 $T+t_1$ における状態

S3.l	a_1	b_1 (°C)	c_1 (%)	d_1 (°C)	e_1	f_1	g_1 (°C)	h_1 (°C)
S3.1	operational state	$t_a = -40$ (under control)	hd < 100	$t_c > Dp1$	Close	On	$t_g > Dp1$	$Dp2 = 16.6$
S3.2	operational state	$t_a = 85$ (under control)	hd=8 (under control)	$t_c > Dp1$	Close	On	$t_g > Dp1$	$Dp2 = 16.6$

表 4-3 時刻 $T+t_2$ における状態

S2. <i>k</i>	a_2	b_2 (°C)	c_2 (%)	d_2 (°C)	e_2	f_2	g_2 (°C)	h_2 (°C)
S2.1	stopped state	$ta \approx -40^\circ\text{C}$ ta gradually rises more than -40°C	$hd < 100$	$tc > Dp1$	Close	On	$tg > Dp1$	$Dp2 = 16.6$
S2.2	stopped state	$ta \approx 85$ ta gradually drops	$hd < 100$ hd gradually rises to saturation	$tc < Dp1$	Close	Off	$tg > Dp1$	$Dp2 = 16.6$
S2.3	operational state	$23 > ta > -40$ ta rises more than -40°C rapidly due to open air flowing in	$hd < 100$ hd rises rapidly due to open air flowing in	$tc < Dp2$	Open	On	$tg < Dp2$	$Dp2 = 16.6$
S2.4	operational state	$23 < ta < 85$ ta drops to less than 85°C rapidly due to releasing heat	$hd < 85$ hd drops to less than 85% due to releasing steam	$tc > Dp2$	Open	On	$tg > Dp2$	$Dp2 = 16.6$

表 4-4 時刻 $T+t_3$ における状態

S1. <i>j</i>	a_3	b_3 (°C)	c_3 (%)	d_3 (°C)	e_3	f_3	g_3 (°C)	h_3 (°C)
S1.1	stopped state	$ta \approx tp$	$hd < 100$	$tc > Dp1$	Close	On	$tg \approx tp$	$Dp2 = 16.6$
S1.2	stopped state	$23 > ta > -40$ ta rises more than -40°C rapidly due to open air flowing in	$hd < 100$ hd rises rapidly due to open air flowing in	$tc < Dp2$	Open	On	$tg < Dp2$	$Dp2 = 16.6$
S1.3	stopped state	$ta \approx 23$ Thermal equilibrium State	$hd \approx 100$	$tc \approx Dp1$	Close	Off	$tg > Dp1$	$Dp2 = 16.6$
S1.4	stopped state	$23 < ta < 85$ ta drops to less than 85°C rapidly due to releasing heat	$hd < 100$ hd drops to less than 85% due to releasing steam	$tc > Dp2$	Open	Off	$tg > Dp2$	$Dp2 = 16.6$

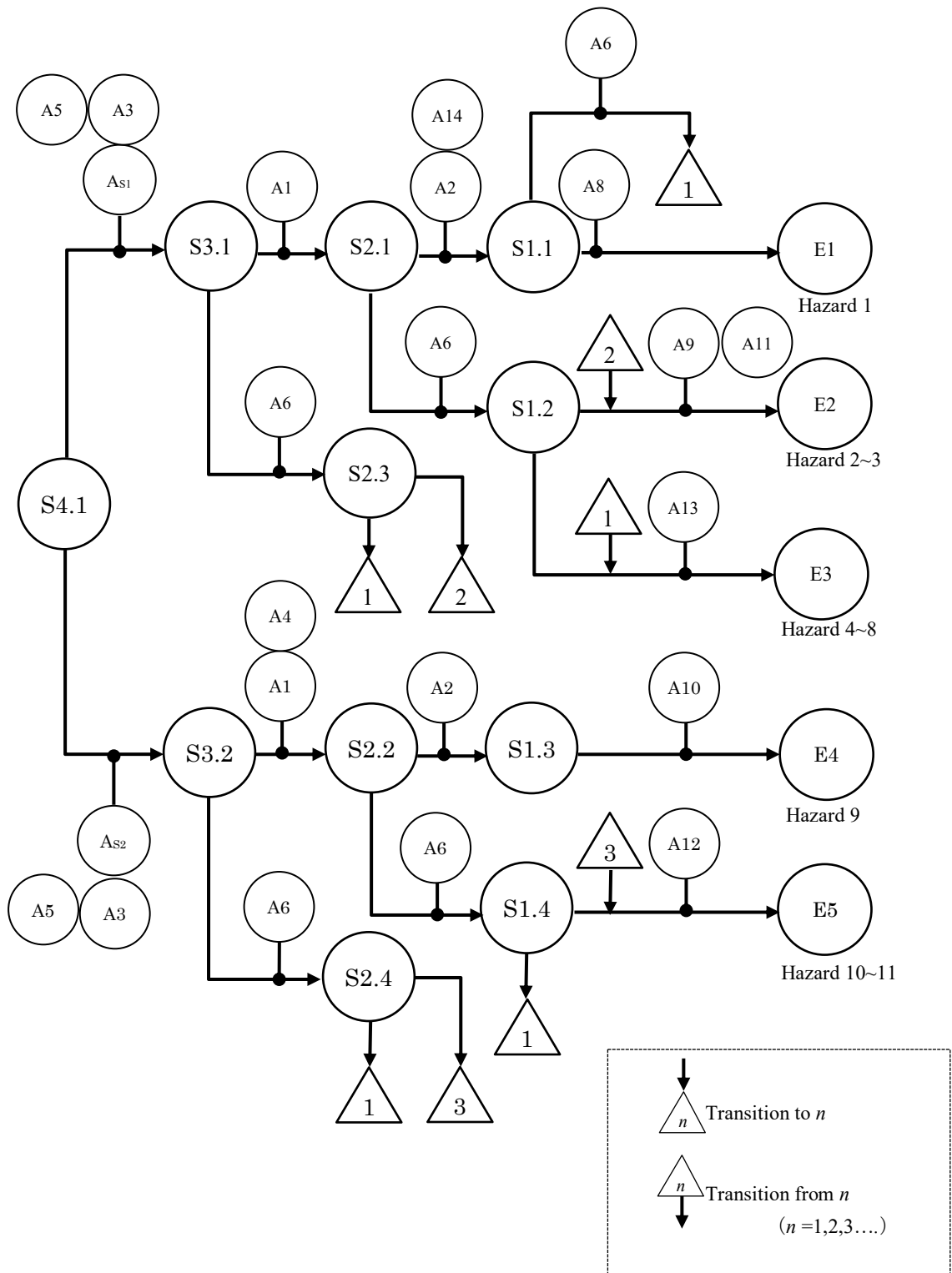


図 4-2 S-A プロセスチャートによる図 4-1 のシステムが持つハザードの同定例

図 4-2 が示す各ハザードは次のとおりである。

a) ハザード 1

- ① S4.1 が, As₁, A5 および A3 によって, S3.1 に遷移する。
- ② S3.1 が, A1 によって, S2.1 に遷移する。
- ③ S2.1 が, A2 および A14 によって, S1.1 に遷移する。
- ④ S1.1 が, A8 によって, 危害 E1 に遷移する。

b) ハザード 2

- ① S2.1 までのプロセスは, ハザード 1 と同じ。
- ② S2.1 が, A6 によって, S1.2 に遷移する。
- ③ S1.2 が, A9 および A11 によって, 危害 E2 に遷移する。

c) ハザード 3

- ① S3.1 までのプロセスは, ハザード 1 と同じ。
- ② S3.1 が, A6 によって, S2.3 に遷移する。
- ③ S2.3 が, A9 および A11 によって, 危害 E2 に遷移する。

d) ハザード 4

- ① S1.2 までのプロセスは, ハザード 2 と同じ。
- ② S1.2 が, A13 によって, 危害 E3 に遷移する。

e) ハザード 5

- ① S2.3 までのプロセスは, ハザード 3 と同じ。
- ② S2.3 が, A13 によって, 危害 E3 に遷移する。

f) ハザード 6

- ① S1.1 までのプロセスは, ハザード 1 と同じ。
- ② S1.1 が, A6 および A13 によって, 危害 E3 に遷移する。

g) ハザード 7

- ① S3.2 までのプロセスは, ハザード 9 と++同じ。
- ② S3.2 が, A6 によって, S2.4 に遷移する。
- ③ S2.4 が, A13 によって, 危害 E3 に遷移する。

h) ハザード 8

- ① S1.4 までのプロセスは, ハザード 10 と同じ。
- ② S1.4 が, A13 によって, 危害 E3 に遷移する。

i) ハザード 9

- ① S4.1 が, As₂, A5, および A3 によって, S3.2 に遷移する。
- ② S3.2 が, A1 および A4 によって, S2.2 に遷移する。
- ③ S2.2 が, A2 によって, S1.3 に遷移する。
- ④ S1.3 が, A10 によって, 危害 E4 に遷移する。

j) ハザード 10

- ① S2.2 までのプロセスは、ハザード 9 と同じ。
- ② S2.2 が、A6 によって、S1.4 に遷移する。
- ③ S1.4 が、A12 によって、危害 E5 に遷移する。

k) ハザード 11

- ① S2.4 までのプロセスは、ハザード 7 と同じ。
- ② S2.4 が、A12 によって、危害 E5 に遷移する。

4.2.4 ハザード抑制策の導出事例

本項では、図 4-2 に示すハザードからハザード 1 を取り上げてその抑制策を 3.8 節に述べた抑制原理に基づき体系的に導出する。

(1) 望ましくない状態遷移をなくす、または抑制するハザード抑制策（抑制原理(a) または (b))

ハザード 1 において、S1.1 はクリティカル状態であり、S2.1 はプレクリティカル状態である。したがって、遷移作用 A1, A2, A14 および A8 は、抑制すべき遷移作用である。

① 遷移作用 A1 の抑制作用 CA2

遷移作用 A1 が、故障、停電、誤操作または誤動作等の不具合に起因している場合、システムの信頼性を向上させることが抑制作用 CA2 の実現策となる。遷移作用 A1 が不具合に起因する停止ではない場合、それは不適切な停止プロセスである。この場合、図 4-3 に示す抑制作用 CA2 を実現するためには、停止せず、S3.1 の状態を維持して、S2.1 への遷移を抑制する方策等が考えられる。

② 遷移作用 A2 の抑制作用 CA1

遷移作用 A2 は、扉を開けて密閉状態を解除することで、抑制することができる。しかし、S2.1 において扉を開けると、急激な温度変化に起因してハザード 6 の発現へ移行する可能性がある。したがって、図 4-3 に示す CA1 を実現するためには、急激な温度変化を与えない様、試験槽の密閉構造を一部解除し、試験槽内空気を外圍環境空気で緩やかに置換し、S1.1 への遷移を抑制する方策等が考えられる。

③ 遷移作用 A14 の抑制作用 CA3

遷移作用 A14 は、温湿度制御停止状態では、常に供試品の電源が Off になる様にインターロック回路を構築することで抑制することができる。これは、後述の制御 5 と同様の方策となる。

④ 遷移作用 A8 の抑制作用 CA0

遷移作用 A8 の抑制は、CA1～CA2、および後述する制御 1～6 が失敗した条件下で行われる。具体的には、図 4-3 に示す抑制作用 CA0 を実現するために、供試品と

供試品電源を接続する回路（試験槽内側）に温度ヒューズを設け、供試品の温度が耐熱温度を超える前に、供試品の電源を遮断する方策等が考えられる。

(2) 危害から遠ざかる移行制御によるハザード抑制策（抑制原理（c））

試験槽を制御して、プレクリティカル状態、クリティカル状態、または危害を回避する。S-A プロセスチャートに追加した矢線（点線）が、ハザード抑制の状態遷移のための移行制御を表している。

① 移行制御 1 および 2

図 4-3 の制御 1 および 2 は、制御による初期状態（標準状態）への状態遷移プロセスを行う。この制御は、S2.1 以降の状態を回避するために、試験終了後、ただちに停止するのではなく、A4 および A7 により、新たに定義した状態 SA.1（表 4-5）を経由して、さらに、A1 および A6 により初期状態 S4.1 に遷移するプロセスを表している。SA.1 において、A1 および A6 は危険側の遷移作用とはならず、安全側の遷移作用と見なされる。

② 移行制御 3 および 2

図 4-3 の制御 3 および 2 は、不適切な停止プロセスによって温湿度制御が停止し、S2.1 が発現した場合に、初期状態（標準状態）への状態遷移プロセスを行う。S2.1 は、A4、A0 および A7 により SA.1 を経由して、さらに A1 および A6 により初期状態 S4.1 に遷移する。

表 4-5 ハザード 1 の移行制御のために新たに定義された状態

SA.x	a ₁	b ₁ (°C)	c ₁ (%)	d ₁ (°C)	e ₁	f ₁	g ₁ (°C)	h ₁ (°C)
SA.1	operational state	$t_a \approx 23$	hd = 65	$t_c > Dp1$	Close	Off	$t_g > Dp1$	Dp2 = 16.6
SA.2	stopped state	$t_a < t_p$	hd < 100	$t_c > Dp1$	Close	Off	$t_g > Dp1$	Dp2 = 16.6

③ 移行制御 4

図 4-3 の制御 4 は、図 4-1 に示すシステムの故障に起因しない温湿度制御停止によって S2.1 が発現した場合に、S3.1 への状態遷移を行う。具体的には、停電により試験槽が停止後、電力回復と共に試験槽の温湿度制御機能を再起動させて、試験を継続する設計方策等が考えられる。

④ 移行制御 5 および 6

図 4-3 の制御 5 および 6 は、故障または誤動作等に起因する A1 を想定している。試験槽の温湿度制御機能が失われた状態で S2.1 または S1.1 が A4 によって SA.2 に移行し、槽内温度の上昇を回避する。具体的には、温湿度制御停止状態では、常に供試品の電源が Off になる様にインターロック回路を構築する等の設計方策が考えられる。この方策は、図 4-2 に示したハザード全体からみると最善の方策ではなく、SA.2 を放置しておく、図 4-2 に示した“S2.2 が A2 によって S1.3 に遷移”と同様に、試験槽内が熱平衡状態へ移行し、E4 が発現する可能性がある。

上述した (1) および (2) の抑制策を実施することにより、新たなハザードが生まれる可能性がある。しかし、本章では、それらに対する検討は省略する。

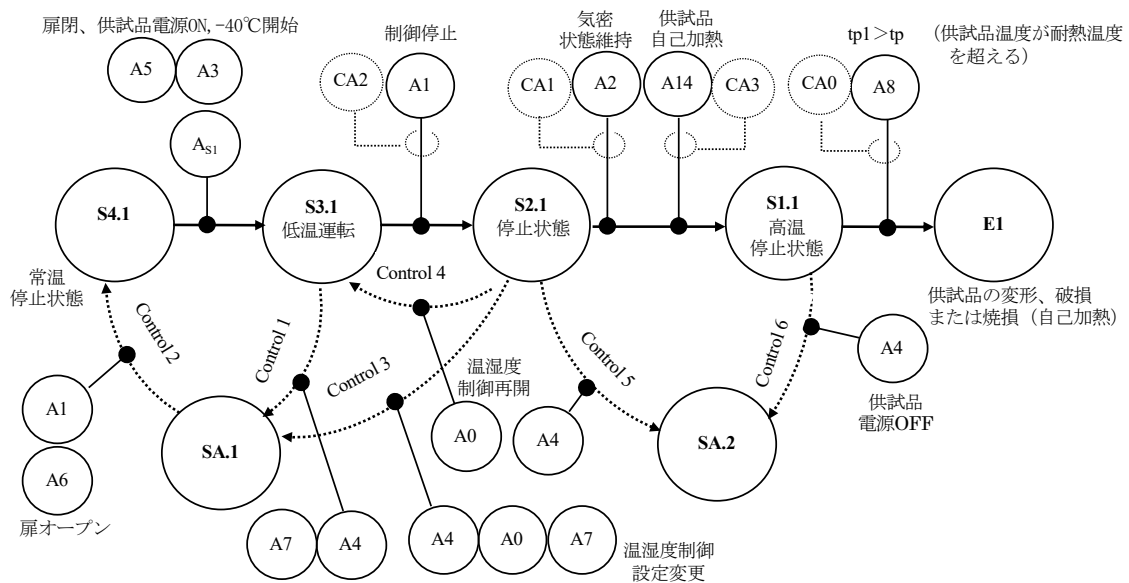


図 4-3 ハザード 1 (図 4-2) の抑制概念図

4.3 事例 2：リチウムイオン 2 次電池の熱暴走に起因するハザードの同定とその抑制策の導出

リチウムイオン 2 次電池（以下 LIB という）は、機械的、電氣的、または熱的ストレスに起因して熱暴走による破裂（Explosion）、開裂（Rupture）および発火等、表 4-6 に示す危険事象を生起させる恐れがある。本節では LIB の信頼性・安全性試験^{77), 78)}において、密閉した試験槽内で LIB の熱暴走が発生したときのハザードを同定する。

表 4-6 LIB 危険事象の分類^{79)~82)}

NO.	危険事象	定義
1	発 煙	単電池，モジュール，電池パックまたは電池システムから煙が放出される現象。
2	発 火	単電池，モジュール，電池パックまたは電池システムから炎が放出される現象。（JIS C 8715-2：2012）
3	破 裂	単電池の容器またはモジュール，電池パック若しくは電池システムの外装が猛烈な勢いで破れ，単電池の容器またはモジュール，電池パック若しくは電池システムの外装の内容物が強制的に放出される現象。（JIS C 8715-2：2012）
4	高温赤熱物質放出（低酸素状態）	内部または外部の要因によって，単電池の容器またはモジュール，電池パック若しくは電池システムの外装が破れ，高温赤熱物質を放出する現象。
5	ガス爆発	内部または外部の要因によって，単電池の容器またはモジュール，電池パック若しくは電池システムより可燃性のガスを放出し，試験槽内で拡散することで爆発雰囲気を形成し，着火エネルギーが加わることによって，ガス爆発に至る現象。

4.3.1 略語

事例 2 で使用する略語は、次のとおりである。

- LEL : 爆発下限界濃度 (vol.%)
- UEL : 爆発上限界濃度 (vol.%)
- Cg : 可燃性ガス濃度 (vol.%)
- Cx : 酸素濃度 (vol.%)
- CXL : 爆発限界酸素濃度 (vol.%)
- LIB : リチウムイオン 2 次電池

4.3.2 リチウムイオン2次電池の信頼性・安全性試験システムの概要

(1) システムの概要

図 4-4 に LIB の信頼性・安全性試験に広く用いられる信頼性・安全性試験システムの概要を示す。図 4-4 に示す試験システムに用いられる試験槽は、温度制御器を備え、試験槽内の温度入力情報に基づきヒータ回路 (Heater) および冷却装置 (Refrigerator unit) の出力量を制御して試験槽内の温度を一定に維持する。試験槽の耐圧圧力は爆発圧力の 1/10 以下であるため、試験槽本体の上部には、爆発圧力で開閉する機構 (以下、爆発ベントという) を設け爆発発生時の爆発圧力を外部に放出して試験槽の破壊を防止する^{83)~91)}。また、LIB の熱暴走に伴って発生する一酸化炭素等の有害ガスを排出するための非常排煙口が備えられている。試験槽内には LIB が設置されており、充放電装置によって充放電サイクル試験等が行われる。

(2) 各システム要素の動作条件

各機器は、次の条件に従って動作または変化する。

- (a) 正常な爆発ベントは、試験槽内での LIB 熱暴走またはガス爆発に起因する圧力上昇によって開き、圧力低下に伴ってただちに閉まる。
- (b) 爆発発生時、爆発ベントが開口に失敗した場合、試験槽本体が変形または破壊し、扉が開く、または破片が飛び散る等の危険事象が発生する。
- (c) LIB の熱分解反応が始まると、熱分解反応は、熱暴走状態を経て焼損 (熱分解反応が完了) するまで継続し途中で停止しない。
- (d) 均圧口による空気の流出入は、微量であり無視できる。
- (e) 非常排煙システムの動作は、煙感知器等によって行われず、人の判断によって起動ボタンを押して行われる。

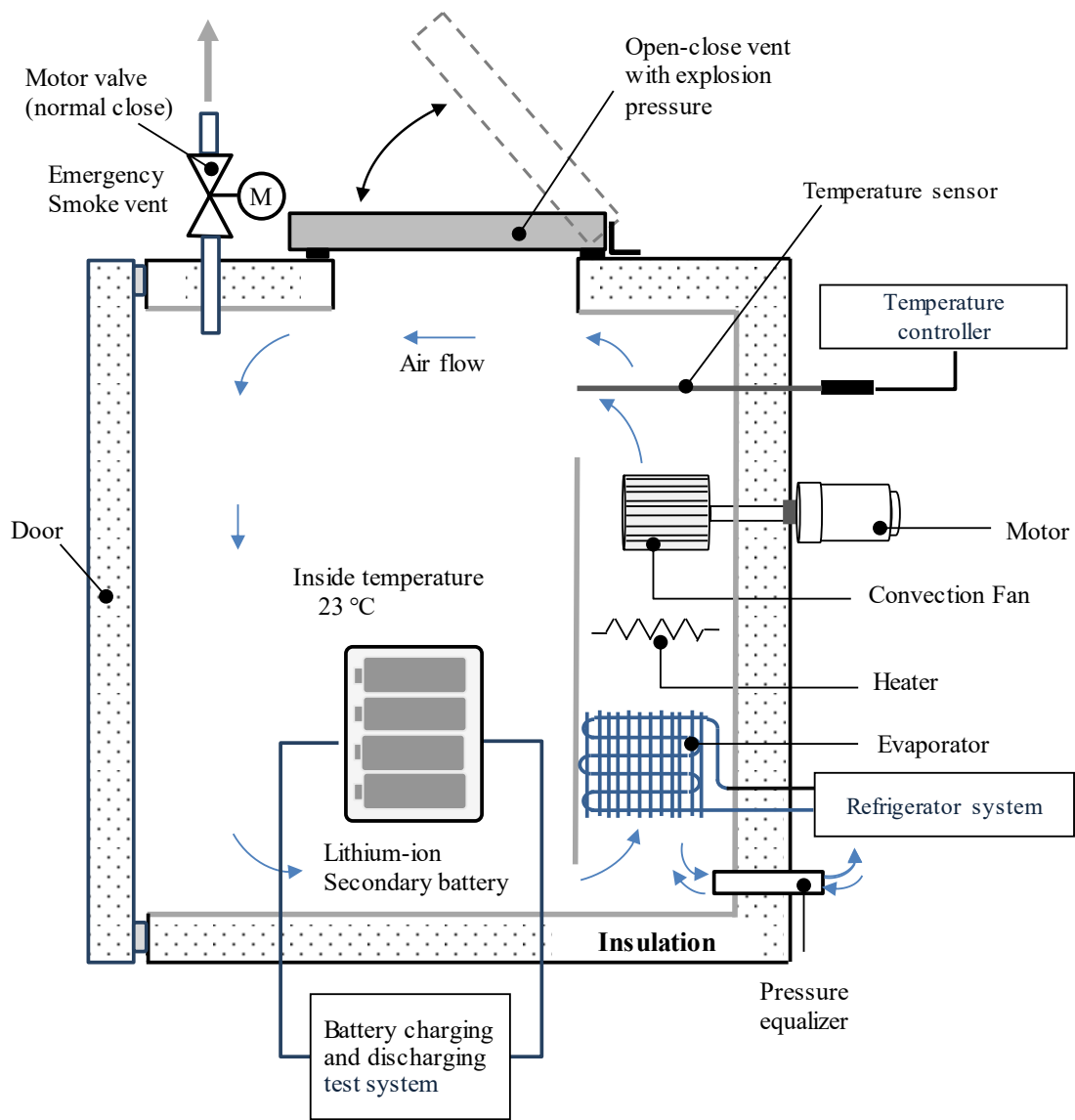


図 4-4 リチウムイオン 2 次電池の信頼性・安全性試験システムの概略図

4.3.3 システム状態の定義

(1) システム要素 $X_{i,j,k}$

システム要素 $X_{i,j,k}$ を表 4-7 のとおり設定する。

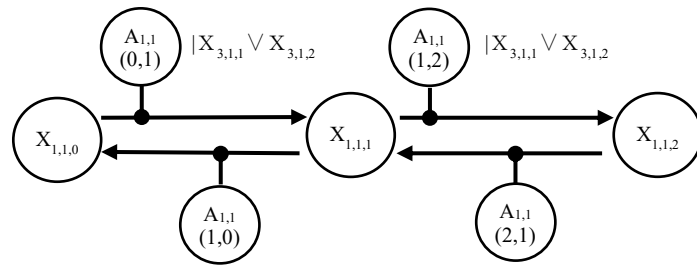
表 4-7 システム要素の状態定義 (LIB 試験システム)

記号	Components i	Attribute j	State variable k
$X_{1,1,0}$	1 : 可燃性ガス	1 : 濃度	0: $C_g < LEL$
$X_{1,1,1}$			1: $LEL \leq C_g < UEL$
$X_{1,1,2}$			2: $C_g \geq UEL$
$X_{2,1,0}$	2 : 酸素	1 : 濃度	0: $C_x < C_{XL}$
$X_{2,1,1}$			1: $C_x \geq C_{XL}$
$X_{3,1,0}$	3 : LIB	1: 化学反応状態	0: 安定状態 (正常状態)
$X_{3,1,1}$			1: 熱分解反応状態 (可燃性ガス放出)
$X_{3,1,2}$			2: 熱暴走状態 (急速な発煙・発火)
$X_{3,1,3}$			3: 不活性 (鎮火) 状態

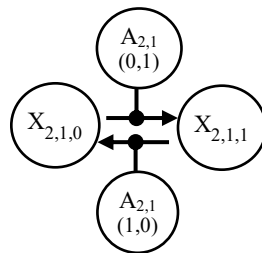
(2) 状態遷移プロセスモデル

システム要素 $X_{i,j,k}$ の状態遷移と遷移作用との次の関係 (a) ~ (c) を図 4-5 に図式化する。

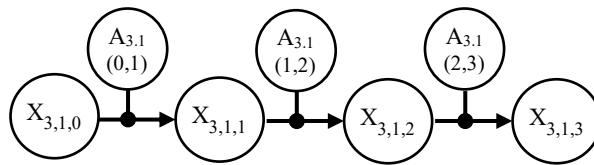
- (a) 可燃性ガスは、それぞれ可逆遷移を行う3状態 $X_{1,1,0}$, $X_{1,1,1}$, $X_{1,1,2}$ を持つ。
また、4個の遷移作用 $A_{1,1}(0,1)$, $A_{1,1}(1,2)$, $A_{1,1}(2,1)$, $A_{1,1}(1,0)$ を持つ。
- (b) 可燃性ガスの発生源は、LIB に限定することとし、 $X_{1,1,0}$ は、LIB の状態 $X_{3,1,1}$ または $X_{3,1,2}$ においてのみ $A_{1,1}(0,1)$ によって $X_{1,1,1}$ に遷移する。また、 $X_{1,1,1}$ は、LIB の状態 $X_{3,1,1}$ または $X_{3,1,2}$ においてのみ $A_{1,1}(1,2)$ によって $X_{1,1,1}$ に遷移する。
- (c) 酸素は、それぞれ可逆遷移を行う2状態、 $X_{2,1,0}$, $X_{2,1,1}$ を持つ。また、2個の遷移作用 $A_{2,1}(0,1)$, $A_{2,1}(1,2)$ を持つ。
- (d) LIB は不可逆遷移を行う4状態 $X_{3,1,0}$, $X_{3,1,1}$, $X_{3,1,2}$ および $X_{3,1,3}$ を持ち、状態 $X_{3,1,2}$ にある LIB は自ら可燃性ガスの着火源となる。また、3個の遷移作用 $A_{3,1}(0,1)$, $A_{3,1}(1,2)$, $A_{3,1}(2,3)$ を持つ。



可燃性ガス濃度



酸素濃度



LIB の化学反応

図 4-5 システム要素の状態遷移プロセスモデル

(3) システム状態の定義

試験槽内の可燃性ガス濃度，酸素濃度および LIB の熱暴走状態に関してシステム状態を定義し表 4-8 に示す。システム要素の組合せより 24 個のシステム状態が定義可能であるが，状態遷移プロセスモデルより，可燃性ガスの発生源は LIB に限定し，LIB の状態 $X_{3,1,1}$ ， $X_{3,1,2}$ は，ガス濃度上昇の必要条件である。次の 4 状態 $S_y' = \{ X_{1,1,1}, X_{2,1,0}, X_{3,1,0} \}$ ， $S_y'' = \{ X_{1,1,1}, X_{2,1,1}, X_{3,1,0} \}$ ， $S_y''' = \{ X_{1,1,2}, X_{2,1,0}, X_{3,1,0} \}$ ， $S_y'''' = \{ X_{1,1,2}, X_{2,1,1}, X_{3,1,0} \}$ は，LIB の状態が $X_{3,1,0}$ であり，4.3.3 項，(2)，(b) の状態遷移プロセスモデルと矛盾するため，予め除外した。さらに表 4-6 に基づき，各システム定義状態において起こり得る事象（出力事象）を想定する。

表 4-8 システム状態の定義 (LIB 試験システム)

生起し得るシステム内部状態	LIB 出力事象
$S_1 = \{ X_{1,1,0}, X_{2,1,0}, X_{3,1,0} \}$	
$S_2 = \{ X_{1,1,0}, X_{2,1,0}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_3 = \{ X_{1,1,0}, X_{2,1,0}, X_{3,1,2} \}$	③高温赤熱物質および有害ガス噴出 (低酸素状態)
$S_4 = \{ X_{1,1,0}, X_{2,1,0}, X_{3,1,3} \}$	
$S_5 = \{ X_{1,1,0}, X_{2,1,1}, X_{3,1,0} \}$	
$S_6 = \{ X_{1,1,0}, X_{2,1,1}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_7 = \{ X_{1,1,0}, X_{2,1,1}, X_{3,1,2} \}$	①発煙, 発火, 破裂, 有害ガス噴出, 爆発ベント開閉
$S_8 = \{ X_{1,1,0}, X_{2,1,1}, X_{3,1,3} \}$	
$S_9 = \{ X_{1,1,1}, X_{2,1,0}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_{10} = \{ X_{1,1,1}, X_{2,1,0}, X_{3,1,2} \}$	③高温赤熱物質および有害ガス噴出 (低酸素状態)
$S_{11} = \{ X_{1,1,1}, X_{2,1,0}, X_{3,1,3} \}$	
$S_{12} = \{ X_{1,1,1}, X_{2,1,1}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_{13} = \{ X_{1,1,1}, X_{2,1,1}, X_{3,1,2} \}$	②ガス爆発 (着火源: LIB), 爆発ベント開閉, 有害ガス噴出,
$S_{14} = \{ X_{1,1,1}, X_{2,1,1}, X_{3,1,3} \}$	
$S_{15} = \{ X_{1,1,2}, X_{2,1,0}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_{16} = \{ X_{1,1,2}, X_{2,1,0}, X_{3,1,2} \}$	
$S_{17} = \{ X_{1,1,2}, X_{2,1,0}, X_{3,1,3} \}$	
$S_{18} = \{ X_{1,1,2}, X_{2,1,1}, X_{3,1,1} \}$	可燃性ガス, 有害ガス放出, 自己加熱進行
$S_{19} = \{ X_{1,1,2}, X_{2,1,1}, X_{3,1,2} \}$	③高温赤熱物質および有害ガス噴出 (低酸素状態)
$S_{20} = \{ X_{1,1,2}, X_{2,1,1}, X_{3,1,3} \}$	

(4) 遷移作用（事象）の設定

遷移作用（事象）は，システム状態を変化させる事象に着目し次のように設定する。

遷移作用（事象）

- (a) LIB 熱分解反応発生
- (b) LIB 自己加熱増大
- (c) 条件 $C_g < LEL$
- (d) 条件 $LEL \leq C_g < UEL$
- (e) 条件 $C_g \geq UEL$
- (f) 爆発ベント開失敗
- (g) 爆発ベント閉失敗
- (h) LIB 熱暴走終了（反応物質の枯渇）
- (i) 槽内混合気流出（排煙口開，扉閉または爆発ベント開）
- (j) 外気流入（排煙口開，扉閉または爆発ベント開）
- (k) 酸素濃度低下（燃焼による酸素消費）
- (l) 密閉状態（排煙口閉，扉閉および爆発ベント閉）
- (m) 衝突
- (n) LIB 外部着火源
- (o) 扉熱変形
- (p) 爆発エネルギー
- (q) 中毒濃度到達
- (r) 人の存在
- (s) 可燃物の存在

(a) ～ (l) は，予め設定された遷移作用であり，(m) ～ (s) は状態遷移プロセスの展開途中に必要な応じて追加された遷移作用である。

4.3.4 ハザードの同定

ハザードの同定に際して、最初に、S-A プロセスチャートの初期状態を決定する。ここでは、初期状態を表 4-9 のとおり設定する。その後、順次、状態と遷移作用を組合せて、危害に至る潜在的状態遷移プロセスを時系列に追跡する。爆発ベント、排煙口、扉等の状態は初期状態からその状態に至る遷移作用を追跡することによりわかるので、本事例では省略し、S-A プロセスチャート上の各システム状態は $X_{i,j,k}$ の組合せのみを明記する。

表 4-9 初期状態 (LIB 試験システム)

項目 NO.	可燃性 ガス濃度	酸素 濃度	電池状態	爆発 ベント	排煙口	扉	槽内 温度
S ₅	X _{1,1,0}	X _{2,1,1}	X _{3,1,0}	閉	閉	閉	23°C

初期状態 S₅ が、各遷移作用によって次々と変化して危害に至る潜在的状態遷移プロセスを図 4-6 に示す。図 4-6 は、次の A~D の危害を同定している。

- A 試験槽での爆発による障害・死亡
- B 施設火災
- C 有毒ガスによる障害
- D 試験槽外（試験槽の設置空間）での爆発による障害・死亡
- E 火傷

SA1~SA4 は、状態遷移プロセス展開中に新たに生じた定義外の状態であり、次を意味している。

- SA1 試験槽外で筐体の破片が飛散
- SA2 試験槽上部爆発ベントから火炎噴出
- SA3 試験槽外でガス爆発
- SA4 高温物質が外部流出

また、状態 S_y の左側の番号①~③は、次の出力事象を表している。

- ① LIB が発煙・発火，爆発ベント開閉，有害ガス噴出
- ② 槽内にてガス爆発発生，爆発ベント開閉，有害ガス噴出
- ③ LIB が赤熱粒子および有害ガス噴出

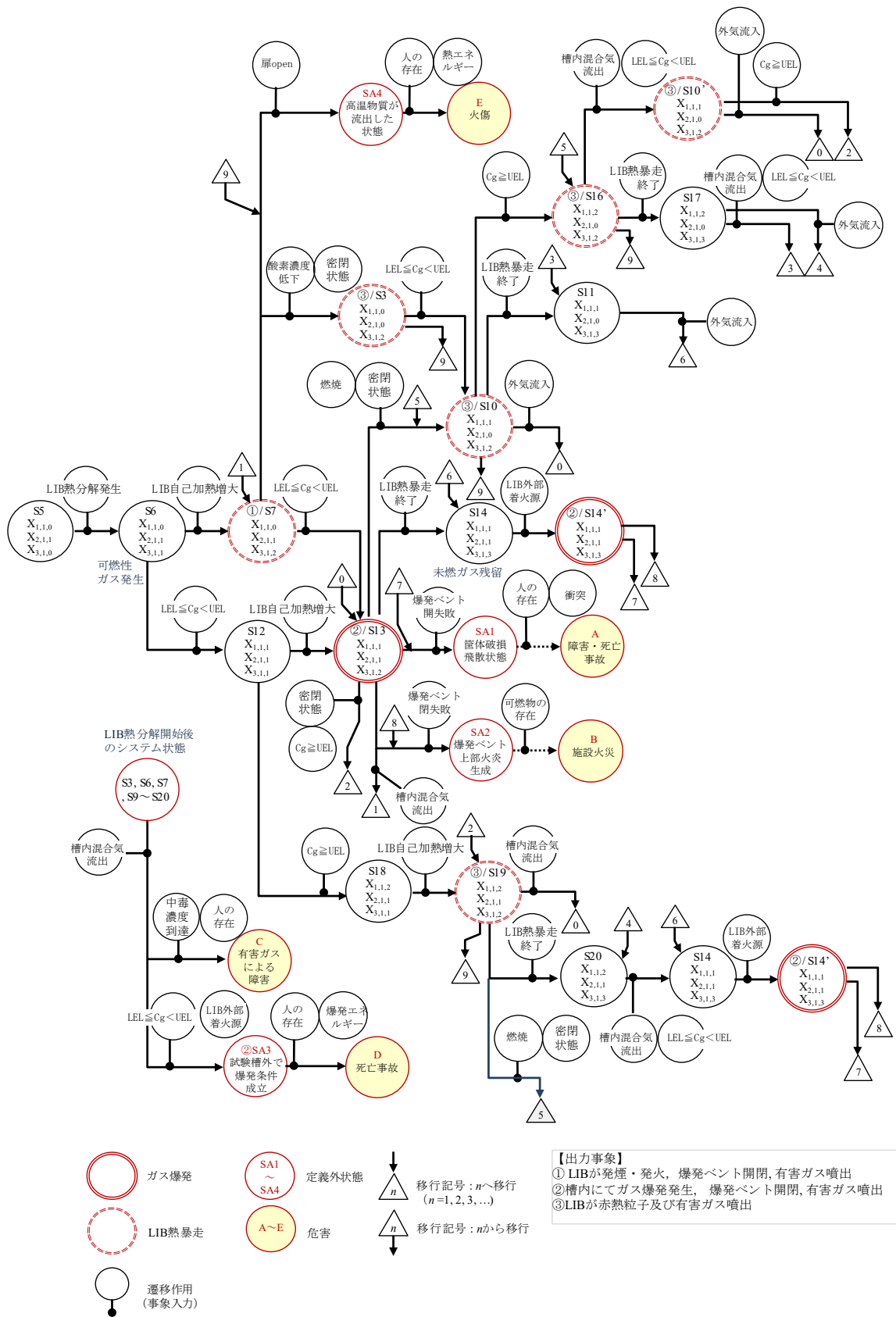
図 4-6 は、それぞれの危害に至る 114 通りの状態遷移プロセスを同定している（付録 1 初期状態～危害に至る図 4-6 の潜在的状態遷移プロセス一覧（No.1～No.114）参照）。付録 1 より No.1～No.10 を抜き出して表 4-10 に示す。

表 4-10 初期状態～危害に至る図 4-6 の潜在的状態遷移プロセス（No.1～No.10）

NO.	初期状態～危害に至る潜在的状態遷移プロセス														
1	S ₅	S ₆	S ₁₂	S ₁₃	SA1	A									
2	S ₅	S ₆	S ₁₂	S ₁₃	SA2	B									
3	S ₅	S ₆	S ₁₂	S ₁₃	SA3	D									
4	S ₅	S ₆	S ₁₂	S ₁₃	C										
5	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	C									
6	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	C								
7	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	C						
8	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	SA1	A					
9	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	SA2	B					
10	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₃	C								

図 4-6 に示すハザードの中から、ハザード 2 を選択し抑制策と共に図 4-7 に示す。ハザード 2 は、表 4-10 の No.2 の状態遷移順序で危害 B “施設火災” を発現する。図 4-7 が示す各ハザードは次のとおりである。

- ① S₅ が，“LIB 熱分解発生”によって，S₆に遷移する。
- ② S₆ が，“ $LEL \leq C_g < UEL$ ”によって，S₁₂に遷移する。
- ③ S₁₂ が，“LIB 自己加熱増大”によって，S₁₃に遷移し爆発が発生する。
- ④ S₁₃ が，“爆発ベント閉失敗”によって，SA2 に遷移し爆発ベント上部に火炎を継続して生成する。
- ⑤ SA2 が，“可燃物の存在”によって，危害 B に遷移する。



4.3.5 ハザード抑制策の導出事例

本項では、図 4-7 に示すハザード 2 の抑制策を系統的に導出する。

(1) 望ましくない状態遷移をなくす、または抑制するハザード抑制策（抑制原理 (a) または (b))

ハザード 2 において、中間事象は存在せず、状態 SA2 はクリティカル状態であり、S₆、S₁₂、S₁₃ はプレクリティカル状態である。したがって、遷移作用 ”LIB 熱分解発生”，“ $LEL \leq C_g < UEL$ ，爆発ベント閉失敗”，“可燃物の存在”は、抑制すべき遷移作用である。ただし、遷移作用”LIB 熱分解発生”は、必ず生起するものとして、その抑制作用 CA4 について考慮しない。

① 遷移作用” $LEL \leq C_g < UEL$ ”の抑制作用 CA3

” $LEL \leq C_g < UEL$ ”は、LIB から放出される可燃性ガスに起因する。ガス濃度を抑制するためには、試験槽内に不活性ガスを送り込み、可燃性ガスを不活性ガスに置換する方策が考えられる（移行制御①および②参照）。

② 遷移作用“LIB 自己加熱増大”の抑制作用 CA2

遷移作用“LIB 自己加熱増大”は、4.3.2, (2), (c)より抑制困難とする。

③ 遷移作用“爆発ベント閉失敗”の抑制作用 CA1

遷移作用“爆発ベント閉失敗”は、“爆発ベントを無くす”すなわち、試験槽の耐圧強度を高めて、ガス爆発圧力に耐え得る構造とすることで抑制可能である。それが不可能な場合、爆発ベントの信頼性を向上させる、爆発ベント開口部にフレームアレスタを増設する等の方策が考えられる。

④ 遷移作用“可燃物存在”の抑制作用 CA0

遷移作用“可燃物の存在”は、爆発ベント周辺を耐火構造とする、爆発ベントからの火炎をダクトで、火炎による 2 次被害の恐れがない区域へ導く等の抑制策が考えられる。

(2) 危害から遠ざかる移行制御によるハザード抑制策（抑制原理 (c))

事例 1 同様、試験槽を制御して、プレクリティカル状態、クリティカル状態、または危害を回避する。S-A プロセスチャートに追加した矢線（点線）が、ハザード抑制の状態遷移のための移行制御を表している。

① 移行制御 1～制御 3

4.3.2 項, (2), (c)より LIB が熱分解反応を開始すると熱暴走は停止しないため、S₆ が生起した場合、ガス濃度抑制の遷移作用 $C_g < LEL$ および酸素濃度抑制の遷移作用 $C_x < C_{XL}$ を用い制御 1～制御 3 によって、システム状態を S₆→S₂→S₃→S₄ と遷移させる。つまり試験槽内のガス濃度および酸素濃度を抑制した状態で LIB の

熱暴走が終了するのを待つ。具体的には、 $C_g < LEL$ は試験槽内の可燃性ガスを不活性ガス（窒素、炭酸ガス等）で置換する、 $C_X < C_{XL}$ は試験槽を密閉し外気を侵入させない、すなわち排煙口、扉および爆発ベント等が閉じられている状態を維持する等の方策が挙げられる。

② 移行制御 4

S_{12} が生じた場合、まず制御 4 を用い S_{12} を S_6 へ遷移させ、次に制御 1～制御 3 によってシステム状態を $S_6 \rightarrow S_2 \rightarrow S_3 \rightarrow S_4$ と遷移させる。 S_{12} の発現は①の制御 1～制御 3 が失敗したことを意味しており、この場合、 $C_g < LEL$ は、2 つの異なる方式によって行われることが望ましい。例えば、①の $C_g < LEL$ は窒素置換システム、②の $C_g < LEL$ は炭酸ガス消化システムで行う等の方策が挙げられる。

③ 移行制御 5～制御 7

S_{13} が生じた場合、制御 1～制御 4 が失敗したことを意味しており、本事例では、 $C_X < C_{XL}$ の遷移作用だけを用い制御 5～制御 7 によって、システム状態を $S_{13} \rightarrow S_{10} \rightarrow S_{16} \rightarrow S_{17}$ へと遷移させることが想定されている。①の制御とは異なり③の制御では、試験槽内の酸素濃度を抑制し、ガス濃度が爆発上限界を超えた状態で LIB の熱暴走が終了するのを待つ。ただし、この方策は、試験槽内のガス濃度を $C_g \geq UEL$ とさせるため、最善の方策ではない。

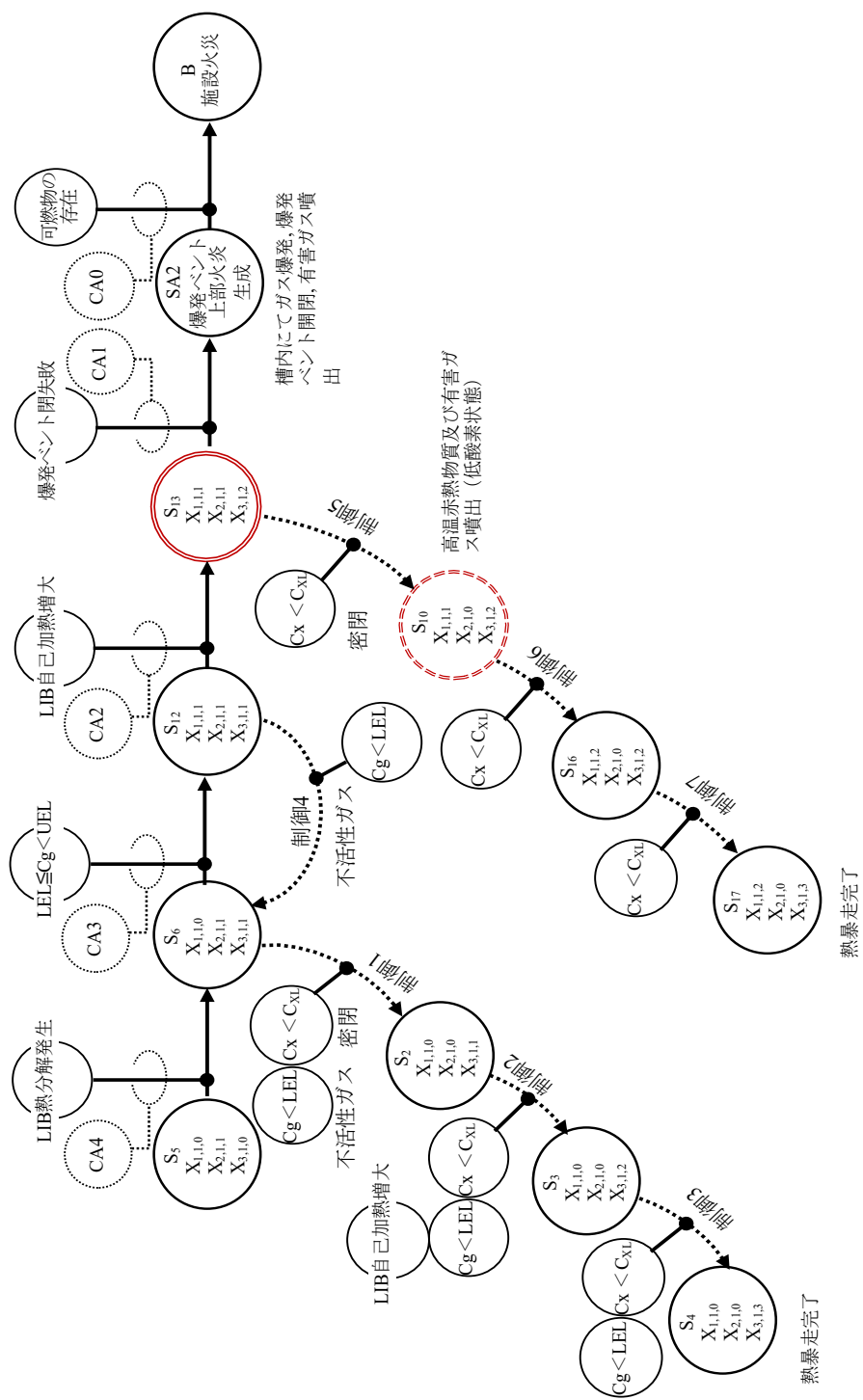


図 4-7 ハザード 2 (図 4-6) の抑制概念図

4.4 第4章のまとめ

ハザードは、システムの状態が内部および外部からの作用によって次々と変化して危害に至るプロセスとして表現できる。S-A プロセスチャートを用いて環境試験槽の停止に起因するハザードおよび LIB の熱暴走に起因するハザードを同定し、その抑制策を導出することにより、次の (1) および (2) を得た。

- (1) システムのそれぞれの状態にシステム要素の故障，エラー（無秩序状態作用）だけでなく，正常機能の履行（秩序状態作用）によって起こる遷移作用を順次作用させることによって，システムの危害に至る状態遷移プロセスを系統的に追跡し，ハザードの網羅的同定が可能である。
- (2) 状態遷移プロセスの状態と遷移作用の配列構造から，ハザード抑制原理に基づき系統的かつ合理的にハザードの抑制策の導出が可能である。

(1) および (2) は，本技法の有効性を裏付ける一端を示すものである。

第 5 章

多状態を持つ要素を含むシステムの S-A プロセスチャートを用いたハザードの分析

第 5 章では、特定された危害と初期状態とを結ぶ状態遷移経路に基づき S-A プロセスチャートを用いハザードを同定するための技法について説明する。

5.1 緒言

危害は、システム要素がアップ状態のまま、あるいはシステム要素がダウン状態からアップ状態に移行することによって起こる場合がある。この課題に対して、本章は、S-A プロセスチャートをハザードの同定技法からすでに生起条件が把握されている危害に対する状態遷移経路の異なるハザードを洗い出すための分析技法へ拡張する。

本提案技法は、まずシステムの各状態を各システム要素が持つ状態の組合せによって定義する。各システム要素状態は遷移作用によって次々と変化し、危害の必要条件を満足する各システム要素状態のある組合せにおいて危害が発現する。危害発現時の各システム要素状態は、故障状態だけでなく正常状態を含む。次にシステム要素が持つ状態の数、状態遷移プロセスの可逆性の有無および状態遷移プロセスの制約条件に基づき、各システム状態の遷移可能な経路が、矢線を用い状態遷移経路図に示される。この状態遷移経路図上で初期状態から各クリティカル状態を経由して危害に至る経路をたどることによって、状態遷移経路の異なるハザードを系統的・網羅的に洗い出し、S-A プロセスチャートで図式化する。一般的な FTA (Fault Tree Analysis), FMEA (Failure Modes and Effects Analysis) 等の従来技法は、システム要素の可逆または不可逆遷移する多状態を扱わないので、状態遷移順序および相反ハザード等の動的分析は困難である。

本提案技法の有効性を検証するために、事例 1 では“着火エネルギー”を 2 状態、“可燃性ガス濃度”を 3 状態にモデル化し、事例 2 では“走行コース”を 2 状態、“車間距離”を 3 状態にモデル化し、ガス爆発および後方車が前方車に追突するプロセスの分析に S-A プロセスチャートを適用する。

5.2 事例検証

事例 1 において“ガス爆発”，事例 2 において“後方車が前方車に追突”の発現プロセスを分析し、その有効性を検証する。

5.2.1 記号および略語

5.2 節で使用する記号および略語は、次のとおりである。

記号

- De 車間距離
Db ブレーキ作動後停止するまでの距離

略語

- LEL 爆発下限界濃度 (vol.%)
UEL 爆発上限界濃度 (vol.%)
Cg 可燃性ガス濃度 (vol.%)
MIE 最小着火エネルギー⁹²⁾ (mJ)
IE 着火エネルギー (mJ)

5.2.2 事例1：溶剤乾燥器のガス爆発の分析

(1) システムの概要

システムの概要を図 5-1 に示す。このシステムは、換気ファン（給気ファンおよびローペラファン）および排気口からなる換気システム、ヒータユニットとそれを制御する制御機器（温度センサおよび温度制御器）によって構成されている。溶剤乾燥器の乾燥エリアには、可燃性の溶剤を含む被乾燥物が設置されている。乾燥器下部の給気ファンによって新鮮空気を乾燥器内に導入し、新鮮空気はヒータユニットで加熱され、熱風となって乾燥エリアに送り込まれる。熱風によって被乾燥物から発生する可燃性ガスは、溶剤乾燥器内を循環することなく排気され、可燃性ガス濃度が抑制される。

(2) システム要素の状態定義

可燃性ガス爆発が発現するために必要な要素は、可燃性ガス、酸素、および着火エネルギーである⁹³⁾。単純化のために、ここでは、酸素は常時存在するものとして、可燃性ガスと酸素の混合気（以下、可燃性混合気という）と着火エネルギーの状態を用いシステム状態を定義する。

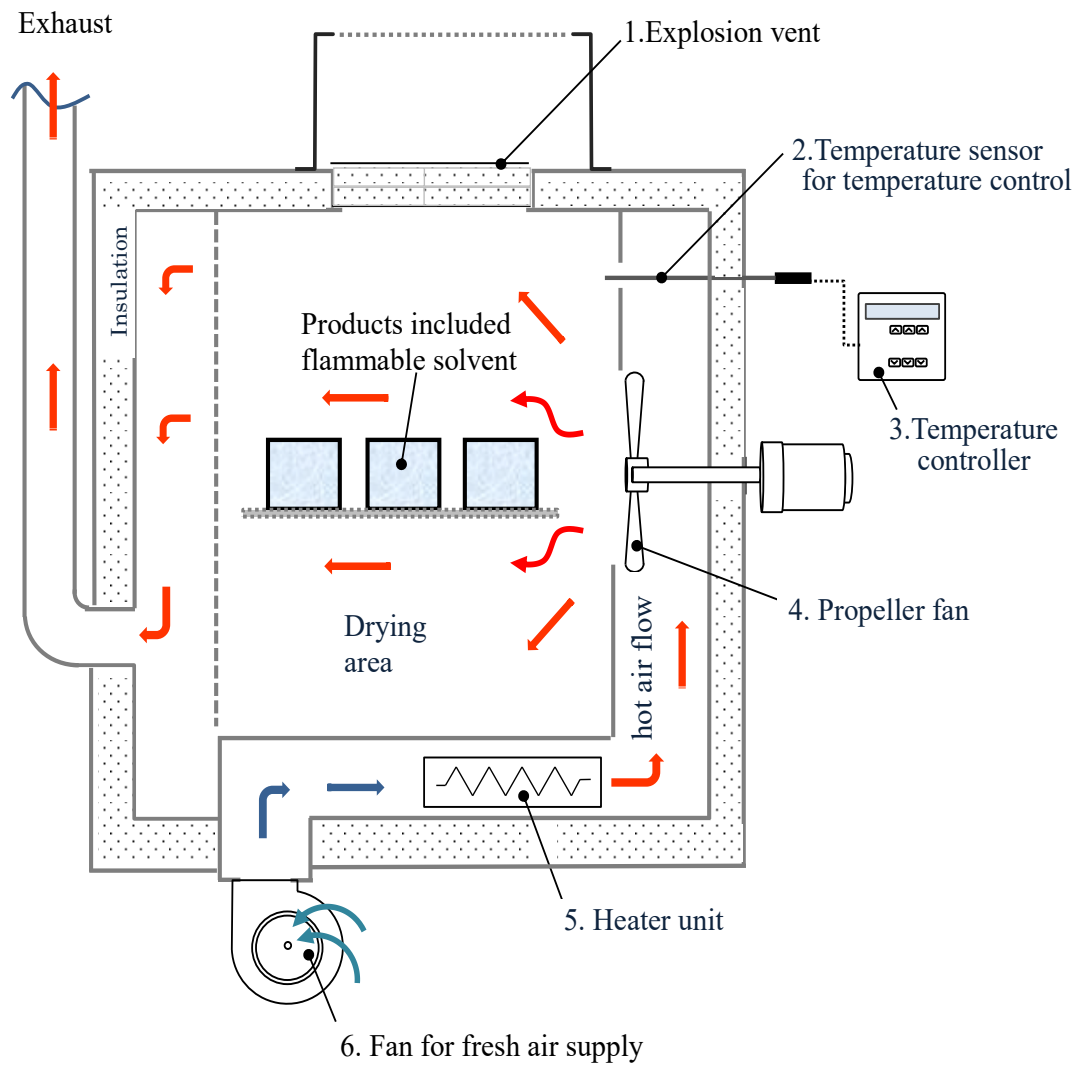


図 5-1 溶剤乾燥器のシステム構造

システム要素 $X_{i,j,k}$ を表 5-1 のとおり設定する。

表 5-1 システム要素の状態定義

$X_{i,j,k}$	Components i	Attribute j	State variable k
$X_{1,1,0}$	1: 可燃性混合気	1: ガス濃度	0: $C_g < LEL$
$X_{1,1,1}$			1: $LEL \leq C_g < UEL$
$X_{1,1,2}$			2: $C_g \geq UEL$
$X_{1,2,0}$		2: 着火エネルギー	0: $IE < MIE$
$X_{1,2,1}$			1: $IE \geq MIE$

(3) 状態遷移プロセスモデル (可燃性混合気)

システム要素 $X_{i,j,k}$ の状態遷移と遷移作用との関係 (a) ~ (b) を図 5-2 に図式化する。

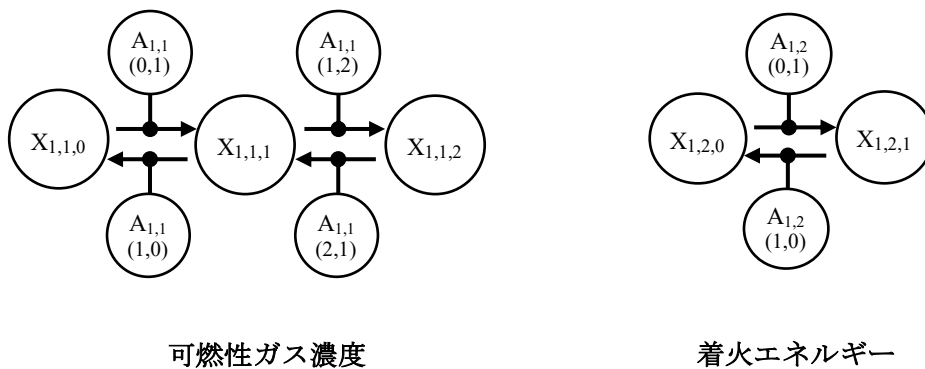


図 5-2 システム要素の状態遷移プロセスモデル

(4) $A_{ij}(k,k')$ を生起させる $E_{ij}(k,k')$ の設定


本事例では、システム要素によって行われる $A_{ij}(k,k')$ を具体的に考察するために、 5-2 に示す遷移作用 $A_{ij}(k,k')$ を生起させる事象 $E_{ij}(k,k')$ を表 5-2 のとおり対応させる。ここで、TYPE IA は無秩序状態作用、AA は秩序状態作用を意味する。

表 5-2 各遷移作用を生起させる事象

Transition action $A_{ij}(k,k')$	Event $E_{ij}(k,k')$ that cause $A_{ij}(k,k')$		Type
$A_{1,1}(0,1)$: The action that changes $X_{1,1,0}$ to $X_{1,1,1}$	E01	Air exhaust line is closed	IA
	E02	Air supply line is closed	
	E03	Ventilation is stopped	
	E04	The temperature in the drying oven is increased	
	E05	Products included flammable solvents are added.	
$A_{1,1}(1,2)$	Same as E01~ E05		
$A_{1,1}(1,0)$: The action that changes $X_{1,1,1}$ to $X_{1,1,0}$	E06	Air exhaust line is opened	AA
	E07	Air supply line is opened	AA
	E08	Ventilation is restarted	AA
	E09	A flammable gas leak path is formed.	IA
	E10	The temperature in the drying oven is decreased due to failure of the required function.	IA
	E11	The temperature in the drying oven is decreased due to performance of the required function.	AA
E12	The amount of flammable gas evaporation decreases with the progress of the drying process.	AA	
$A_{1,1}(2,1)$:	Same as E06~ E012		
$A_{1,2}(0,1)$: The action that changes $X_{1,2,0}$ to $X_{1,2,1}$	E13	Sparks are generated due to the start /stop of electrical devices.	IA
	E14	Static electricity is generated.	IA
	E15	Impact force is generated.	IA
	E16	A hot surface is generated such as a red-heated heater surface.	IA
	E17	The temperature in the drying oven increases to the ignition point of the flammable gas.	IA
$A_{1,2}(1,0)$: The action that changes $X_{1,2,1}$ to $X_{1,2,0}$	E18	Static relay is applied.	AA
	E19	Electrostatic is discharged.	AA
	E20	The heater circuit is shut off.	AA
	E21	The enclosure covers the ignition source.	AA
	E22	The air in the drying oven is replaced by inert gas.	AA

AA: Activated action

IA: Inert action

(5) ガス爆発のシステム状態遷移表および状態遷移経路図

各システム要素状態 $X_{i,j,k}$ を組合せることより 6 個のシステム状態 S_y が定義可能である。また、表 5-1 および図 5-2 に基づき 3.7.3 項の表 3-1 と同じシステム状態遷移表および図 3-7 と同じ状態遷移経路図を得る。さらに図 3-7 に対して S-A プロセスチャートを導出するための導出条件 $C_{r1} \sim C_{r4}$ を適用した場合の状態遷移経路図を図 5-3 に示す。

- C_{r1} 初期状態 $S_{ys} = S_1$ (正常状態)
- C_{r2} 最終状態 $S_{ye} = S_4$ (爆発状態)
- C_{r3} S_{ys} は繰返し出現しない
- C_{r4} S_{ye} は繰返し出現しない (爆発によってシステムは停止する)

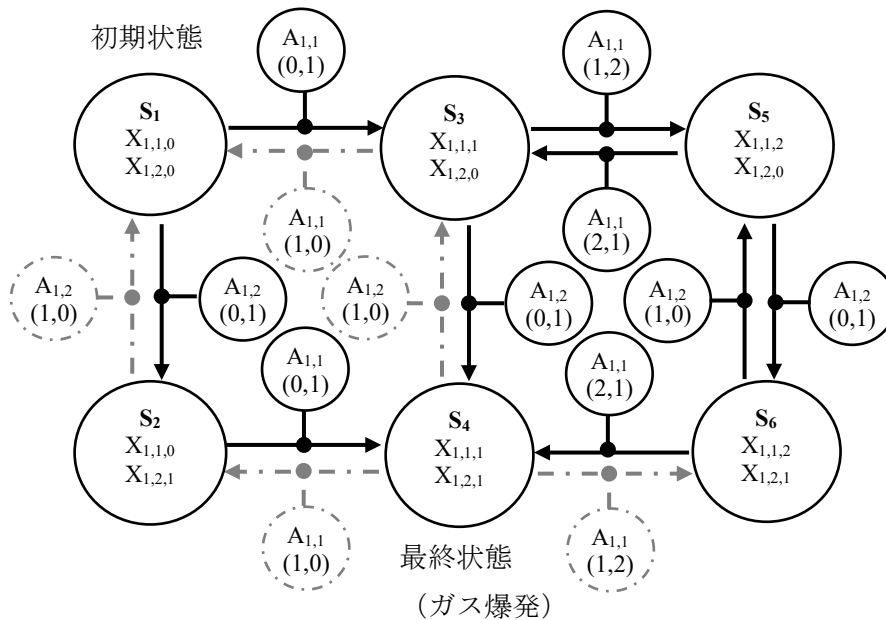


図 5-3 導出条件 $C_{r1} \sim C_{r4}$ を図 3-7 に適用した場合の状態遷移経路図 (ガス爆発の場合)

図 5-3 において一点鎖線で示された状態遷移 $S_3 \rightarrow S_1$, $S_2 \rightarrow S_1$, $S_4 \rightarrow S_2$, $S_4 \rightarrow S_3$ および $S_4 \rightarrow S_6$ は、導出条件 $C_{r1} \sim C_{r4}$ によって S-A プロセスチャートの導出に際して省くことが可能である。図 5-3 は、システム構造に関係なく可燃性ガス濃度と着火エネルギーとに起因して爆発に至る経路を一般化している。

(6) 状態遷移経路図からの S-A プロセスチャートの導出

図 5-3 に対して、さらに次の導出条件 $C_{r5} \sim C_{r7}$ を適用することによって、初期状態から最終状態（危害）に至る 4 つの経路が確定し、図 3-10 と同じ S-A プロセスチャート（ハザード 1～ハザード 4）が導かれる。

C_{r5} 1 つの経路は、同じ $A_{ij}(k, k')$ を含まない。

C_{r6} 1 つの経路は、同じ状態を含み得る。

C_{r7} 各クリティカル状態を経由する少なくとも各 1 個の経路が存在する。

本事例では、3.7.4 項に示した条件下では $S_y \rightarrow S_y' \rightarrow S_y$ の 2 回以上の繰り返しは省くことが可能であり、導出条件 $C_{r5} \sim C_{r6}$ によって繰り返し回数は、1 回に制限されている。

(7) 遷移作用の具象化によるシステム要素挙動分析

システム要素によって行われる $A_{ij}(k, k')$ の挙動を、表 5-2 に示す各 $A_{ij}(k, k')$ と各 $E_i(k, k')$ との関係に基づき具体的に考察する。図 3-10 のハザード 3 を抑制概念と共に図 5-4 に示す。図 5-4 は、次のハザードを表している。

- ① S_1 が遷移作用 $A_{1,1}(0,1)$ すなわち事象 E01～E05 によって S_3 に遷移する。
- ② S_3 が遷移作用 $A_{1,1}(1,2)$ すなわち事象 E01～E05 によって S_5 に遷移する。
- ③ S_5 が遷移作用 $A_{1,2}(0,1)$ すなわち事象 E13～E17 によって S_6 に遷移する。
- ④ S_6 が遷移作用 $A_{1,1}(2,1)$ すなわち事象 E06～E12 によって S_4 に遷移する。
- ⑤ S_4 において、ガス爆発が発生する。

また、図 5-4 は、次の①～⑦の抑制概念を表している。

- ① $A_{1,1}(0,1)$ を抑制する CA3 の適用
- ② S_3 から S_1 へ向かう制御 1 の適用（移行制御： $A_{1,1}(1,0)$ を伴う制御）
- ③ $A_{1,1}(1,2)$ を抑制する CA2 の適用
- ④ S_5 から S_3 へ向かう制御 2（移行制御： $A_{1,1}(2,1)$ を伴う制御）、さらに S_1 へ向かう制御 1 の適用
- ⑤ $A_{1,2}(0,1)$ を抑制する CA1 の適用
- ⑥ S_6 から S_5 へ向かう制御 3（移行制御： $A_{1,2}(1,0)$ を伴う制御）、さらに S_3 を経由して S_1 へ向かう制御 2 および制御 1 の適用
- ⑦ $A_{1,1}(2,1)$ を抑制する CA0 の適用

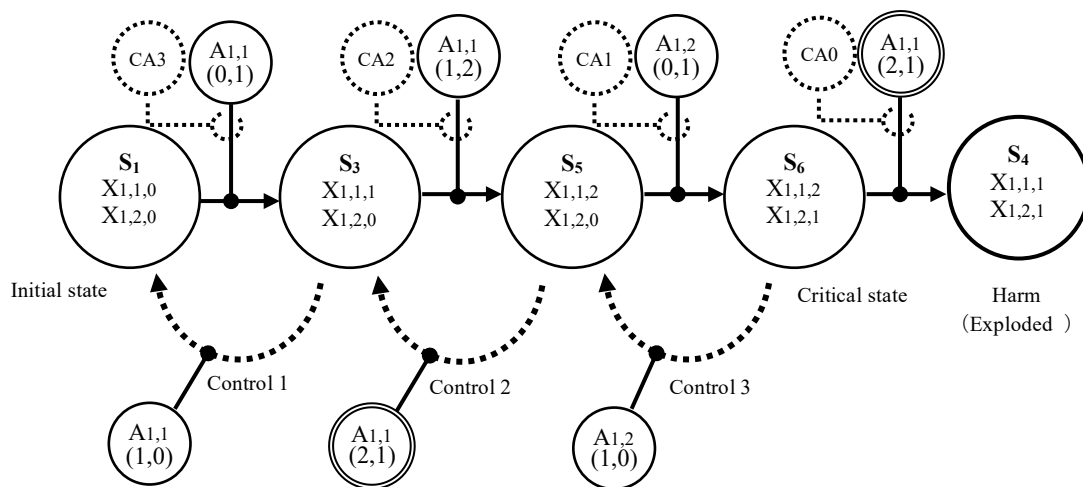


図 5-4 ハザード 3 (図 3-10) の抑制概念図

図 5-4 の S-A プロセスチャートにおいて、クリティカル状態 S_6 は、抑合作用 CA3, CA2, CA1, 制御 1, 制御 2 がすべて無効、または失敗した場合に生起すると考えられる。2 重丸で示した $A_{1,1} (2,1)$ は、システム要素の正常な機能の履行 (E06~E08, E11, E12), すなわちシステム要素の秩序状態作用によって行われる $A_{i,j} (k,k')$ を含む。 $A_{1,1} (2,1)$ は、クリティカル状態 S_6 に対して危害を発現させる遷移作用であり、 S_5 に対して S_5 を危害とは反対方向の S_3 に向かわせる抑合作用であることが図 5-4 からわかる。これは、ガス爆発の必要条件の一つであるガス濃度の状態 $X_{1,1,1}$ が、ガス濃度をもつ 3 状態の中央に位置し、 $X_{1,1,1}$ への変化が $A_{1,1} (0,1)$ と $A_{1,1} (2,1)$ とによって双方向から行われることに起因している。ある状態では抑合作用となり、別の状態では危害へと向かわせる $A_{i,j} (k,k')$ は、秩序状態作用によって行われ得る。この様な $A_{i,j} (k,k')$ は、常時、システム状態を検出して、危害に向かう遷移作用とならない様、制御される必要がある。例えば、図 5-4 においてクリティカル状態 S_6 が発現した場合、次の①~⑥に示す危害とは反対の方向へ向かわせるプロセスが考えられる。ここで、 S_5 の $X_{1,2,0}$ の実現に A22 を用いる理由は、着火エネルギーの直接的な検知の困難さによる。

- ① ガス濃度計等で $X_{1,1,2}$ を確認する。
- ② CA0 : 給気経路を閉鎖 (A02), 換気ファンの停止 (A03) 等を継続し、 $X_{1,1,2}$ を維持する。
- ③ 制御 3 : 乾燥器内の酸素濃度を不活性ガスで置換 (E22) する。
- ④ 酸素濃度計等で $X_{1,2,0}$ を確認する (S_5 への移行完了確認)。
- ⑤ 不活性ガスの供給を継続し、不活性ガスによる換気を行う。

- ⑥ ガス濃度計等で、乾燥器内のガス濃度が $X_{1,1,2} \rightarrow X_{1,1,1} \rightarrow X_{1,1,0}$ と変化し、システムの状態が状態 S_1 に移行したことを確認する。

次に、**図 3-10** のハザード 1 およびハザード 2 を **図 5-5** に示す。

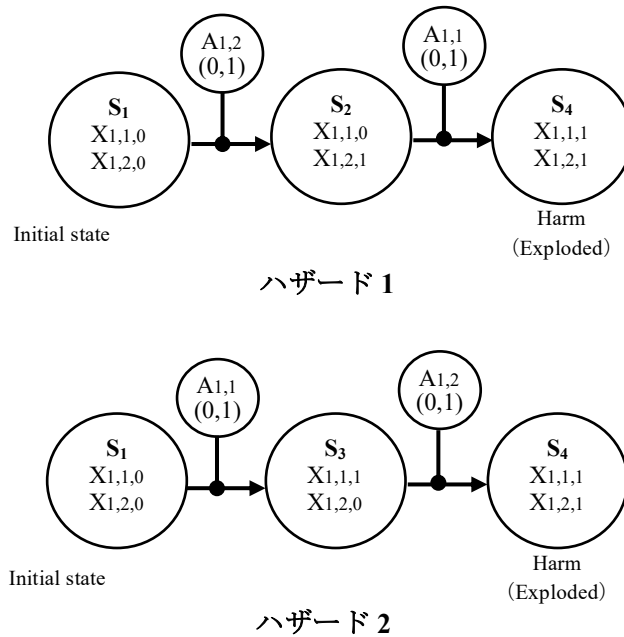


図 5-5 ハザード 1 およびハザード 2 (**図 3-10**)

図 5-5 は次のハザードを表している。

ハザード 1

- ① S_1 が遷移作用 $A_{1,2} (0,1)$ すなわち事象 $E_{13} \sim E_{17}$ によって S_2 に遷移する。
- ② S_2 が遷移作用 $A_{1,1} (0,1)$ すなわち事象 $E_{01} \sim E_{05}$ によって S_4 に遷移する。
- ③ S_4 において、ガス爆発が発生する。

ハザード 2

- ① S_1 が遷移作用 $A_{1,1} (0,1)$ すなわち事象 $E_{01} \sim E_{05}$ によって S_3 に遷移する。
- ② S_3 が遷移作用 $A_{1,2} (0,1)$ すなわち事象 $E_{13} \sim E_{17}$ によって S_4 に遷移する。
- ③ S_4 において、ガス爆発が発生する。

$A_{1,1} (0,1)$ および $A_{1,1} (2,1)$ が換気システムの動作に起因するとして、ハザード 1～ハザード 3 と事象 E_1 : 換気システム稼働状態→停止状態への変化および事象 E_2 : 換気システム停止状態→稼働状態への変化との関係を **表 5-3** に示す。

表 5-3 溶剤乾燥器の相反ハザードと換気システム動作との関係

ハザード No.	換気システム動作	
	E ₁ : 稼働状態→停止状態	E ₂ : 停止状態→稼働状態
1	危険側	安全側
2	危険側	安全側
3	S ₁ に対して危険側	S ₁ に対して安全側
	S ₆ に対して安全側	S ₆ に対して危険側

ハザード 1, ハザード 2 およびハザード 3 の S₁ に対して事象 E₁ は危険側であり, ハザード 1, ハザード 2 およびハザード 3 の S₆ に対して E₂ は安全側である。すなわち, E₁ および E₂ に関してハザード 1 とハザード 3, およびハザード 2 とハザード 3 は相反ハザードである。

図 5-6 は, ハザード 4 の抑制概念を表している。ハザード 4 とハザード 3 は, 同じ A_{ij} (k, k') で構成されているが, A_{ij} (k, k') の順序が入れ替わることによって, システム状態の組合せが {S₁, S₃, S₄, S₅, S₆} から {S₁, S₃, S₄, S₅} に変化する。また, 図 5-6 において A_{1,1} (2,1) は, 危害を発現させる遷移作用ではなく, プレクリティカル状態 S₅ をクリティカル状態 S₃ に向かわせる遷移作用であり, 同時に, S₅ を危害とは反対方向の S₃ に向かわせる遷移作用である。S₃ は, S₅ の前後に存在する。S₁ から遷移した S₃ は CA3 失敗によって, また, S₅ から遷移した S₃ は CA3, 制御 1, CA2, 制御 2, CA1 の失敗によって発現した状態であるとも考えられ, ハザードの抑制概念の観点から, 両者は区別できる。

例えば, 事例 1 においてクリティカル状態 S₃ が発現した場合, 次の①～④に示す危害とは反対の方向へ向かわせる状態遷移 (移行制御) が考えられる。ここで, S₃ から S₁ へ移行するために A22 を用いる理由は, 換気システムの故障を前提とすることによる。

- ① ガス濃度計等で X_{1,1,1} を確認する。
- ② CA0: 給気経路を閉鎖 (A02), 乾燥器内の酸素濃度を不活性ガスで置換 (A22) する。
- ③ 制御 3: 不活性ガスの供給を継続し (A22), 不活性ガスによる換気を行う。
- ④ ガス濃度計等で, 乾燥器内のガス濃度が X_{1,1,1}→X_{1,1,0} と変化し, システムの状態が状態 S₁ へ移行したことを確認する。

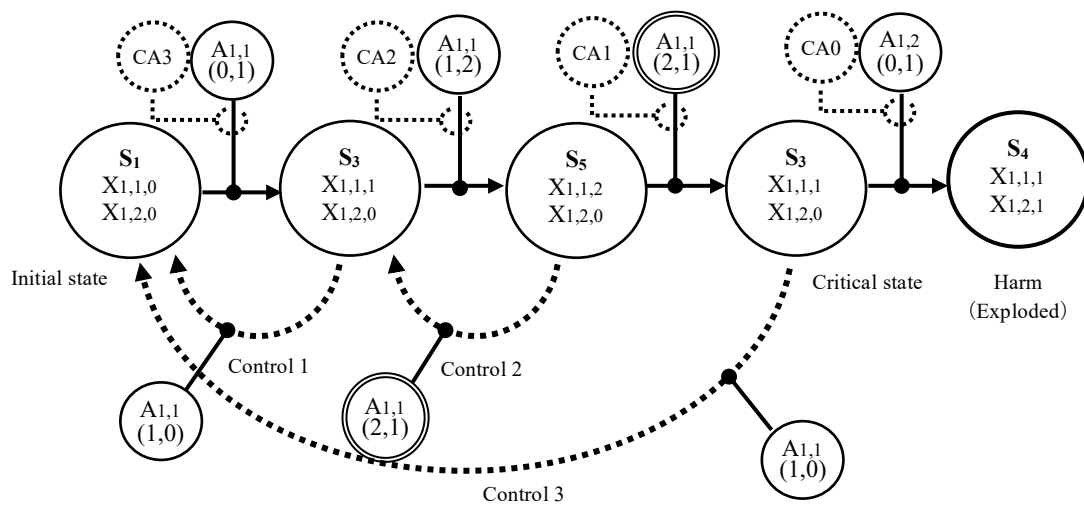


図 5-6 ハザード 4 (図 3-10) の抑制概念図

5.2.3 事例2 後方車が前方車に追突の分析

後方車が先行車の接近に気づかずに追突するプロセスを洗い出す。後方車と前方車との車間距離および走行コースの状態を用い S_p を定義する。対向車は存在せず、コース変更は瞬時に行われるものとする。

(1) システム要素の状態定義

システム要素 $X_{i,j,k}$ を表 5-4 のとおり設定する。

表 5-4 システム要素の状態定義 (後方車及前方車)

$X_{i,j,k}$	Components i	Attribute j	State variable k
$X_{1,1,0}$	1: 後方車 および前方車	1: 車間距離	0: $D_e > D_b$
$X_{1,1,1}$			1: $D_e \leq D_b$
$X_{1,1,2}$			2: $D_e = 0$
$X_{1,2,0}$		2: 走行コース	0: 後方車と前方車とが異なる コースに存在
$X_{1,2,1}$			1: 後方車と前方車とが同一 コースに存在

(2) 状態遷移プロセスモデル

システム要素 $X_{i,j,k}$ の状態遷移と遷移作用との関係を図 5-7 に示す。

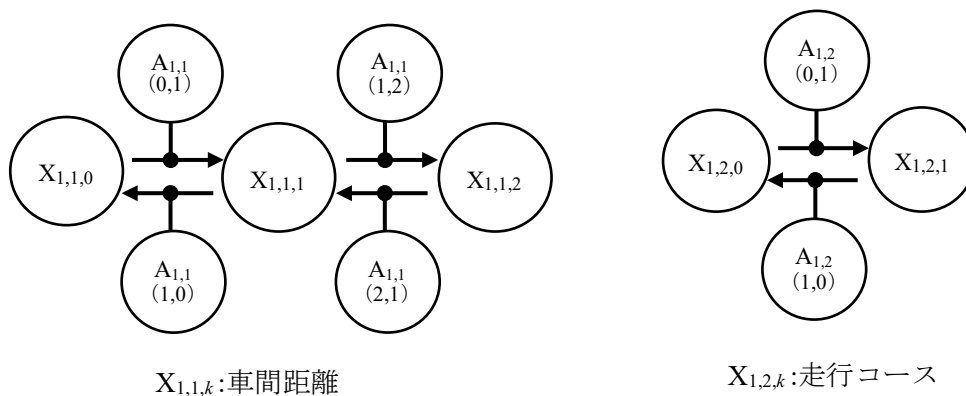


図 5-7 システム要素の状態遷移プロセスモデル

(3) 後方車が前方車に追突のシステム状態遷移表および状態遷移経路図

各システム要素状態 $X_{i,j,k}$ を組合せることより 6 個のシステム状態 S_y が定義可能である。また、表 5-4 および図 5-7 に基づき 3.7.3 項の表 3-1 と同じシステム状態遷移表および図 3-7 と同じ状態遷移経路図を得る。さらに図 3-7 に対して次の導出条件 $C_{r1} \sim C_{r4}$ を適用した場合の状態遷移経路図を図 5-8 に示す。

- C_{r1} 初期状態 $S_{ys} = S_1$
- C_{r2} 最終状態 $S_{ye} = S_6$ (追突)
- C_{r3} S_{ys} は繰返し出現しない。
- C_{r4} S_{ye} は繰返し出現しない

図 5-8 において一点鎖線で示された $S_3 \rightarrow S_1$, $S_2 \rightarrow S_1$, $S_6 \rightarrow S_4$ および $S_6 \rightarrow S_5$ は、導出条件 $C_{r1} \sim C_{r4}$ によって S-A プロセスチャートの導出に際して省くことが可能である。

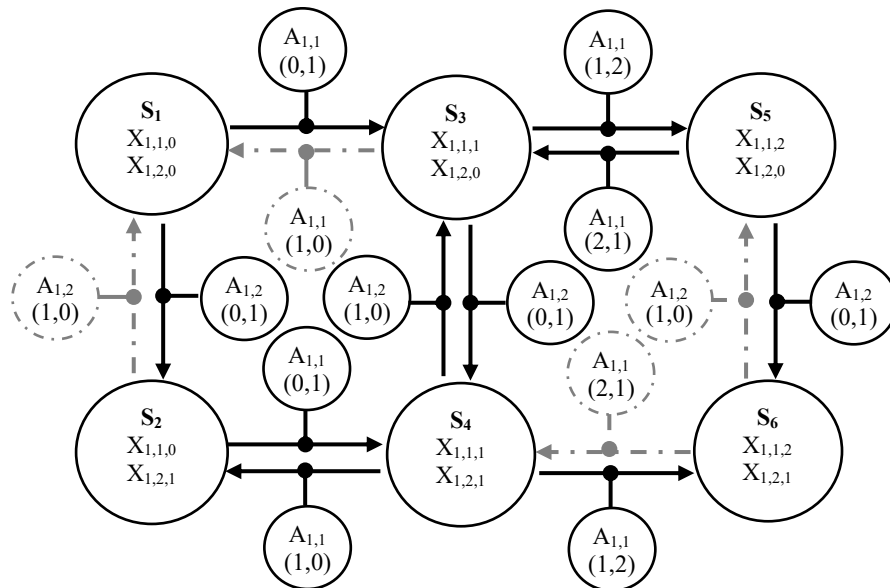


図 5-8 導出条件 $C_{r1} \sim C_{r4}$ を図 3-7 に適用した場合の状態遷移経路図
(事例 2 後方車が前方車に追突の場合)

(4) 後方車が前方車に追突の S-A プロセスチャートの導出

図 5-8 に対して，さらに次の導出条件 $C_{r5} \sim C_{r7}$ を適用することによって，初期状態から危害（最終状態）に至る 3 つの経路が確定し，図 5-9 の S-A プロセスチャート（ハザード 5～ハザード 7）が導かれる。

C_{r5} 1 つの経路は，同じ $A_{ij}(k,k')$ を含まない。

C_{r6} 1 つの経路は，同じ状態を含み得る。

C_{r7} 各クリティカル状態を経由する少なくとも各 1 個の経路が存在する。

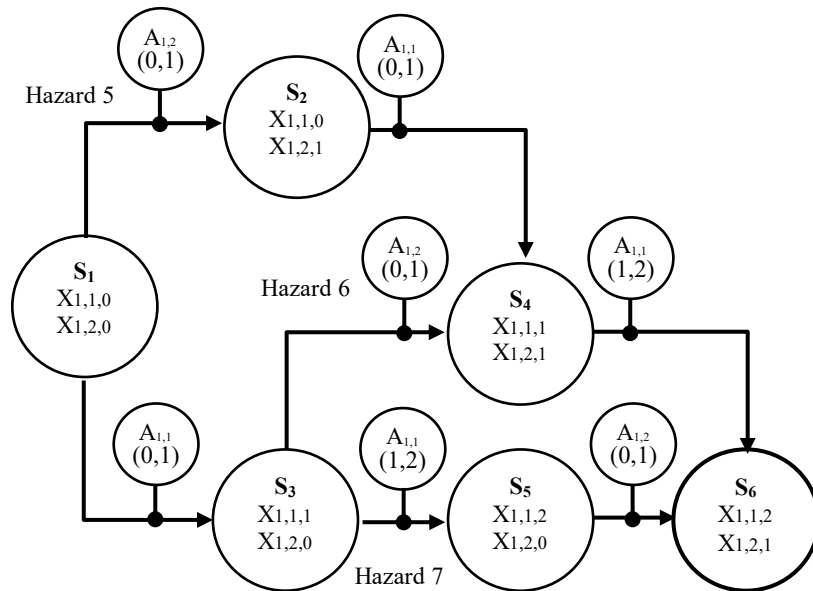


図 5-9 状態遷移経路図 (図 5-8) に $C_{r5} \sim C_{r7}$ を適用して求めた S-A プロセスチャート

(5) ハザード5の抑制概念

図5-10は、ハザード5の抑制概念を表している。ハザード5において、ある状態ではシステムの状態を危害に向かわせる $A_{1,1}(1,2)$ が、別の状態では抑制作用となることはない。これは、追突の必要条件の一つである車間距離の状態 $X_{1,1,2}$ が、車間距離がもつ3状態の右端に位置し、 $X_{1,1,2}$ への変化が $A_{1,1}(1,2)$ によってのみ行われることに起因している。

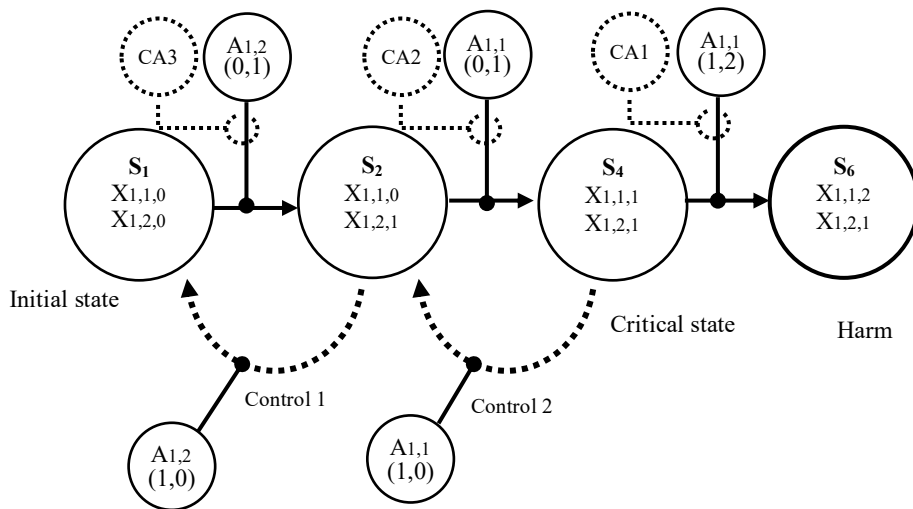


図 5-10 ハザード5の抑制概念図

5.3 第5章のまとめ

第5章では、S-A プロセスチャートをハザードの同定技法から、状態遷移経路の異なるハザードを洗い出すための分析技法へ拡張した。本提案技法は、多状態を持つシステム要素の状態遷移プロセスモデルに基づいて、まずシステムの状態を2状態またはそれ以上の状態をもつシステム要素の状態の組合せによって定義する。次に各状態の遷移できるすべての経路を、矢線を用い状態遷移経路図に示した。

- (1) この状態遷移経路図上で、初期状態と危害を結ぶ経路をたどることで、状態遷移経路の異なるハザードを系統的・網羅的に洗い出せることを示した。
- (2) 事例に対して検討・考察した結果、多状態をもつシステム要素の次の特性を示した。
 - (a) システム要素が可逆遷移を行う3状態を持ち、3状態の中央の状態がシステムの危害の必要条件となり得る場合、ある $A_{ij}(k, k')$ は、抑制作用にも危害に向かわせる作用にもなり得る。
 - (b) システム要素が可逆遷移を行う3状態を持ち、3状態の端の状態がシステムの危害の必要条件となり得る場合、ある $A_{ij}(k, k')$ は、抑制作用または危害に向かわせる作用のどちらかにはなるが、両方になることはない。

(2) , (a) の場合には、序論に記した課題、すなわち、相反ハザードを持つシステムでは、あるハザードの抑制を目的とする機能の履行（安全側事象）が、他のハザードでは危害を発生させる危険側事象となり得る。また、その危険側事象は、故障、エラー、失敗等だけでなく、システム要素の正常な要求機能の履行、修復、回復等によって行われる可能性があることを S-A プロセスチャートを用い特定できた。本提案技法の“ある危害に至る状態遷移経路の異なるハザードを系統的・網羅的に洗い出す”特徴は、一般的な FTA 等の従来技法では見落としやすい状態遷移順序に依存する相反的事象を含むハザードを洗い出す。本論文は、ガス爆発の事例を用い換気システムの起動と停止とが、ある状態では抑制作用となり、別の状態では危害へ向かわせる遷移作用を伴う事象であることを S-A プロセスチャート上で特定した。換気システムのこのような挙動は、可逆遷移を行うガス濃度の3個の状態の中央にガス爆発を起こす必要条件が位置していることに起因する。

第 6 章

S-A プロセスチャートから導出される FT による事象生起順序依存ハザードの分析

第 6 章では、まず S-A プロセスチャートで表される状態変化および遷移作用と FT (フォールトツリー) の事象とが関連付けられた優先 AND 構造を持つ FT (S-A-FT) への展開法を提案する。次に、2 冗長電源システムの故障に至るプロセスの分析に本技法を適用し、S-A-FT では S-A プロセスチャートと FTA とが互いに補完的役割を担うことによって、合理的なハザードおよびリスクの分析が可能となることを示す。

6.1 緒言

ハザードをより詳細に分析するためには、システムレベルの事象および状態とこれを生成させるシステムの要素レベルの変化との関係を明らかにする必要がある。しかし S-A プロセスチャートは部品の故障等、システム要素レベルでの分析に適していない。一方、従来技法である FTA (Fault Tree Analysis) は同定されたハザードを頂上事象として、システムの要素レベルの変化まで分析が可能であるが、ハザードの同定すなわち頂上事象およびその生起プロセスの洗い出しを行うことは困難である。また、主に信頼性工学分野で用いられるコヒーレントシステム^{94)~98)}を前提とする FT では、頂上事象(要求機能失敗)はシステム要素がアップ状態からダウン状態に移行することによって生起し、ダウン状態からアップ状態に移行することによって生起することはない。ところが危害はシステム要素がアップ状態のまま、あるいはシステム要素がダウン状態からアップ状態に移行することによって生起し得る。従って、危害生起を頂上事象とする FT は、システム要素のダウン状態だけでなくアップ状態にも着目し事象を展開する必要がある^{99)~103)}。この課題に対して、本章はまず S-A プロセスチャートで表される状態変化および遷移作用と FT の事象とが関連付けられた優先 AND 構造を持つ S-A-FT (S-A-process-chart-based FT) を定義する。次に、多状態を持つシステム要素を含む修理系 2 冗長電源システムを離散事象システムでモデル化し、当該システムの故障に至るプロセスを S-A プロセスチャートで洗い出す。さらに得られた S-A プロセスチャートを S-A-FT で展開することによって、合理的に次の (a) ~ (d) の分析が可能となることを示す。

- (a) 多状態を持つシステム要素を含むシステムのハザードを S-A-FT で展開する。
- (b) S-A-FT から求めた事象生起順序付きプライムインプリカント (O-PrIm: Ordered Prime-Implicant) (1.5 節 (27) 参照) を構成する遷移作用を特定する。
- (c) S-A-FT から事象生起順序依存型ハザードを基本事象のレベルで識別する。
- (d) 相反事象および/または排他事象を有する事象生起順序付きプライムインプリカントを導出する。

6.2 S-A-FT の構造

本節では、S-A プロセスチャートに基づく S-A-FT の構造的特徴について説明する

6.2.1 S-A プロセスチャートと S-A-FT との関係

遷移作用 $A_{i,j} (k,k')$ は、システム要素 $X_{i,j,k}$ を $X_{i,j,k'}$ に遷移させる働きであり、システム内部または外部の要素の変化すなわち事象に伴って生起する。システム状態の別の状態への変化もまた事象である。図 6-1 は、S-A プロセスチャートにおける遷移作用、事象およびシステム状態¹⁹⁾ の関係を、タイムチャートを用い示している。すなわち、

- ① 時刻 t_1 において事象 E1.1 に伴う遷移作用 $A_{1,1} (0,1)$ が生起し、時刻 t_2 においてシステム状態が $S_1 \{X_{1,1,0}, X_{1,2,0}\}$ から $S_2 \{X_{1,1,1}, X_{1,2,0}\}$ に遷移する（事象 $S_1 \rightarrow S_2$ ）。
- ② 時刻 t_3 において事象 E1.2 に伴う遷移作用 $A_{1,2} (0,1)$ が生起し、時刻 t_4 においてシステム状態が $S_2 \{X_{1,1,1}, X_{1,2,0}\}$ から最終状態 $S_3 \{X_{1,1,1}, X_{1,2,1}\}$ に遷移する（事象 $S_2 \rightarrow S_3$ ）。

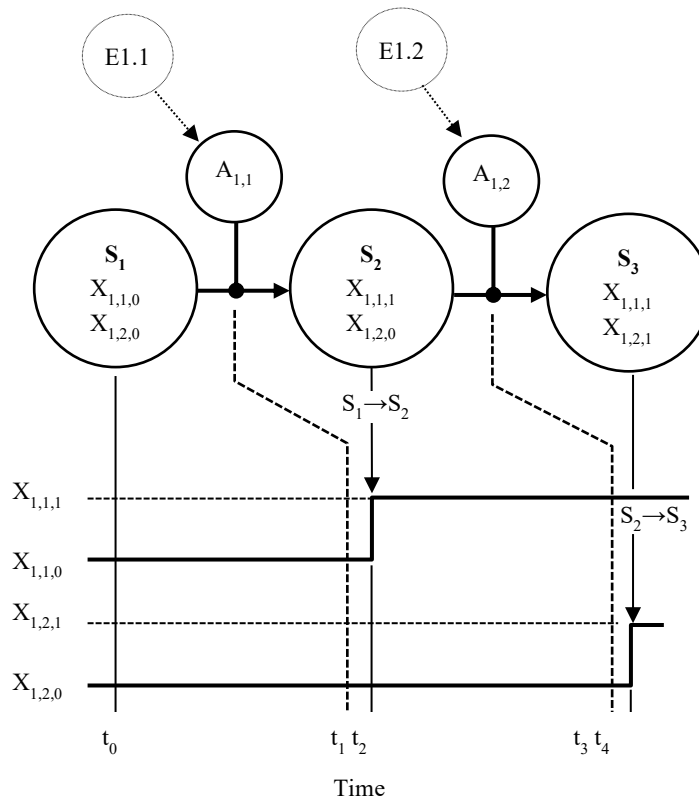
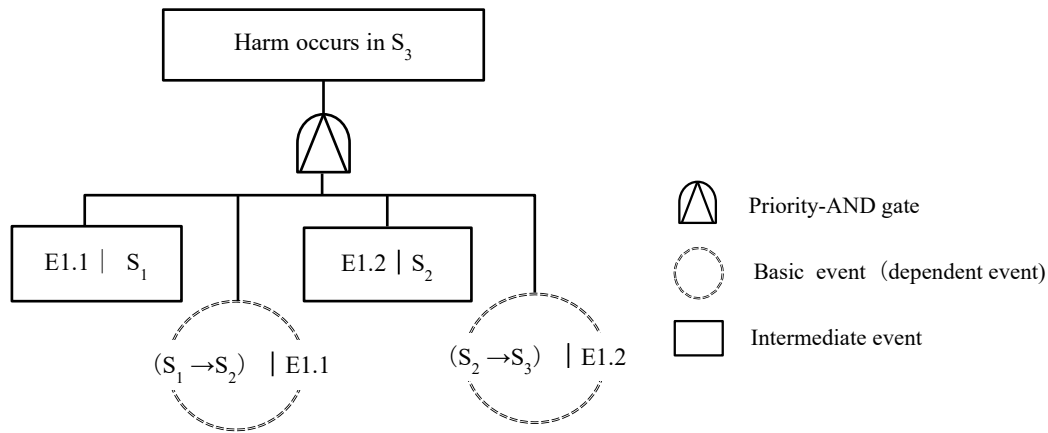


図 6-1 タイムチャートによる遷移作用と事象との関係

図 6-1 と等価な FT は、優先 AND ゲートを用い、図 6-2 のように表される。



$E1.1 \mid S_1$: Independent event E1.1 has occurred in state S_1 .

$(S_1 \rightarrow S_2) \mid E1.1$: Dependent event $(S_1 \rightarrow S_2)$ has occurred under E1.1 had occurred.

$E1.2 \mid S_2$: Independent event E1.2 has occurred in state S_2 .

$S_2 \rightarrow S_3 \mid E1.2$: Dependent event $(S_2 \rightarrow S_3)$ occurs under E1.2 has occurred.

図 6-2 図 6-1 と等価な S-A-FT

$(S_1 \rightarrow S_2)$ は S_1 の条件下で E1.1 の生起後、時間遅れ $(t_2 - t_1)$ をもって必ず生起する事象である。すなわち $(S_1 \rightarrow S_2)$ は E1.1 の従属事象である。 $(S_2 \rightarrow S_3)$ は S_2 の条件下で E1.2 の発生後、時間遅れ $(t_4 - t_3)$ をもって必ず生起する事象である。すなわち $(S_2 \rightarrow S_3)$ は E1.2 の従属事象である。 $(t_2 - t_1)$ または $(t_4 - t_3)$ が短く無視できる場合、図 6-2 の従属事象 $(S_1 \rightarrow S_2)$ または $(S_2 \rightarrow S_3)$ は省略が可能である。しかしそれらの時間幅が別の事象（他の機器の故障、修復等）の割り込み、あるいは危害の発生率の定量的解析結果等に関連して無視できない場合、従属事象は省略できない。

6.2.2 S-A-FT の階層構造

S-A-FT の例を図 6-3 に示す。S-A プロセスチャートが決まれば S-A-FT の最終状態、最終事象、初期状態、第 1 階層入力事象群が決まる。第 1 階層入力事象群はすべて優先 AND ゲートで結合した構造となる。また第 2 階層入力事象以下の入力事象群を従来の FT と同様に展開することによって、部品の故障等システム要素レベルでの分析が可能となる。2.3 節に示すが、S-A-FT では、事象生起順序を考慮した 2 状態以上の多状態システムを対象とした O-PrIm を導出しなければならない。O-PrIm には、相反基本事象および/または排他基本事象が含まれる場合がある。

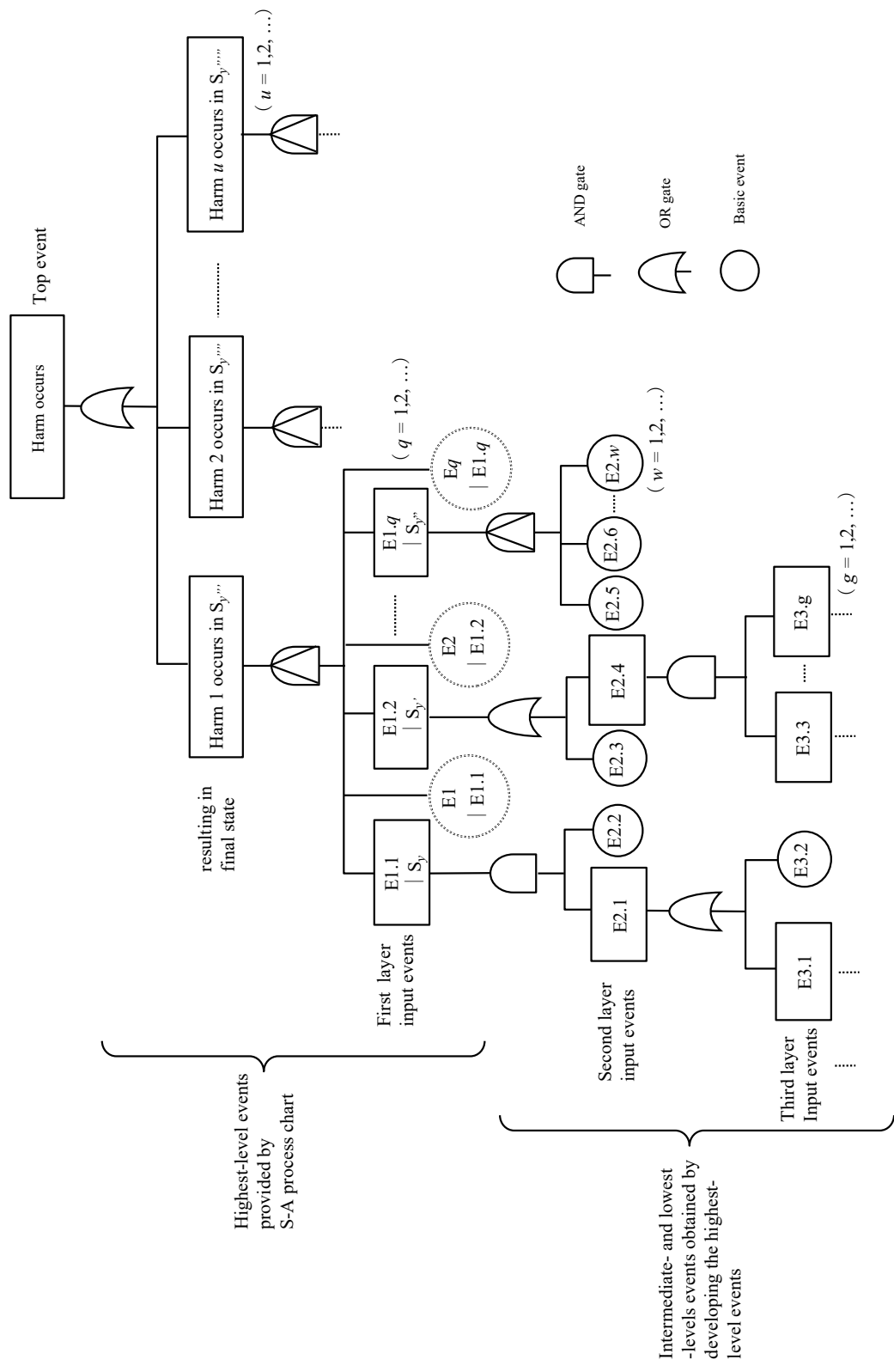


図 6-3 S-A-FT の階層構造

6.2.3 順序依存 O-PrIm 群

図 6-4 は文献^{48), 104), 105)}における事象生起順序依存型故障論理を表している。出力事象が入力事象の生起順序に影響を受ける場合、出力事象は優先 AND ゲートの各入力事象が順番に $E_1, E_2 \dots E_c$ と生起し、結果的にすべての入力事象が生起しているときにのみ真となるものと定義している。一方、6.2.4 項に示すが、システムの状態遷移プロセスモデルに基づく S-A-FT において、出力事象は、すべての入力事象が生起しつづけることを前提としない。

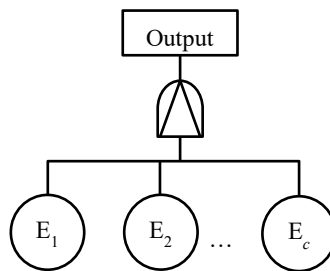


図 6-4 事象生起順序依存型故障論理

本論文は事象生起順序依存性を次のように定義する。 c 個の重複しない基本事象 E_d ($d = 1, 2, \dots, c$) から成る O-PrIm は、最大で $c!$ 通りの事象生起順序を持つ。 $c!$ 通りのうち r ($r < c!$) 通りの事象生起順序においてのみ頂上事象が生起する場合、基本事象 E_d ($d = 1, 2, \dots, c$) は順序依存 O-PrIm 群 (Sequential O-PrIm group) を構成する。 $r = c!$ の場合、 E_d ($d = 1, 2, \dots, c$) は順序依存 O-PrIm 群を構成しない。

6.2.4 相反/排他事象を含む O-PrIm

S-A-FT は相反事象および/または排他事象を伴ってシステム要素がアップ状態のまま、あるいはシステム要素がダウン状態からアップ状態に移行することによって頂上事象が生起し得る。例えば空気中の可燃性ガスをシステム要素とした場合、その属性であるガス濃度は、

- S₁: 爆発下限界以下
- S₂: 爆発範囲 (爆発性雰囲気)
- S₃: 爆発上限界以上

の 3 個の状態を持つ。図 6-5 は換気システムを装備した溶剤乾燥器のガス爆発を頂上事象

とする S-A-FT である。頂上事象は、以下の事象生起順序で生起する。

- ① S₁の条件下で、“E1.1換気システム故障停止”が生起する。
- ② E1.1によってS₁がS₂に遷移する。
- ③ S₂の条件下で“ $\overline{E1.2}$ 着火エネルギー非生起”が生起する。
- ④ $\overline{E1.2}$ によって、S₂がS₃に遷移する。
- ⑤ S₃の条件下で“E1.2 着火エネルギー生起”が生起する。
- ⑥ E1.2によって、S₃がS₃'（着火エネルギーを伴うS₃）に遷移する。
- ⑦ S₃'の条件下で“E1.3換気システム修復”が生起する。
- ⑧ E1.3によってS₃'がS₂'（着火エネルギーを伴うS₂）に遷移する。
- ⑨ S₂'において、ガス爆発が発生する。

ここで、E1.1 と E1.3 とは相反事象であり、E1.2 と $\overline{E1.2}$ とは排他事象である。S-A-FT では、相反事象および/または排他事象を論理的矛盾なく展開することが可能である。以上に示した様に、S-A-FT は、例えばシステム要素の温度、圧力、濃度または速度等の状態を高～中～低、システム要素状態を正常～固着～誤動作～断線等の可逆遷移を行う多状態でモデル化し、状態を変化させる基本事象を順序付けて展開することを前提とする。これらの前提条件はコヒーレントシステムの前提条件の枠外である。

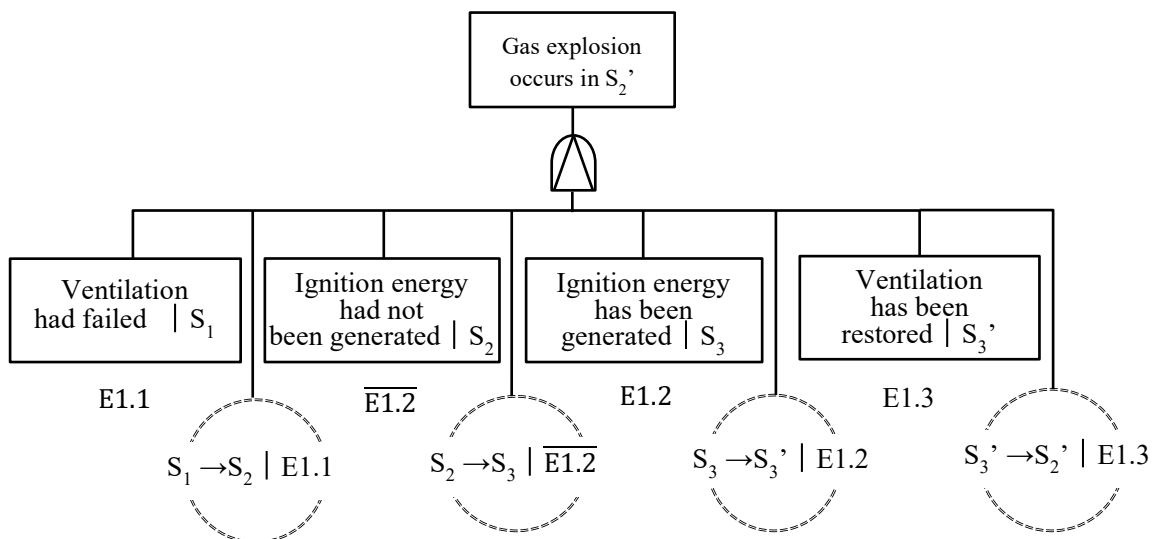


図 6-5 ガス爆発の S-A-FT

6.3 事例 “電源システム故障” の分析

例えば多くの医療用機器では、電源が失われると危害が起こり得る。本節では、電源システムの故障状態（フォールト（Fault）：故障による電力供給不能状態）を危害と想定し、**図 6-6** の修理系 2 冗長電源システムの故障に至るプロセスを S-A プロセスチャートで同定し S-A-FT で展開する。

6.3.1 S-A プロセスチャートの導出（電源システム故障）

(1) システムの基本動作

この電源システムは、次の条件に従って動作すると仮定しても不自然ではない。

- (a) この電源システムは、システム要素である主電源 (X_1)、予備電源 (X_2) および切替えスイッチ (X_3) から構成され、それぞれの要素は故障後に事後保全（修理）が実施される。
- (b) 事後保全はシステムを停止せずに行う。
- (c) X_1 , X_2 , X_3 は、故障に関して十分な独立性を有し共通原因故障が無視でき、システム要素群の故障および修理が同時に発生する確率は無視できる。
- (d) X_1 または X_2 から電力を供給できれば、電源システムはアップ状態（電力供給可能状態）を維持する。
- (e) アップ状態（接点切替え可能状態）にある X_3 は、 X_1 が故障すると瞬時に接点を a から b に切替え、また X_1 がアップ状態に戻ると瞬時に接点を b から a に切替える。
- (f) X_3 の故障モードは接点 a または b に固着、a から b または b から a に誤動作、並びに接点不良等により a および b に非接続となる断線がある。ただし、これらの故障は X_3 が正常の時のみ生ずる。

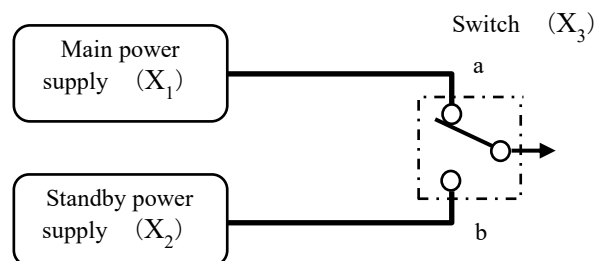


図 6-6 修理系 2 冗長電源システム

(2) システム要素の状態定義

$X_{i,j,k}$ (システム要素 i が持つ属性 j の状態 k) を表 6-1 のとおり設定する。

表 6-1 システム要素の状態定義

$X_{i,j,k}$	Components i	Attribute j	State variable k
$X_{1,1,0}$	1: Main power supply	1: Power supply function	0: Up state
$X_{1,1,1}$			1: Fault
$X_{2,1,0}$	2: Standby power supply	1: Power supply function	0: Up state
$X_{2,1,1}$			1: Fault
$X_{3,1,0a}$	3: Switch	1: Switching function	0a: Up state connecting with the a-point
$X_{3,1,0b}$			0b: Up state connecting with the b-point
$X_{3,1,1a}$			1a: Fault connecting with the a-point
$X_{3,1,1b}$			1b: Fault connecting with the b-point
$X_{3,1,1c}$			1c: Fault disconnecting with any points

(3) 状態遷移プロセスモデル

図 6-6 のシステム要素 X_1 , X_2 および X_3 の状態遷移と遷移作用との関係 (a) ~ (g) を図 6-7 に図式化する。

- (a) X_1 はそれぞれ可逆遷移を行う 2 状態 $X_{1,1,0}$ および $X_{1,1,1}$ を持つ。また、それぞれ独立した 2 個の遷移作用 $A_{1,1}$ (0,1) および $A_{1,1}$ (1,0) を持つ。
- (b) X_2 はそれぞれ可逆遷移を行う 2 状態 $X_{2,1,0}$ および $X_{2,1,1}$ を持つ。また、それぞれ独立した 2 個の遷移作用 $A_{2,1}$ (0,1) および $A_{2,1}$ (1,0) を持つ。
- (c) X_3 の状態 $X_{3,1,0a}$ は、 X_1 の状態 $X_{1,1,0}$ において $A_{1,1}$ (0,1) によって $X_{3,1,0b}$ に、固着の $A_{3,1}$ (0a,1a) によって $X_{3,1,1a}$ に、誤動作の $A_{3,1}$ (0a,1b) によって $X_{3,1,1b}$ に、または断線 (どの接点にも接続しないことをいう、表 6-1 参照) の $A_{3,1}$ (0a,1c) によって $X_{3,1,1c}$ に遷移する。
- (d) X_3 の状態 $X_{3,1,0b}$ は、 X_1 の状態 $X_{1,1,1}$ において修復の遷移作用 $A_{1,1}$ (1,0) によって $X_{3,1,0a}$ に、固着の $A_{3,1}$ (0b,1b) によって $X_{3,1,1b}$ に、誤動作の $A_{3,1}$ (0b,1a) によって $X_{3,1,1a}$ に、または断線の $A_{3,1}$ (0b,1c) によって $X_{3,1,1c}$ に遷移する。

- (e) X_3 の状態 $X_{3,1,1a}$ は、 X_1 の状態 $X_{1,1,0}$ において修復の $A_{3,1}$ ($1a,0a$) によって $X_{3,1,0a}$ に、または X_1 の状態 $X_{1,1,1}$ において修復の $A_{3,1}$ ($1a,0b$) によって $X_{3,1,0b}$ に遷移する。
- (f) X_3 の状態 $X_{3,1,1b}$ は、 X_1 の状態 $X_{1,1,1}$ において修復の $A_{3,1}$ ($1b,0b$) によって $X_{3,1,0b}$ に、または X_1 の状態 $X_{1,1,0}$ において修復の $A_{3,1}$ ($1b,0a$) によって $X_{3,1,0a}$ に遷移する。
- (g) X_3 の状態 $X_{3,1,1c}$ は、 X_1 の状態 $X_{1,1,1}$ において修復の $A_{3,1}$ ($1c,0b$) によって $X_{3,1,0b}$ に、または X_1 の状態 $X_{1,1,0}$ において修復の $A_{3,1}$ ($1c,0a$) によって $X_{3,1,0a}$ に遷移する。

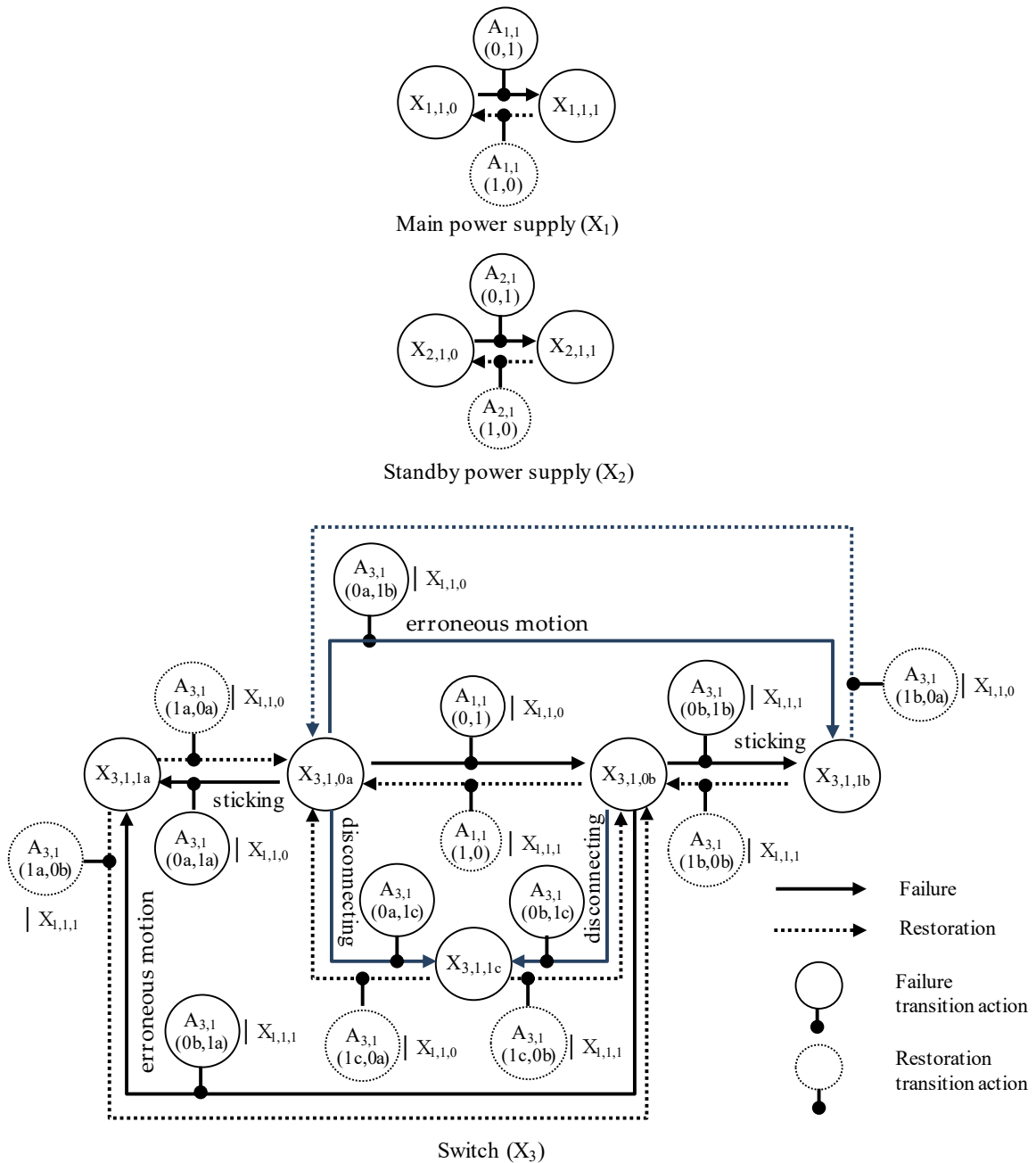


図 6-7 システム要素の状態遷移プロセスモデル

(4) $A_{ij}(k, k')$ を生起させる $E_{ij}(k, k')$ の設定

本事例では図 6-7 に示す遷移作用 $A_{ij}(k, k')$ に対して、遷移作用を生起させる事象 $E_{ij}(k, k')$ を表 6-2 のとおり対応させる。(1) の (c) より、中間事象 $E_{ij}(k, k')$ を生起させる代表的な基本事象の組合せを $E_{ij}(k, k')$ と同じ記号で表したとして以下の分析を行う。

表 6-2 各遷移作用を生起させる事象

Transition action $A_{i, j}(k, k')$		Event $E_{i, j}(k, k')$ that causes $A_{i, j}(k, k')$	
$A_{1,1}(0,1)$	The action that changes $X_{1,1,0}$ to $X_{1,1,1}$ The action that changes $X_{3,1,0a}$ to $X_{3,1,0b}$	$E_{1,1}(0,1)$	Main power supply fails.
$A_{1,1}(1,0)$	The action that changes $X_{1,1,1}$ to $X_{1,1,0}$ The action that changes $X_{3,1,0b}$ to $X_{3,1,0a}$	$E_{1,1}(1,0)$	Main power supply is restored.
$A_{2,1}(0,1)$	The action that changes $X_{2,1,0}$ to $X_{2,1,1}$	$E_{2,1}(0,1)$	standby power supply fails.
$A_{2,1}(1,0)$	The action that changes $X_{2,1,1}$ to $X_{2,1,0}$	$E_{2,1}(1,0)$	Standby power supply is restored.
$A_{3,1}(0a,1b)$	The action that changes $X_{3,1,0a}$ to $X_{3,1,1b}$ under $X_{1,1,0}$	$E_{3,1}(0a,1b)$	Contact changes to b-point from a-point due to an erroneous motion.
$A_{3,1}(1b,0a)$	The action that changes $X_{3,1,1b}$ to $X_{3,1,0a}$ under $X_{1,1,0}$	$E_{3,1}(1b,0a)$	Contact changes to a-point from b-point due to restoration of switch correctly.
$A_{3,1}(0b,1a)$	The action that changes $X_{3,1,0b}$ to $X_{3,1,1a}$ under $X_{1,1,1}$	$E_{3,1}(0b,1a)$	Contact changes to a-point from b-point due to an erroneous motion.
$A_{3,1}(1a,0b)$	The action that changes $X_{3,1,1a}$ to $X_{3,1,0b}$ under $X_{1,1,1}$	$E_{3,1}(1a,0b)$	Contact changes to b-point from a-point due to restoration of switch correctly.
$A_{3,1}(0a,1c)$	The action that changes $X_{3,1,0a}$ to $X_{3,1,1c}$ under $X_{1,1,0}$	$E_{3,1}(0a,1c)$	Contact changes to disconnection status from a-point due to failure.
$A_{3,1}(1c,0a)$	The action that changes $X_{3,1,1c}$ to $X_{3,1,0a}$ under $X_{1,1,0}$	$E_{3,1}(1c,0a)$	The disconnection status changes to the a-point connection due to restoration of switch correctly.
$A_{3,1}(0b,1c)$	The action that changes $X_{3,1,0b}$ to $X_{3,1,1c}$ under $X_{1,1,1}$	$E_{3,1}(0b,1c)$	Contact changes to disconnection status from b-point due to failure.
$A_{3,1}(1c,0b)$	The action that changes $X_{3,1,1c}$ to $X_{3,1,0b}$ under $X_{1,1,1}$	$E_{3,1}(1c,0b)$	The disconnection status changes to the b-point connection due to restoration of switch correctly.
$A_{3,1}(0a,1a)$	The action that changes $X_{3,1,0a}$ to $X_{3,1,1a}$ under $X_{1,1,0}$	$E_{3,1}(0a,1a)$	Contact sticks at the a-point due to failure.
$A_{3,1}(1a,0a)$	The action that changes $X_{3,1,1a}$ to $X_{3,1,0a}$ under $X_{1,1,0}$	$E_{3,1}(1a,0a)$	Contact changes to a normal state at the a-point due to restoration.
$A_{3,1}(0b,1b)$	The action that changes $X_{3,1,0b}$ to $X_{3,1,1b}$ under $X_{1,1,1}$	$E_{3,1}(0b,1b)$	Contact sticks at the b-point due to failure.
$A_{3,1}(1b,0b)$	The action that changes $X_{3,1,1b}$ to $X_{3,1,0b}$ under $X_{1,1,1}$	$E_{3,1}(1b,0b)$	Contact changes to a normal state at the b-point due to restoration.

(5) システム状態-遷移作用-出力事象の関係

各システム要素状態 $X_{i,j,k}$ を組合せることより 20 個のシステム状態 S_y が定義可能である。しかし、6.3.1 項 (1) の (e) より、① $X_{3,1,0a}$ ならば $X_{1,1,0}$ 、② $X_{3,1,0b}$ ならば $X_{1,1,1}$ でなければならず、 $\{X_{1,1,1}, X_{2,1,0}, X_{3,1,0a}\}$ 、 $\{X_{1,1,1}, X_{2,1,1}, X_{3,1,0a}\}$ 、 $\{X_{1,1,0}, X_{2,1,0}, X_{3,1,0b}\}$ および $\{X_{1,1,0}, X_{2,1,1}, X_{3,1,0b}\}$ は、①又②を満足せず生起し得ない状態群である。これらの状態群を除外すると、生起し得るシステム状態は 16 個である。また“ τ_1 ”は出力事象“電源システム故障”を意味する。システム状態 $S_4, S_6, S_8, S_{11} \sim S_{16}$ がシステム故障状態であることは自明である。

表 6-3 システム要素の状態遷移プロセスモデル (図 6-7) に基づくシステム状態遷移表

System state	Transition action	$A_{1,1}$ (0,1)	$A_{1,1}$ (1,0)	$A_{2,1}$ (0,1)	$A_{2,1}$ (1,0)	$A_{3,1}$ (0a,1b)	$A_{3,1}$ (1b,0a)	$A_{3,1}$ (0b,1a)	$A_{3,1}$ (1a,0b)	$A_{3,1}$ (0a,1c)	$A_{3,1}$ (1c,0a)	$A_{3,1}$ (0b,1c)	$A_{3,1}$ (1c,0b)	$A_{3,1}$ (0a,1a)	$A_{3,1}$ (1a,0a)	$A_{3,1}$ (0b,1b)	$A_{3,1}$ (1b,0b)
$S_1 = \{X_{1,1,0}, X_{2,1,0}, X_{3,1,0a}\}$		S_5	n_t	S_9	n_t	S_3	n_t	n_t	n_t	S_4/τ_1	n_t	n_t	n_t	S_2	n_t	n_t	n_t
$S_2 = \{X_{1,1,0}, X_{2,1,0}, X_{3,1,1a}\}$		S_6/τ_1	n_t	S_{10}	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	S_1	n_t	n_t
$S_3 = \{X_{1,1,0}, X_{2,1,0}, X_{3,1,1b}\}$		S_7	n_t	S_{11}/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t
$S_4 = \{X_{1,1,0}, X_{2,1,0}, X_{3,1,1c}\}$		S_8/τ_1	n_t	S_{12}/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	S_1	n_t	n_t	n_t	n_t	n_t	n_t
$S_5 = \{X_{1,1,1}, X_{2,1,0}, X_{3,1,0b}\}$		n_t	S_1	S_{13}/τ_1	n_t	n_t	n_t	S_6/τ_1	n_t	n_t	n_t	S_8/τ_1	n_t	n_t	n_t	S_7	n_t
$S_6 = \{X_{1,1,1}, X_{2,1,0}, X_{3,1,1a}\}$		n_t	S_2	S_{14}/τ_1	n_t	n_t	n_t	n_t	S_5	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t
$S_7 = \{X_{1,1,1}, X_{2,1,0}, X_{3,1,1b}\}$		n_t	S_3	S_{15}/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	S_5
$S_8 = \{X_{1,1,1}, X_{2,1,0}, X_{3,1,1c}\}$		n_t	S_4/τ_1	S_{16}/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	S_5	n_t	n_t	n_t	n_t
$S_9 = \{X_{1,1,0}, X_{2,1,1}, X_{3,1,0a}\}$		S_{13}/τ_1	n_t	n_t	S_1	S_{11}/τ_1	n_t	n_t	n_t	S_{12}/τ_1	n_t	n_t	n_t	S_{10}	n_t	n_t	n_t
$S_{10} = \{X_{1,1,0}, X_{2,1,1}, X_{3,1,1a}\}$		S_{14}/τ_1	n_t	n_t	S_2	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t
$S_{11} = \{X_{1,1,0}, X_{2,1,1}, X_{3,1,1b}\}$		S_{15}/τ_1	n_t	n_t	S_3	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t
$S_{12} = \{X_{1,1,0}, X_{2,1,1}, X_{3,1,1c}\}$		S_{16}/τ_1	n_t	n_t	S_4/τ_1	n_t	n_t	n_t	n_t	n_t	S_6	n_t	n_t	n_t	n_t	n_t	n_t
$S_{13} = \{X_{1,1,1}, X_{2,1,1}, X_{3,1,0b}\}$		n_t	S_9	n_t	S_5	n_t	n_t	S_{14}/τ_1	n_t	n_t	n_t	S_{16}/τ_1	n_t	n_t	n_t	S_{15}/τ_1	n_t
$S_{14} = \{X_{1,1,1}, X_{2,1,1}, X_{3,1,1a}\}$		n_t	S_{10}	n_t	S_6/τ_1	n_t	n_t	n_t	S_{13}/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t
$S_{15} = \{X_{1,1,1}, X_{2,1,1}, X_{3,1,1b}\}$		n_t	S_{11}/τ_1	n_t	S_7	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	n_t	S_{13}/τ_1
$S_{16} = \{X_{1,1,1}, X_{2,1,1}, X_{3,1,1c}\}$		n_t	S_{12}/τ_1	n_t	S_8/τ_1	n_t	n_t	n_t	n_t	n_t	n_t	n_t	S_{13}/τ_1	n_t	n_t	n_t	n_t

τ_1 : システムダウン, n_t : 遷移先なし

(6) S-A プロセスチャートの洗い出し

表 6-3 を図式化し図 6-8 の状態遷移経路図に示す。図 6-8 は、システムの各定義状態が持つ遷移可能なすべての遷移先と $A_{i,j}(k,k')$ との組合せを示す。

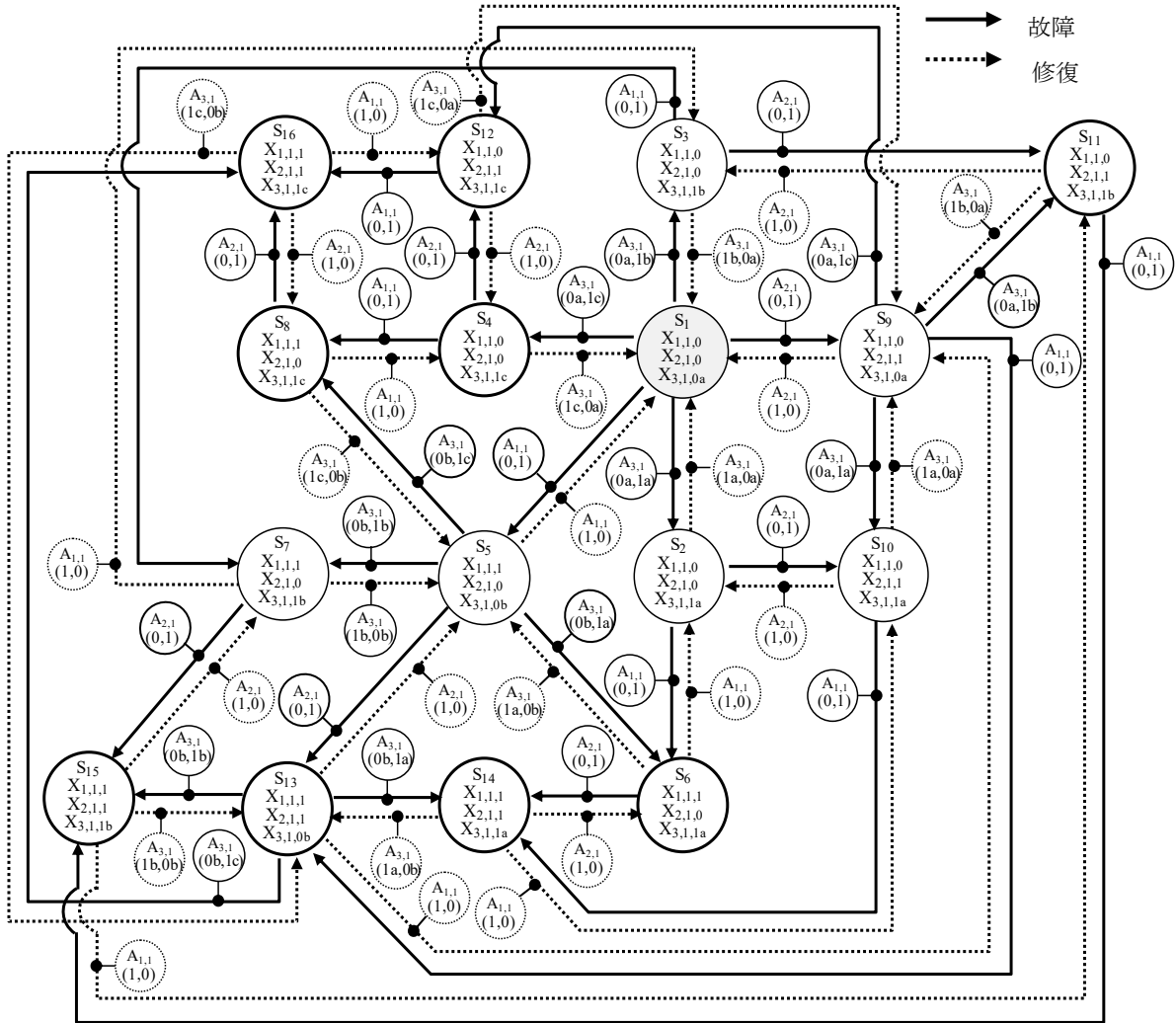


図 6-8 表 6-3 から求めた状態遷移経路図

図中の実線はシステム要素の故障状態への遷移，点線はアップ状態への遷移である。ある S_y から $S_{y'}$ に至る状態遷移経路は，図 6-8 の矢線をたどることによって網羅的に洗い出すことができる。ただし，可逆遷移によって状態間を無制限に往復する経路を回避し，また作用し得る全ての遷移作用の組み合わせを洗い出すために，図 6-8 に対して 3.7.4 項と同じ導出条件 $C_{r1} \sim C_{r7}$ を適用する。ただし，初期状態 $S_{ys} = S_1$ ，最終状態 $S_{ye} = \{S_4, S_6, S_8, S_{11}, S_{12}, S_{13}, S_{14}, S_{15}, S_{16}\}$ とする。

初期状態 S_1 から最終状態 S_{11} に至る状態遷移経路は、図 6-9 の S-A プロセスチャートのとおり表される。

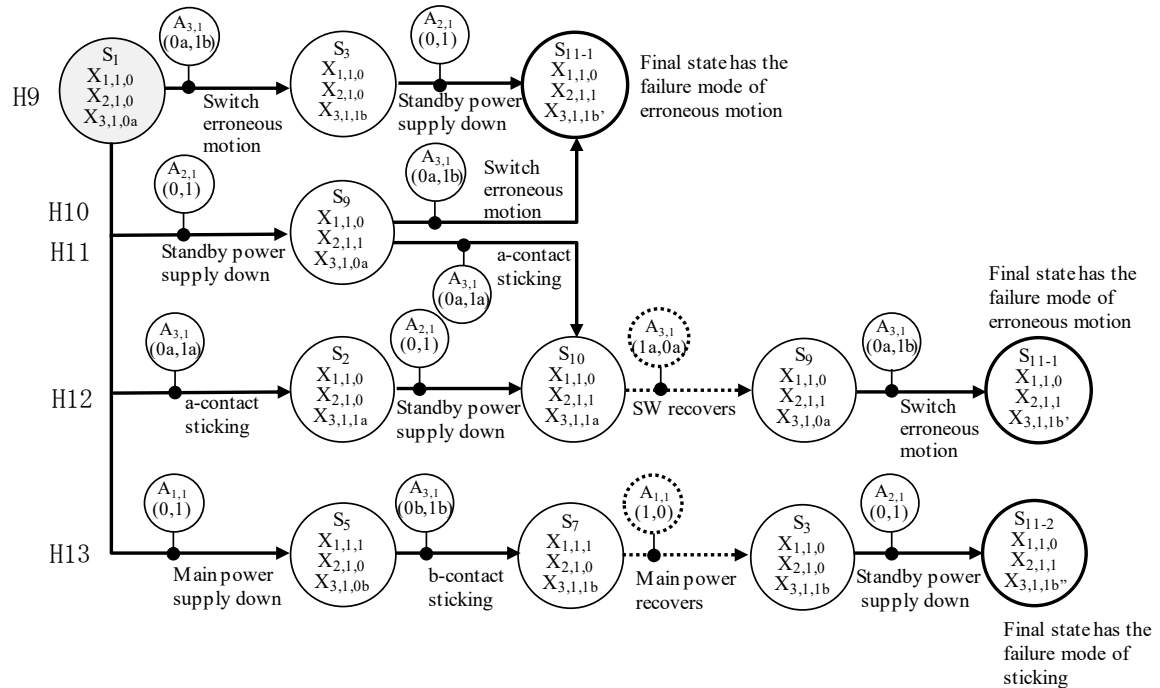


図 6-9 図 6-8 で分類された最終状態 S_{11-1} および S_{11-2} の S-A プロセスチャート

最終状態の形態は同じでも異なる故障（失敗）モードを持つ場合、最終状態は区別する必要がある。例えば、 S_{11} の $X_{3,1,1b}$ は誤動作起因の $X_{3,1,1b'}$ と固着起因の $X_{3,1,1b''}$ を持つ。従って図 6-9 は、 S_{11} を S_{11-1} と S_{11-2} とに区別して示している。

6.3.2 S-A-FT の展開とその分析

(1) S-A-FT の導出

6.2.1 項で示した S-A プロセスチャートと S-A-FT との関係に基づき図 6-9 を S-A-FT に展開し図 6-10 に示す。ただし、独立事象生起後、従属事象（システム状態の変化）は瞬時に行われるものとして省略する。また、2 重丸の事象は修復を意味する。

S_{11-1} は O-Im; C₉ ~ C₁₂, S_{11-2} は C₁₃ によって生起する。O-Im; C₉ ~ C₁₃ を西らの研究⁹⁹⁾ による表記形式に準じて式 (1) に示す。

$$\begin{aligned}
C_9 &= \{(E_{3,1}(0a,1b) \mid S_1) \rightarrow (E_{2,1}(0,1) \mid S_3)\} \\
C_{10} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0a,1b) \mid S_9)\} \\
C_{11} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0a,1a) \mid S_9) \rightarrow (E_{3,1}(1a,0a) \mid S_{10}) \rightarrow (E_{3,1}(0a,1b) \mid S_9)\} \\
C_{12} &= \{(E_{3,1}(0a,1a) \mid S_1) \rightarrow (E_{2,1}(0,1) \mid S_2) \rightarrow (E_{3,1}(1a,0a) \mid S_{10}) \rightarrow (E_{3,1}(0a,1b) \mid S_9)\} \\
C_{13} &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0b,1b) \mid S_5) \rightarrow (E_{1,1}(1,0) \mid S_7) \rightarrow (E_{2,1}(0,1) \mid S_3)\}
\end{aligned}
\tag{1}$$

同様に、各最終状態 S_4 , S_{6-1} , S_{6-2} , S_8 , S_{12} , S_{13} , S_{14} , S_{15-1} , S_{15-2} を生起させる O-Im; C_w ($w = 1 \sim 26$) を導出し図 6-11 の S-A-FT に示す。最終状態 S_8 , S_{12} または S_{13} を経由して生起する S_{16} は、3.7.4 項の制約条件 Cr4 より除外される。

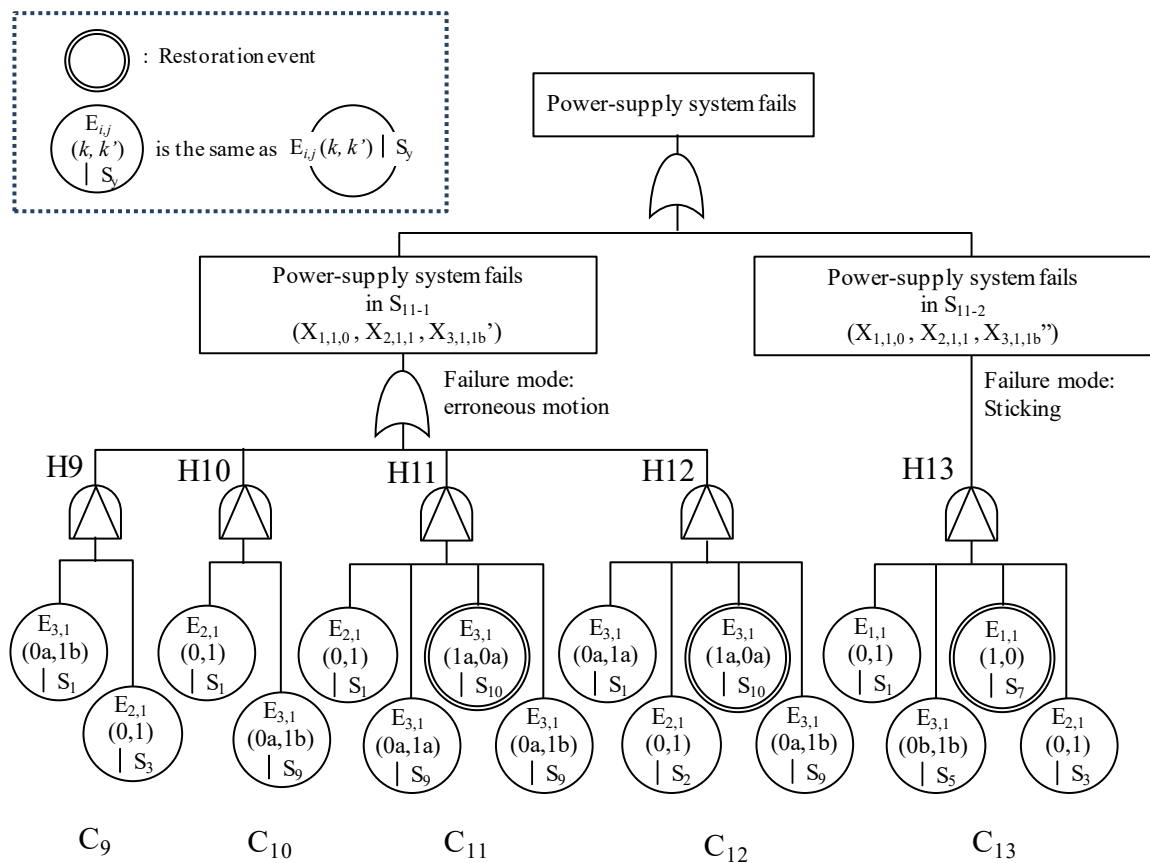


図 6-10 S_{11-1} および S_{11-2} の S-A プロセスチャート (図 6-9) の S-A-FT

(2) O-PrIm の導出

図 6-11 の C_W から最終状態の生起に関して省略できる基本事象を含む C_W' を除外する。例えば, S_{11-1} を生起させる C_{11} , C_{12} は省略可能な $E_{3,1}(0a,1a)$ および $E_{3,1}(1a,0a)$ を含む C_W' である。同様の方法でその他の C_W' を洗い出し除外することによって, 式 (2) の O-PrIm 群の導出が可能である。

$$\begin{aligned}
 C_1 &= \{(E_{3,1}(0a,1c) \mid S_1)\} \\
 C_2 &= \{(E_{3,1}(0a,1a) \mid S_1) \rightarrow (E_{1,1}(0,1) \mid S_2)\} \\
 C_4 &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0b,1a) \mid S_5)\} \\
 C_7 &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0b,1c) \mid S_5)\} \\
 C_9 &= \{(E_{3,1}(0a,1b) \mid S_1) \rightarrow (E_{2,1}(0,1) \mid S_3)\} \\
 C_{10} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0a,1b) \mid S_9)\} \\
 C_{13} &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0b,1b) \mid S_5) \rightarrow (E_{1,1}(1,0) \mid S_7) \rightarrow (E_{2,1}(0,1) \mid S_3)\} \\
 C_{14} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0a,1c) \mid S_9)\} \\
 C_{17} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{1,1}(0,1) \mid S_9)\} \\
 C_{18} &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{2,1}(0,1) \mid S_5)\} \\
 C_{22} &= \{(E_{3,1}(0a,1a) \mid S_1) \rightarrow (E_{2,1}(0,1) \mid S_2) \rightarrow (E_{1,1}(0,1) \mid S_{10})\} \\
 C_{23} &= \{(E_{2,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0a,1a) \mid S_9) \rightarrow (E_{1,1}(0,1) \mid S_{10})\} \\
 C_{24} &= \{(E_{1,1}(0,1) \mid S_1) \rightarrow (E_{3,1}(0b,1b) \mid S_5) \rightarrow (E_{2,1}(0,1) \mid S_7)\} \\
 C_{26} &= \{(E_{3,1}(0a,1b) \mid S_1) \rightarrow (E_{1,1}(0,1) \mid S_3) \rightarrow (E_{2,1}(0,1) \mid S_7)\}
 \end{aligned}
 \tag{2}$$

図 6-11 の S-A-FT では, O-PrIm は故障 (失敗) モード別に分類された各最終状態に至る最短経路を構成する基本事象の組み合わせとしても導出可能である。

(3) 順序依存 O-PrIm 群の導出

O-PrIm 群 (2) において, 基本事象 $E_{3,1}(0a,1b)$ および $E_{2,1}(0,1)$ から成る O-PrIm 群は, 最大で 2 通り ($2! = 2$) の O-PrIm を持ち得るが, 実際にも 2 通りの O-PrIm すなわち C_9 および C_{10} を有しているので, 順序依存 O-PrIm 群ではない。同様に, 1 個の基本事象 $E_{3,1}(0a,1c)$ から成る C_1 , および $E_{2,1}(0,1)$, $(E_{1,1}(0,1))$ から成る C_{17} および C_{18} は, 順序依存 O-PrIm 群ではない。

基本事象 $E_{3,1}(0a,1a)$ および $E_{1,1}(0,1)$ から成る O-PrIm 群は, 最大で 2 通り ($2! = 2$) の O-PrIm を持ち得るが, 実際には 1 通りの O-PrIm すなわち C_2 のみであり, 順序依存 O-PrIm 群である。同様に, $E_{1,1}(0,1)$ および $E_{3,1}(0b,1a)$ から成る C_4 , $E_{1,1}(0,1)$ および $E_{3,1}(0b,1c)$ から成る C_7 , $E_{2,1}(0,1)$ および $E_{3,1}(0a,1c)$ から成る C_{14} , $E_{3,1}(0a,1a)$, $E_{2,1}(0,1)$, $E_{1,1}(0,1)$ から成る C_{22} および C_{23} , $E_{1,1}(0,1)$, $E_{3,1}(0b,1b)$ および $E_{2,1}(0,1)$ から成る

C_{24} , $E_{3,1}$ (0a,1b) , $E_{1,1}$ (0,1) および $E_{2,1}$ (0,1) から成る C_{26} は, 順序依存 O-PrIm 群である。また, $E_{1,1}$ (0,1) , $E_{3,1}$ (0b,1b) , $E_{1,1}$ (1,0) および $E_{2,1}$ (0,1) から成る C_{13} は, 相反事象 $E_{1,1}$ (0,1) および $E_{1,1}$ (1,0) を持つ順序依存 O-PrIm 群である。

6.4 第6章のまとめ

S-A プロセスチャートはシステムレベルの事象および状態の生起順序, タイミング等に依存して発現するハザードの同定・分析に適しているが, 部品の故障等のシステム要素レベルでの分析に適していない。FTA は頂上事象からシステムの要素レベルまでの分析が可能であるが, 一般的 (コヒーレント) FT では, システム要素の多状態およびその遷移順序に起因してシステム要素がダウン状態からアップ状態に移行することによって生起するハザードを系統的に展開することは困難である。この課題に対して本章は, まず S-A プロセスチャートのシステム状態および遷移作用と FT の事象とが関連付けられた S-A-FT を定義した。次に, 多状態を持つシステム要素を含む修理系 2 冗長電源システムを離散事象システムでモデル化し, 当該システムの故障に至るプロセスを S-A プロセスチャートで洗い出した。さらに得られた S-A プロセスチャートを S-A-FT で展開することによって次の (a) ~ (d) の結果を得た。

- (a) 多状態を持つシステム要素を含むシステムのハザードを S-A-FT で系統的に展開することができた。
- (b) S-A-FT から O-PrIm を導出し必要最小限の遷移作用の特定ができた。
- (c) S-A-FT から順序依存 O-PrIm 群を特定し, 事象生起順序依存型ハザードを基本事象のレベルで識別できた。
- (d) 相反基本事象および/または排他基本事象を有する順序依存 O-PrIm 群を系統的かつ論理的矛盾なく導出できた。

(a) ~ (d) の結果は, S-A プロセスチャートと FTA とが互いに補完的な役割を担うことによって, より合理的なハザード/リスク分析が可能となることを示している。

第7章 結言

7.1 研究成果

序論に示したが複雑化したシステムでは、可変安全状態、相反事象等に起因して多様なハザードが顕在化し得る。本論文では、この様なハザードを同定・分析し、より系統的かつ合理的に安全方策を導出するための手法として S-A プロセスチャートが提案されている。

相反事象に関して相反ハザードを持つシステムでは、あるハザードの抑制を目的とする機能の履行（安全側事象）が、他のハザードでは危険側事象となり得る。また、故障、エラー、失敗等だけでなく、システム要素の正常な要求機能の履行、修復、回復等が危険側事象となる可能性も存在する。例えば、システムのダウン状態からアップ状態への変化（事象）が、危害発現の危険側事象となり得る。相反ハザードの生成は事象（状態）生起順序と強い相関がある。このため、相反ハザードの同定および分析にあたっては、ハザード生成過程の動的挙動の検討、すなわち危害に至る潜在的状態遷移プロセスを次々と変化する状態および事象の連鎖として把握することが必要である。しかし、従来技法、例えば HAZOP スタディーズ、What-if、FTA、ETA、FMEA 等は、危害発現プロセスにおける状態と事象との関係およびその生起順序を系統的に同定して図式化する手段を持たず、相反ハザードの分析には不十分な側面をもつ（第1章、第2章）。

この課題に対して、本研究は、まず、状態と作用の生起順序に着目したハザードの図式表現技法、すなわち S-A プロセスチャートを提案した（第3章）。

次に、第4章では、環境試験槽の停止に起因する、および試験槽内での LIB の熱暴走に起因するハザードの同定とその抑制策の導出に S-A プロセスチャートを適用し、次の①～⑤に示す手順（図 7-1 参照）でそれらのハザードを同定し、当該技法の有効性を検証した。

- ① システムの初期状態および遷移作用を設定する。
- ② システムの初期状態に各遷移作用を組合せる。
- ③ システム状態遷移プロセスを展開し到達し得る危害を同定する。
- ④ ハザードの抑制概念を求める。
- ⑤ ハザードの抑制策を導出する。

その結果、S-A プロセスチャートを用い、次の (1) および (2) が可能であることが示された。

- (1) システムのそれぞれの状態にシステム要素の故障（無秩序状態作用）だけで

なく、正常機能の履行（秩序状態作用）によって起こる遷移作用を順次作用させることによって、危害発現までのシステムの状態遷移プロセスを系統的に追跡し、ハザードの網羅的同定が可能である。

- (2) S-A プロセスチャートにハザード抑制原理を適用しハザードの抑制策を系統的かつ合理的に導出することが可能である。

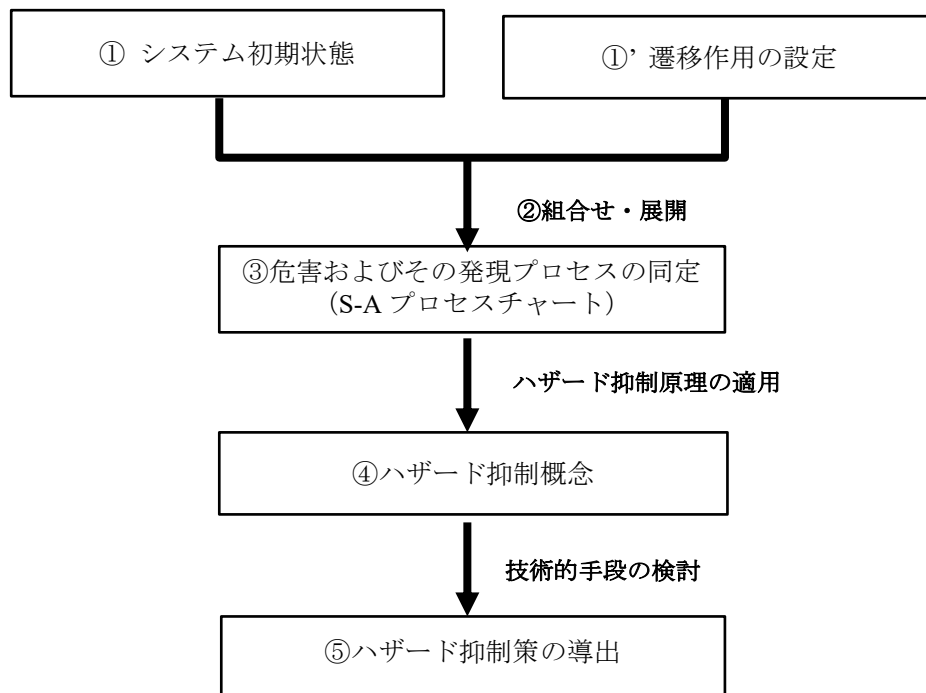


図 7-1 第 4 章の危害同定から抑制策導出までの手順

第5章では、すでに特定された危害と初期状態とを結ぶ状態遷移経路を識別し、S-A プロセスチャートで図式化するための技法を示した。この技法の有効性を検証するために、事例1では“着火エネルギー”を2状態，“可燃性ガス濃度”を3状態にモデル化し、事例2では“走行コース”を2状態，“車間距離”を3状態にモデル化し、ガス爆発および後方車が前方車に追突するプロセスの分析にS-A プロセスチャートを適用し、次の①～⑦に示す手順（図7-2参照）でそれらのハザードを分析した。

- ① すでに特定された危害状態から危害発現のための必要条件を構成するシステム要素を推定する。
- ② システム要素の属性がもつ状態からシステム状態および遷移作用を定義する。
- ③ システム状態遷移表を作成する。
- ④ 状態遷移経路図を求める。
- ⑤ 状態遷移経路図上で初期状態から危害に至る経路を同定する。
- ⑥ ハザードの抑制概念を求める。
- ⑦ ハザードの抑制策を導出する。

その結果、次の(1)および(2)の知見を得た。

- (1) 状態遷移経路図上で、初期状態と危害を結ぶ経路をたどることで、状態遷移経路の異なるハザードを系統的・網羅的に洗い出せることを示した。
- (2) 事例に対して検討・考察した結果、多状態をもつシステム要素の次の特性(a)および(b)を示した。

- (a) システム要素が可逆遷移を行う3状態を持ち、3状態の中央の状態がシステムの危害の必要条件となり得る場合、ある遷移作用 $A_{ij}(k, k')$ は、抑制作用にも危害に向かわせる作用にもなり得る。
- (b) システム要素が可逆遷移を行う3状態を持ち、3状態の端の状態がシステムの危害の必要条件となり得る場合、ある遷移作用 $A_{ij}(k, k')$ は、抑制作用または危害に向かわせる作用のどちらかにはなるが、両方になることはない。

(2), (a) の場合には、序論に記した課題、すなわち、あるハザードに対する安全方策が、他のハザードでは危険状態または危害を発現させる危険側事象となり得る。さらにその危険側事象は、故障、エラー、失敗等の無秩序状態作用だけでなく、システム要素の正常な要求機能の履行による秩序状態作用、修復、回復等によって行われることを、S-A プロセスチャートを用い特定できた。

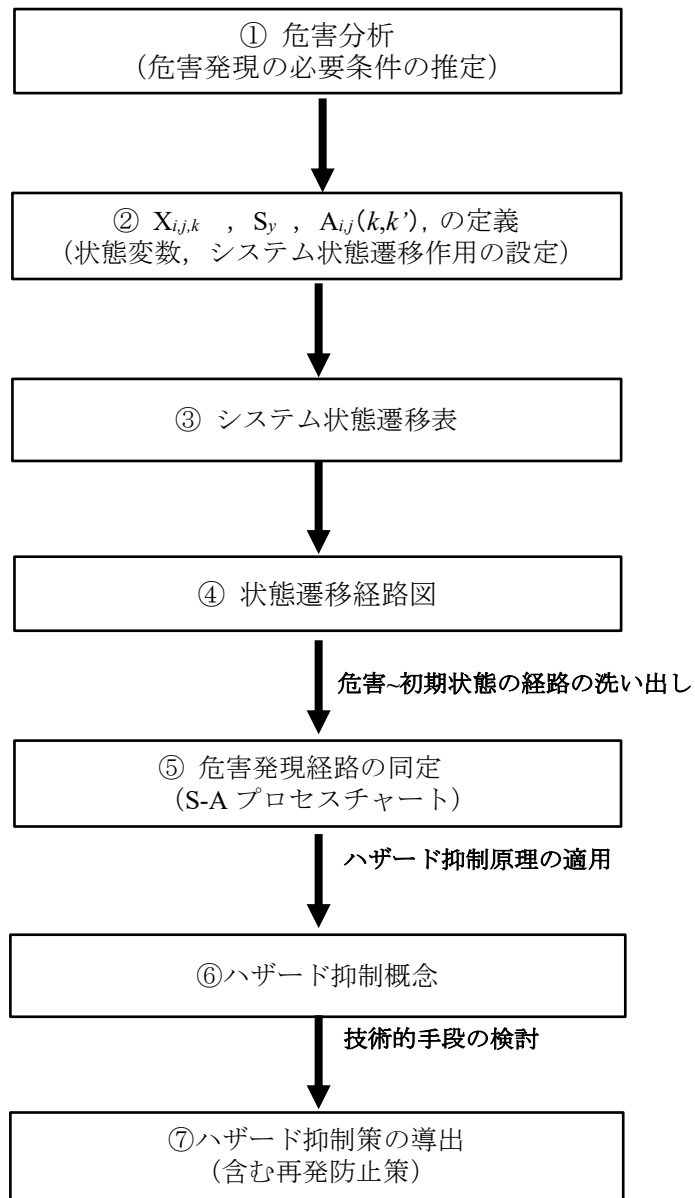


図 7-2 第 5 章の危害発現経路の同定～抑制策導出までの手順

第6章では、S-AプロセスチャートとFTAとの関係について論じた。S-Aプロセスチャートはハザードをシステムレベルの事象および状態の生起順序、タイミング等に依存して発現するハザードの同定・分析に適しているが、部品の故障等のシステム要素レベルでの分析に適していない。FTAは頂上事象からシステムの要素レベルまでの分析が可能であるが、システム要素の多状態およびその遷移順序に起因してシステム要素がダウン状態からアップ状態に移行することによって生起するハザードを系統的に展開することは困難である。この課題に対して、まずS-Aプロセスチャートのシステム状態および遷移作用とFTの事象とが関連付けられたS-A-FTを定義した。次に、多状態を持つシステム要素を含む修理系2冗長電源システムをシステム要素の状態遷移プロセス特性に基づきモデル化し、当該システムの故障に至るプロセスをS-Aプロセスチャートで洗い出した。さらに得られたS-AプロセスチャートをS-A-FTで展開することによって次の(a)～(d)の知見を得た。

- (a) 多状態を持つシステム要素を含むシステムのハザードをS-A-FTで系統的に展開することができた。
- (b) S-A-FTからO-PrImを導出し必要最小限の遷移作用の特定ができた。
- (c) S-A-FTから順序依存O-PrIm群を特定し、事象生起順序依存型ハザードを基本事象のレベルで識別できた。
- (d) 相反基本事象および/または排他基本事象を有する順序依存O-PrIm群を系統的かつ論理的矛盾なく導出できた。

(a)～(d)は、S-AプロセスチャートとFTAとが互いに補完的な役割を担うことによって、より合理的なハザード/リスク分析が可能となることを示している。

7.2 結論

本研究が明らかにした S-A プロセスチャートによるハザードの同定、分析、および抑制策導出手法の特徴を次の (a) ~ (d) に示す。

- (a) システム状態が状態を変化させる作用を伴う事象によって次々と遷移し到達し得る危害の洗い出し、すなわちハザードの網羅的同定が可能である。
- (b) 網羅的に同定したハザード群の中から相反ハザードの識別が可能である。
- (c) 相反ハザードの抑制策の系統的かつ合理的な導出が可能である。
- (d) さらに、S-A プロセスチャートを S-A-FT で展開することによって、より合理的なハザード/リスク分析が可能である

以上、本研究による S-A プロセスチャートは、ハザードを網羅的に同定・分析し、合理的に抑制策を導出するための手法として有用であり、その適用範囲は広い。

7.3 S-A プロセスチャートの今後の展開

S-A プロセスチャートには次の課題がある。

- (a) システム状態を各システム要素の状態変数の組み合わせで表す場合（第 5 章，5.2.2 項の例等），定義可能なシステム状態の最大数は，各システム要素が持つ状態変数の個数の総積となる。システム状態数が 18~20 個を超えると状態遷移経路等が複雑になり，人による作業では効率的な分析が困難となる。分析効率向上のため，今後，コンピュータ支援システムが必要となるが，コンピュータ支援ソフトの開発に本研究が理論的基礎を与える。
- (b) S-A プロセスチャートは，あるシステムが別のシステムとつながることによるシステムの複雑化，およびそれに伴うハザードの多様化に対する対応策としてその有効性が期待される。
- (c) S-A-FTは相反事象又は排他事象含むノンコヒーレントFTの側面を持つ。事象生起順序を持つノンコヒーレントFTに関する先行研究は見当たらず，O-PrImの識別とその論理的妥当性についてさらに研究が必要である。
- (d) S-A プロセスチャートの定量的分析技法，例えば，マルコフ状態遷移モデル等の分析技法との関連付け等が，今後の研究課題である。

参考文献

- 1) JIS Z 8051 : 安全側面－規格への導入方針 (2015)
- 2) JIS B 9700: 機械類の安全性-設計のための一般原則-リスクアセスメント及びリスク低減 (2013)
- 3) JIS C 0508-4: 電気・電子・プログラマブル電子安全関連系の機能安全-第 4 部 : 用語の定義および略語 (2012)
- 4) MIL-STD-882E: Department of Defense Standard Practice System Safety (2012)
- 5) ISO 12100: Safety of machinery-General principles for design-Risk assessment and risk reduction (2010)
- 6) I. Yoshimura, Y. Sato, Safety Achieved by the Safe Failure Fraction (SFF) in IEC 61508, IEEE Transactions on Reliability, Vol. 57, No. 4, pp. 662-669 (2008)
- 7) 杉本旭, 蓬原弘一, 安全の原理, 日本機械学会論文集 (C 編), 56 巻, 530 号 pp.2601-2609 (2017)
- 8) 梅崎重夫, 杉本旭, 安全作業システムの原理とその論理的構造, RIIS-RR-87, 産業安全研究所研究報告, 労働省産業安全研究所 (1988)
- 9) 杉本旭, 中村英夫, 産業機械の安全方策に関する基礎的考察－リスク評価に含まれる不確定性を考慮した安全方策の提案－, 信頼性, Vol.23, NO7, pp.659-675 (1990)
- 10) 木村真, 杉本旭, 機械のエネルギー遮断とロックアウトに関する論理的研究, 日本機械学会論文集 (C 編), Vol.75, No.752, pp.437-444 (2009)
- 11) 芳司俊郎, 安全原則に基づく生産システムの安全性と生産性の向上に関する研究, 明治大学大学院理工学研究科博士学位請求論文, pp.87-94 (2015)
- 12) 経済産業省, 次世代ロボットガイドライン (2007)
- 13) 竹市正彦, 陶山貢市, 佐藤吉信, 相反ハザードを考慮したプリクラッシュシステムの機能安全アセスメント, 日本機械学会論文集 (C 編), Vol.79, No.806, pp. 3839-3853 (2013)
- 14) JIS Z 8115: ディペンダビリティ (総合信頼性) 用語 (2019)
- 15) 杉本旭, 桑川壮一, 深谷潔, 安全制御におけるセンサ, RIIS-RR-85-7, 産業安全研究所研究報告, 労働省産業安全研究所 (1986)
- 16) E.Hollnagel, 小松原明哲 (監訳), 社会技術システムの安全分析, 海文堂出版 (2013)
- 17) 北村正晴, レジリエンスエンジニアリングが目指す安全 Safety-II とその実現法, IEICE Fundamentals Review, Vol.8, No.2, pp.84-95 (2014)
- 18) 野本秀樹, 道浦康貴, 石濱直樹, 片平真史, FRAM(機能共鳴分析手法)による成功学に基づく安全工学, SEC Journal, Vol.14, No.1, pp.42-49 (2018)
- 19) 野田浩幸, 小松原明哲, FRAM 分析を用いた機能共鳴型事故の対策導出手順の提案 FRAM 図の表記に関する提案, 人間工学, Vol.51, Supplement, pp.234-235 (2015)

- 20) 野田浩幸, 小松原明哲, FRAM 分析における FRAM 図の表記に関する提案, ヒューマンファクターズ, Vol.20, No.2, pp.83-87 (2016)
- 21) 高木伸夫, プロセス安全性評価における HAZOP の効率的運用, 安全工学 Vol.44, NO.1, pp.244-251 (2005)
- 22) H.G.Lawley, Operability Studies And Hazard Analysis, Chemical Engineering Progress, Vol.70, No.4, pp.45-56 (1974)
- 23) IEC 61882: Hazard and operability studies (HAZOP studies) – Application guide (2016)
- 24) IEC 31010: Risk management-Risk assessment techniques (2019)
- 25) Alan J. Card, James R. Ward, P. John Clarkson, Beyond FMEA: the structured what-if technique (SWIFT), Journal of Healthcare Risk Management, 31(4), pp. 23–29 (2012)
- 26) IEC 60812 : Failure modes and effects analysis (FMEA and FMECA) (2018)
- 27) 石山敬幸, 新しい信頼性の技術 FMEA と FTA, オペレーションズ・リサーチ, pp.432-441 (1976)
- 28) 石井博司, 飛岡利明, 中野一夫, 信頼性予測のためのフォールト・ツリー手法の有効性, オペレーションズ・リサーチ, pp.32-40 (1983)
- 29) Jerry B. Fussell, Gary j. Powers, R. G. Bennetts, Fault Trees-A Safe of Art Discussion, IEEE Transactions on Reliability, Vol. R-23, No. 1, pp. 51-55 (1974)
- 30) NUREG 0492: Fault Tree Handbook, U.S. Nuclear Regulatory Commission (1981)
- 31) JIS C 5750-4-4 : ディペンダビリティマネジメントー第 4-4 部, システム信頼性のための解析技法ー故障の木解析 (2011)
- 32) 井上威恭, FTA 安全工学, 日刊工業新聞社 (1979)
- 33) J. B. Fussell, A Formal Methodology for Fault Trees Construction, Nuclear Science and Engineering:52, pp. 421-432 (1973)
- 34) 幸田武久, 熊本博光, 井上絃一, イベントツリー解析による大規模システムのリスク評価, 安全工学, Vol.24, No.2, pp.85-92 (1985)
- 35) 井上絃一, 熊本博光, リスクアナリシスの方法論, 安全工学, Vol.23, NO6, pp.323-329 (1984)
- 36) JIS C 5750-4-3 : ディペンダビリティマネジメントー第 4-3 部, システム信頼性のための解析技法ー故障モード・影響解析 (FMEA) の手順 (2011)
- 37) 鈴木順次郎, 槇野鉄治, 石坂茂樹, FMEA・FTA 実施法, 日科技連出版社, pp.36-116 (1986)
- 38) 益田昭彦, 高橋正弘, 本田陽広, 新 FMEA 技法, 日科学技連 (2012)
- 39) 豊嶋伊知郎, 西川武一郎, PetriNet によるシステム非正常系可視化の検討, 信学技法, CAS2008-59, CST2008-37, pp.83-88 (2008)
- 40) MIL-STD-1629A: Procedures for Performing a Failure Mode, Effects and Critically Analysis (1980)

- 41) 柴垣光男, 福田隆文, 佐藤吉信, ハザードの同定と抑制策導出のための S-A プロセスチャートとその適用, 安全工学, Vol.56, NO3, pp.197-198 (2017)
- 42) 柴垣光男, 福田隆文, 佐藤吉信, 多状態を持つ要素を含むシステムの S-A プロセスチャートを用いたハザードの分析, 安全工学, Vol.59, No.1, pp.15-26 (2020)
- 43) EC TR 63039: Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state (2016)
- 44) ISO/IEC Guide51: Safety aspects – Guidelines for their inclusion in standards (2014)
- 45) 佐藤吉信, 井上紘一, 人間-ロボット系の安全性評価 (第 6 報, 移動ロボットにおける潜在危険制御系の構成について) 日本機械学会論文集 (C 編), Vol.55, No.518, pp.2663-2671 (1989)
- 46) 佐藤吉信, 井上紘一, 人間-ロボット系の安全性評価 (第 5 報, 潜在危険制御系の構成原理), 日本機械学会論文集 (C 編), Vol.54, No.505, pp.2164-2673 (1988)
- 47) 佐藤吉信, 井上紘一, 熊本博光, 人間-ロボット系の安全性評価 (第 4 報, 1 台の産業用ハンドリングロボットの潜在危険抑制措置の評価), 日本機械学会論文集 (C 編), Vol.52, No.482, pp.2754-2763 (1986)
- 48) 佐藤吉信, 井上紘一, 熊本博光, 人間-ロボット系の安全性評価 (第 3 報, 順序依存型故障理論の定量化について), 日本機械学会論文集 (C 編), Vol.52, No.475, pp.1110-1117 (1986)
- 49) 佐藤吉信, 井上紘一, 人間-ロボット系の安全性評価 (第 2 報, 災害発生機構の解析のための論理モデルその 1), 日本機械学会論文集 (C 編), Vol.52, No.474, pp.823-832 (1986)
- 50) 佐藤吉信, 井上紘一, 人間-ロボット系の安全性評価 (第 1 報, 作用-変化と作用連鎖モデルによる潜在危険の同定), 日本機械学会論文集 (C 編), Vol.51, No.468, pp.2188-2195 (1985)
- 51) Nancy G. Leveson, John P. Thomas, “STPA HAND BOOK”,
http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
- 52) Castilho, D.S. Urbina, L.M.S. de Andrade, D. , STPA for continuous controls: A flight testing study of aircraft crosswind takeoffs , Safety Science, pp.129-139 (2018)
- 53) 独立行政法人情報処理推進機構, はじめての STAMP/STPA – システム思考に基づく新しい安全性解析手法 – (2016)
- 54) 兼本茂, システムズ理論で考える複雑システムの安全, STAMP/STPA, 安全工学 Vol.57, p362~p368, NO5 (2018)
- 55) 柴垣光男, 福田隆文, 佐藤吉信, 状態変化と作用連鎖に注目したハザードの図式表現 – S-A プロセスチャートと A-C モデルの比較 –, 信学技法, Vol.118, No.370, pp.21-24 (2018)
- 56) 文献 38) の pp.26-29

- 57) 平井邦彦, 形式的モデル化, pp.2-13, 森北出版 (2019)
- 58) 児玉慎三, 離散事象システム研究の動向と課題, 計測と制御, Vol.31, No.1, pp.208-213 (1992)
- 59) 西尾章治郎, システム性能評価のための時間および確率ペトリネット, 計測と制御, Vol.28, No.9, pp.760-769 (1989)
- 60) 文献 57) の pp.30-46
- 61) 高原康彦, “システム工学の理論”, pp.17-22, 日刊工業新聞社 (1974)
- 62) Nancy G. Leveson, Janice L. Stolzy, Safety Analysis Using Petri Nets, IEEE Transactions on Software Engineering, Vol.SE-13, No.3, pp.386-397 (1987)
- 63) 佐々木亮悦, 米田友洋, タイムペトリネットを用いた踏切制御プログラムの形式的検証, 電学論 C, Vol. No.1151, pp.157-164 (1995)
- 64) T. S. Liu & S. B. Chiou, The application of Petri nets to failure analysis, Reliability Engineering and System Safety 57 pp.129-142 (1997)
- 65) 佐藤吉信, “固有フェール・セーフ・システムの構成と多相安全設計について”, 安業安全研究所研究報告, RIIS-RR-90, p.11 (1990)
- 66) 佐藤吉信, “新技術を用いたシステムに生ずる潜在危険の評価”, 産業安全研究所特別研究報告, RIIS-RR-86, No.1, pp. 103-117 (1986)
- 67) 佐藤吉信, 機能安全の基礎, P101~P107, 日本規格協会 (2014)
- 68) 特別研究報告, 機械の安全化のための計測技術に関する特別研究, RIIS-RR-86, No.1, pp. 103-117 (1986)
- 69) 柴垣光男, 福田隆文, 佐藤吉信, 環境試験槽の停止によるハザードの考察, 第 48 回安全工学研究発表会, pp.121-124 (2015)
- 70) 高木伸夫, “非正常 HAZOP の基本手順と進め方”, 安全工学 Vol.53, NO4, pp.244-251 (2014)
- 71) 高圧ガス保安協会, リスクアセスメント・ガイドライン (概要版) (2015)
- 72) IEC61800-5-2 : Adjustable speed electrical power drive system- Part 5-2:Safety requirements-Functional (2007)
- 73) IEC 60204-1 : Safety of machinery – Electrical equipment of machines – Part 1: General requirements (2005)
- 74) JIS C 60068-1 : 環境試験方法—電気・電子—第 1 部 : 通則および指針 (2016)
- 75) JIS C 60068-2-1 : 環境試験方法—電気・電子—第 2-1 部 : 低温 (耐寒性) 試験方法 (試験記号 : A) (2010)
- 76) JIS C 60068-2-67 : 環境試験方法—電気・電子—基本的に構成部品を対象とした高温高湿, 定常状態の促進試験 (2001)
- 77) JIS C 8715-2 産業用リチウム二次電池の単電池および 電池システム—第 2 部 : 安全性要求事項 (2019)

- 78) JIS C 8712 ポータブル機器用二次電池（密閉小型二次電池）の安全性（2015）
- 79) 柴垣光男，密閉容器内におけるリチウムイオン 2 次電池の熱暴走試験結果に基づく環境試験用恒温槽のリスク低減策の考察，pp.101-104，第 47 回安全工学研究発表会（2014）
- 80) 鶴田俊，火災時のリチウムイオン電池の赤熱粒子飛散挙動，消研輯報 53 号，pp.8-11 消防庁消防研究所（1999）
- 81) 柴垣光男，神山敦，下坂幸，“リチウムイオン 2 次電池の強制発火試験結果に基づく環境試験用恒温槽のリスク低減策の考察”，pp.243-248，第 42 回信頼性・保全性（2012）
- 82) リチウムイオン電池を用いた蓄電設備の普及に対応した火災予防対策等検討委員会報告書，東京消防庁予防部（2011）
- 83) 鶴見平三郎，林年宏，産業安全研究所研究報告 RIIS-RR-18-3，耐圧容器の内容積と爆発圧力の関係について－防爆電気機器の試験法に関する一考察－（1969）
- 84) 柴垣，佐藤，溶剤乾燥用高温槽の安全対策-爆発事故防止対策とその効果，第 25 回日科技連信頼性・保全性シンポジウム，pp.343-350（1995）
- 85) 松田東栄，内藤道夫：産業安全研究所研究報告 RIIS-SD-75-1，粉じん爆発に対する圧力放散設備（1975）
- 86) 田口昇，鶴見平三郎，林年宏，松井英憲，爆発放散孔に関する研究（第 1 報）－熱風流動式箱型乾燥機に対する応用について－，RIIS-RR-19-1 産業安全研究所研究報告，労働省産業安全研究所（1970）
- 87) 下重，柴垣，水圧および爆発圧力による爆発放散口の動作特性比較，日科技連 第 47 回 信頼性・保全性シンポジウム，pp.114-119（2017）
- 88) 林年宏，爆発放散孔に関する研究（第 3 報）－破裂膜式放散孔の設計方法について－，RIIS-RR-85-2，産業安全研究所研究報告，労働省産業安全研究所（1985）
- 89) 林年宏，爆発放散孔に関する研究（第 4 報）－離脱式放散孔の特性について－，RIIS-RR-88，産業安全研究所研究報告，労働省産業安全研究所（1988）
- 90) 産業安全研究所技術指針：NIIS-TR-No.38，爆発圧力放散設備技術指針（2005）
- 91) Yoshinobu Sato, Mitsuo Shibagaki, “Analysis of the Hazard-Control System for Alcoholic-Abstergent-Drying Ovens”, International Conference on Probabilistic Safety Assessment Methodology and Applications, pp.763-768（1995）
- 92) 平野敏右，燃焼学－燃焼現象とその制御－，海分堂出版，pp.112-122（1986）
- 93) 安全工学協会編，安全工学講座 2 爆発，pp.15-38，海文堂出版（1983）
- 94) Richard E. Barlow, Frank Proschan, Statistical Theory of Reliability and Life Testing , Holt, Rinehart and Winston, Inc.（1975）
- 95) 文献 24 の pp.72-77
- 96) 大鑄史男，システム信頼性の数理，pp.21-61，コロナ社（2019）
- 97) 佐藤吉信，安全工学と信頼性工学の接点－その 4: コヒーレントシステムと非コヒー

- レントシステム, 安全工学, Vol.41, pp.329-334, NO5 (2002)
- 98) 西田俊夫, 大鑄史男, コヒーレント・システム, オペレーションズ・リサーチ, pp.650-657 (1982)
- 99) 西干機, 佐藤吉信, 事象生起順序依存-非コヒーレント FTA の提案と事故解析, 安全工学, Vol.49, pp.28-37, NO1 (2010)
- 100) Hiromitsu Kumamoto and Ernest J.Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists-Second Edition, IEEE Press, pp.251-252 (1996)
- 101) Takehisa Koda, “A Simple Method to Derive Minimal Cut Set for a Non-coherent Fault Tree”, International Journal of Automation and Computing 2, pp.151-156 (2006)
- 102) Septavera Sharvia, Yiannis Papadopoulos, Non-coherent Modelling in Compositional Fault Tree Analysis, Proceedings of the 17th World Congress The International Federation of Automatic Control Seoul, Korea, pp.4138-4143 (2008)
- 103) Sally Chdstian Beeson, Non-coherent Fault Tree Analysis, A Doctoral Thesis for the award of Doctor of Philosophy of Loughborough University (2002)
- 104) J.J.B. Fussel, E.F. Aber, R.G. Rahl, On the Quantitative Analysis of Priority-AND Failure Logic, IEEE Transactions on Reliability, Vol.R-25, NO.5, pp.324-326 (1976)
- 105) W. Long, Y. Sato, M. Horigome, Quantification of sequential failure logic for fault tree analysis, Reliability Engineering and System Safety 67, pp.269-274 (2000)
- 106) E. Hollnagel, Functional Resonance Analysis Method (2018)
<https://functionalresonance.com/onewebmedia/Manual%20ds%201.docx.pdf>

謝 辞

本研究は、エタックエンジニアリング株式会社および楠本化成株式会社において筆者が従事した製品企画、開発、設計等業務の多忙を理由に長年放置されていた課題であった。しかし、長岡技術科学大学大学院工学研究科博士後期課程情報・制御工学専攻に入学する機会を得て研究を再開し、その在籍期間を通して得られた成果をまとめたものである。

本研究を進めるに当たり、指導教員の福田隆文教授からは研究テーマの絞り込みから調査、論文執筆まで多くのご指導をいただいた。ここに感謝の意を表す。

また、元東京海洋大学佐藤吉信教授には本研究の契機をいただき、その遂行にあたって終始ご指導をいただいた。ここに感謝の意を表す。

予備審査および最終審査では、多方面の視点からご指摘および有益なご助言をいただいた長岡技術科学大学 門脇敏教授、三好孝典教授、木村哲也准教授、芳司俊郎准教授に対し感謝の意を表す。

長岡技術科学大学への入学に際しご理解をいただいた楠本化成株式会社石川伸吾取締役副社長に対し感謝の意を表す。

さらに、長岡技術科学大学への入学に際しご支援をいただいた楠本化成株式会社エタック事業部信頼性クリニック井原惇行特別顧問（当時）に対し感謝の意を表す。

最後に、本研究の遂行にあたって遅々として進まず悲観的になりがちな筆者を支えてくれた先輩、後輩、友人の皆様に心より感謝する。

付録 1 初期状態～危害に至る図 4-6 の潜在的状態遷移プロセス一覧 (No.1～No.114)

この一覧表は、本文第 4 章、図 4-6 の初期状態～危害に至る潜在的状態遷移プロセス No.1～No.114 である。各行の左端は初期状態を、右端は最終状態（危害）を表している。

NO.	初期状態～危害に至る潜在的状態遷移プロセス一覧													
1	S ₅	S ₆	S ₁₂	S ₁₃	SA1	A								
2	S ₅	S ₆	S ₁₂	S ₁₃	SA2	B								
3	S ₅	S ₆	S ₁₂	S ₁₃	SA3	D								
4	S ₅	S ₆	S ₁₂	S ₁₃	C									
5	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	C								
6	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	C							
7	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	C					
8	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	SA1	A				
9	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S ₁₄ '	SA2	B				
10	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₃	C							
11	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₃	SA1	A						
12	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₃	SA2	B						
13	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₃	SA3	D						
14	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	C							
15	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	C					
16	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S ₁₄ '	C			
17	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S ₁₄ '	SA1	A		
18	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S ₁₄ '	SA2	B		
19	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S ₁₄ '	C			
20	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S ₁₄ '	SA1	A		
21	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S ₁₄ '	SA2	B		
22	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	S ₁₆	SA3	D						
23	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₀	SA3	D							
24	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₄	S ₁₄ '	C							
25	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₄	S ₁₄ '	SA1	A						
26	S ₅	S ₆	S ₁₂	S ₁₃	S ₁₄	S ₁₄ '	SA2	B						
27	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	C								
28	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₀ '	S ₁₃	C					
29	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₀ '	S ₁₃	S ₁₀	C				

NO.	初期状態～危害に至る潜在的状態遷移プロセス一覧															
30	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₁	C					
31	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA1	A		
32	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA2	B		
33	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	C			
34	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₃	C					
35	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₃	SA1	A				
36	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₃	SA2	B				
37	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₃	SA3	D				
38	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	C					
39	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	C			
40	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	SA1	A
41	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	SA2	B
42	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	C	
43	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA1	A
44	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA2	B
45	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	C	
46	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	S ₁₆	SA3	D				
47	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₀	SA3	D					
48	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₄	S _{14'}	C					
49	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₄	S _{14'}	SA1	A				
50	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	S ₁₄	S _{14'}	SA2	B				
51	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	SA1	A						
52	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	SA2	B						
53	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S _{10'}	S ₁₃	SA3	D						
54	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	C								
55	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	S ₂₀	S ₁₄	C						
56	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	S ₂₀	S ₁₄	S _{14'}	C					
57	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	S ₂₀	S ₁₄	S _{14'}	SA1	A				
58	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	S ₂₀	S ₁₄	S _{14'}	SA2	B				
59	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	SA3	D							
60	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₁₆	S ₁₉	SA4	E							
61	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₂₀	S ₁₄	C								
62	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₂₀	S ₁₄	S _{14'}	C							
63	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₂₀	S ₁₄	S _{14'}	SA1	A						

NO.	初期状態～危害に至る潜在的状態遷移プロセス一覧														
64	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	S ₂₀	S ₁₄	S _{14'}	SA2	B					
65	S ₅	S ₆	S ₁₂	S ₁₈	S ₁₉	SA3	D								
66	S ₅	S ₆	S ₇	C											
67	S ₅	S ₆	S ₇	S ₁₃	C										
68	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	C									
69	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₁	C								
70	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	C						
71	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA1	A					
72	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA2	B					
73	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₃	C								
74	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₃	SA1	A							
75	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₃	SA2	B							
76	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₃	SA3	D							
77	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	C								
78	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	C						
79	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	C				
80	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	SA1	A			
81	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	S ₁₄	S _{14'}	SA2	B			
82	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	C				
83	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA1	A			
84	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA2	B			
85	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	S ₁₆	SA3	D							
86	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	SA3	D								
87	S ₅	S ₆	S ₇	S ₁₃	S ₁₀	SA4	E								
88	S ₅	S ₆	S ₇	S ₁₃	S ₁₄	S _{14'}	C								
89	S ₅	S ₆	S ₇	S ₁₃	S ₁₄	S _{14'}	SA1	A							
90	S ₅	S ₆	S ₇	S ₁₃	S ₁₄	S _{14'}	SA2	B							
91	S ₅	S ₆	S ₇	S ₁₃	SA1	A									
92	S ₅	S ₆	S ₇	S ₁₃	SA2	B									
93	S ₅	S ₆	S ₇	S ₁₃	SA3	D									
94	S ₅	S ₆	S ₇	S ₃	C										
95	S ₅	S ₆	S ₇	S ₃	S ₁₀	C									
96	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₁	C								
97	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	C						

NO.	初期状態～危害に至る潜在的状態遷移プロセス一覧															
98	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA1	A						
99	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₁	S ₁₄	S _{14'}	SA2	B						
100	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₃	C									
101	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₃	SA1	A								
102	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₃	SA2	B								
103	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₃	SA3	D								
104	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	C									
105	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	S ₁₇	S ₁₁	C							
106	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	C					
107	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA1	A				
108	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	S ₁₇	S ₂₀	S ₁₄	S _{14'}	SA2	B				
109	S ₅	S ₆	S ₇	S ₃	S ₁₀	S ₁₆	SA3	D								
110	S ₅	S ₆	S ₇	S ₃	S ₁₀	SA3	D									
111	S ₅	S ₆	S ₇	S ₃	SA3	D										
112	S ₅	S ₆	S ₇	S ₃	SA4	E										
113	S ₅	S ₆	S ₇	SA3	D											
114	S ₅	S ₆	S ₇	SA4	E											

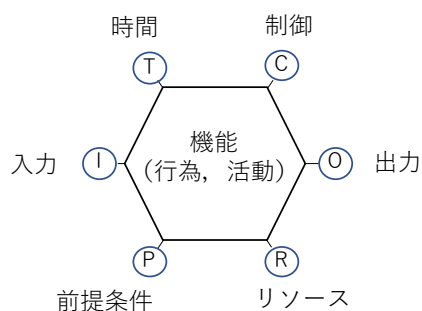
付録 2 FRAM (機能共鳴分析技法:Functional Resonance Analysis Method) の概要

1. 背景

FRAM (機能共鳴分析技法) は、を理論的背景として、E. Hollnagel によって提案された安全分析技法である^{16), 17)}。レジリエンスエンジニアリングは、システムを十分に記述することが可能な単一の電気機械システム等の場合、危害事象を単純な因果関係で分析することが可能であるが、システムを十分に記述することが不可能なシステム、すなわち複雑システム、開発上流の設計仕様が明確でないシステム、社会システム、組織、人間行動を含むシステム等の場合、危害事象を単純な因果関係で分析することは困難である、との観点を持つ。この観点から、FRAM は、十分に記述できないシステムに適用可能な安全分析技法として位置づけられている。

2. 技法の概要

FRAM は、システムを構成要素とその組み合わせとしてではなく、機能の組み合わせとしてとらえる。FRAM において機能とは、目標を達成するために必要な手段であり、特定の結果を生成するために必要な行為または活動を意味する。機能は付図 2-1 に示す 6 角形で表される 6 つの側面を持つ。



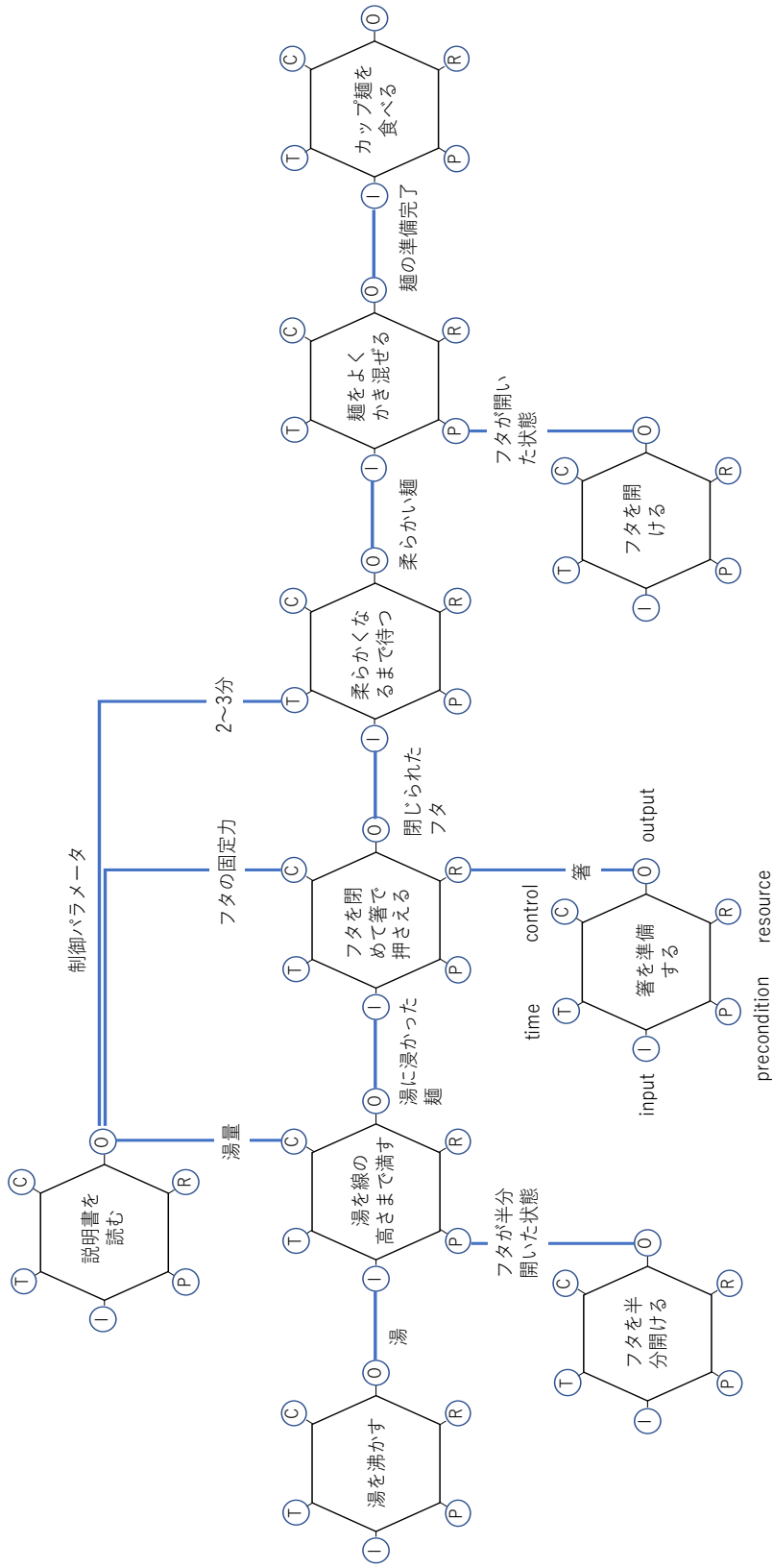
- 入力 (I) : 機能の開始指示
- 出力(O) : 機能が行なったこと (入力(I)の処理) の結果
- 前提条件(P) : 入力を実行される前に行われるべき条件
- リソース(R) : 機能の実行に必要なもの (実行条件: ツール, 技術, データ等)
消費されるもの (資源: 資金, 原材料, エネルギー等)
- 制御 (C) : 所望の出力が得られる様に機能を制御する。(計測と修正, 手順, ガイドライン等による指示)
- 時間 (T) : 機能の実行時間

付図 2-1 FRAM の機能表現

FRAM では、六角形で表された各機能の結合によってシステムの構造を表現する。“カップ麺を食べる”の過程をモデル化した例を付図 2-2 に示す¹⁰⁶⁾。付図 2-2 は各機能によって行われる次の入出力を表している。

- 1) 機能“湯を沸かす”を実行し“湯”が出力される。
- 2) 機能“フタを半分開ける”を実行し“フタが半分開いた状態”が出力される。
- 3) 2) によって“湯”が、入力として許可される。
- 4) 機能“説明書を読む”を実行し，“湯量”が出力される。
- 5) 1) , 2) , 4) が入力されることによって機能“湯を線の高さまで満す”を実行し，“湯に浸かった麺”が出力される。
- 6) 機能“箸を準備する”を実行し，資源“箸”が出力される。
- 7) 機能“説明書を読む”を実行し“フタの固定力”が出力される。
- 8) 5) ~7) が入力されることによって“フタを閉めて箸で押さえる”を実行し，“閉じられたフタ”が出力される。
- 9) 機能“説明書を読む”を実行し“2~3分”が出力される。
- 10) 8) , 9) が入力されることによって機能“柔らかくなるまで待つ”を実行し，“柔らかい麺”が出力される。
- 11) 機能“フタを開ける”を実行し，“フタが開いた状態”が出力される。
- 12) 11) によって“柔らかい麺”の入力が許可される。
- 13) 10) , 11) が入力されることによって機能“麺をよく混ぜる”を実行し，“麺の準備完了”が出力される。
- 14) 13) が入力されることによって，“カップ麺を食べる”が実行される。

FRAM は、システムの成功要因から失敗要因を導出する。付図 2-2 は“カップ麺を食べる”という目的を達成するための成功要因を表しているといえる。最終的な結果の不確かさは、各機能の入出力の変動（振幅）を明らかにすることによって推定される。例えば、付図 2-2 の変動要因として、湯の温度、湯量、箸の重さ、待機時間などが考えられる。これらの変動要因が許容値から逸脱する場合、目的の達成は困難である。しかし、これ等の各変動要因が許容値内であっても、いくつかの変動が連鎖する、変動順序、変動組み合わせが変化する等に起因して目的の達成に失敗する場合がある。この様な失敗は FRAM において機能共鳴型といわれる。



付図2-2 カップ麺を準備して食べるまでの機能の連携 (文献¹⁰⁶⁾より修正引用)