

ソフトウェア安全設計概説

2008年2月

株式会社レンタコーチ

<http://homepage2.nifty.com/rent-a-coach/>

講座概要

◆受講対象者

- ソフトウェア安全設計を学ぼうとするソフトウェア技術者
- ソフトウェア安全設計の要点を把握したいマネージャ層

◆習得事項

- 安全の意味と安全設計の進め方
- 安全設計に関する標準規格、基本概念、一般原則
- リスクアセスメント技法の種類と特徴
- 各種リスク低減技法の特徴

講座内容

- ◆安全設計に関する各分野での動き
- ◆安全設計に関する国際規格
- ◆リスクアセスメント技法
- ◆リスク低減のための設計技法
- ◆安全設計への取組み方法

まず、安全という言葉はどのように使われている？

◆ Googleで「安全」を検索すると、次のように多くの分野で使われている：

- (労働)安全衛生
- 安心安全な生活、暮らしの安全
- 交通安全、安全運転
- 食品安全委員会
- 原子力安全
- スポーツ安全
- 電気用品安全法
- 製品安全
- 安全保障
- 環境安全、等々

◆ 製品安全4法によれば、

- 安全性の確保には、生命又は身体に対する危害の発生を防止するための技術基準に適合することが必要となる。

製品安全4法:電気用品安全法、消費生活用製品安全法、ガス関連2法

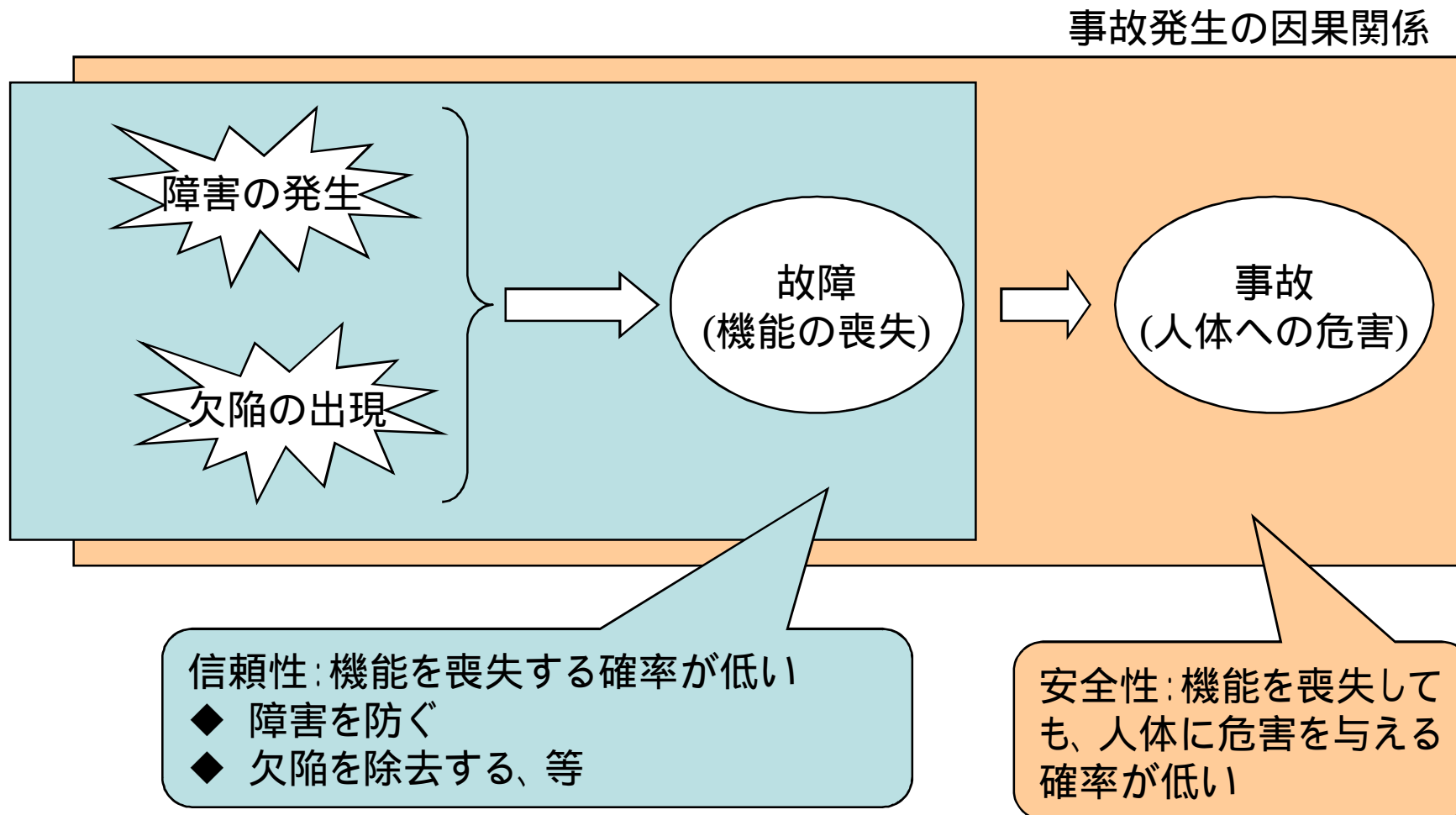
共通認識として:安全と安全設計の意味

- ◆安全とは、人体に危害を与える等のリスクが許容できる水準まで低減されている状態を意味する。
- ◆安全設計とは、設計の段階で安全を作りこむことであり、そのためのリスクアセスメントとリスク低減を行うことを意味する。

safetyとは:

freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment (IEC61508から引用)

共通認識として:安全性と信頼性の違い



障害: fault、欠陥: defect、故障: failure

福知山線脱線事故対策にリスクアセスメントを

107人が死亡した福知山線脱線事故(05年4月)を受け、JR西日本が新たな安全計画を策定するために設けた外部有識者による「安全推進有識者会議」が18日、新安全計画についての提言をまとめた。「リスクアセスメント」と呼ばれる危険評価手法の導入などが柱。実施されれば部門間や上司と部下の連携が不可欠となり、企業風土の大幅な改善を迫られる。同社は提言に基づき、来月にも「死傷事故ゼロ」を目標とする新たな安全計画を策定する。

リスクアセスメントは、主に建設業など危険の伴う職場で労働災害防止に用いられる手法。新たな作業を行う際、現場に潜む危険や最悪の場合にどんな事故が起こり得るかを把握し、対策を立てることをいう。

有識者会議は、この手法を労災だけでなく、乗客の死傷事故防止に応用するよう提言した。具体的には、現場の社員が気がかりに感じる軽微なトラブルがあった場合、重大事故を招くリスクの有無を検討する他、線路や信号など施設の改良やダイヤ改正などの前に「実施した場合の危険を見落としていないか」などを考えるという。

出典:毎日jp、2/18/2008

第1章 安全設計に関する各分野での動き

- ◆技術雑誌
- ◆行政、IPA SEC
- ◆展示会

技術雑誌での取組み状況

◆日経エレクトロニクス

- 2005年12月19日号、特集「ソフトウェアは硬い」で IEC61508を紹介し、形式手法を解説。
- 2006年9月25日号、特集「不具合を転機に」で製品安全を取り上げ、FTA等のリスク分析手法を紹介。
- 2006年12月18日号、特集「レクサスのカイゼン」で自動車開発におけるモデルベース開発、機能安全を紹介。

行政の動向

- ◆ 経済産業省は、組込みソフトウェア開発力強化推進委員会に機能安全部会準備部会を2006年4月に発足させた
 - 準備部会の活動成果として、ET2006(11月開催)において「組込みシステムの安全性向上の勧め(機能安全編)」という小冊子を配布

IPA SECの動向

- ◆ SEC journal第7号(2006年9月発行)で機能安全に関する解説を掲載。
 - 「機能安全の枠組み」、(株)日本機能安全
- ◆ IPAフォーラム2006(10月開催)で啓蒙的な講演を実施。
 - 「機能安全の標準化について」、東京海洋大学
- ◆ ET2006(11月開催)で機能安全に関する小冊子を配布
 - 「組込みシステムの安全性向上の勧め(機能安全編)」
- ◆ IEC61508規格改訂審議への意見反映を計画中。
- ◆ 2007年度には機能安全実現手法を整備し、組込みソフト向けの開発プロセスガイドESPRver2.0にセイフティエンジニアリングプロセスを追加。

ESEC:組込みシステム開発技術展

◆ESEC2006(6月開催)に機能安全関係の講演、技術セッションが登場

- 「組込みシステムの機能安全」、ベルコンサルティング
- 「組込みソフトウェアの品質と安全性向上」、東芝
- 「IEC61508に基づくソフトウェア設計と認証」、日本システム安全研究所

◆ESEC2007(5月開催)でも機能安全関係の専門セミナーを継続

- 機能安全を実現する設計手法とリスク分析
- 事例に学ぶ機能安全の実際

組込み総合技術展

- ◆(社)組込みシステム技術協会JASA主催
- ◆機能安全に関するテクニカルセッションがET2006(11月開催)に始めて登場
 - 「組込みシステムの機能安全」、日本機能安全
 - 「自動車業界の機能安全最新動向」、トヨタ
- ◆ET2007(11月開催)でも機能安全に関するセッションが開かれた
 - 「車載システムの機能安全に関わる国際規格への取り組み」、トヨタ
 - 「高信頼性リアルタイムOSと機能安全」、名古屋大学

第2章 安全設計に関する国際規格

◆ 国際安全規格

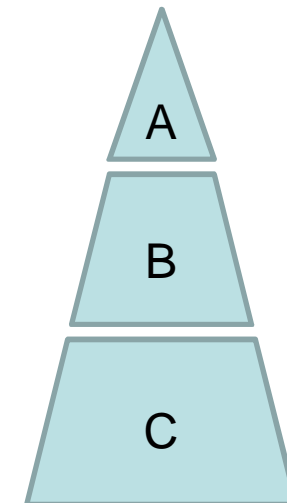
- 機械安全規格: ISO12100 (JIS B 9700)
- 機能安全規格: IEC61508 (JIS C 0508)

◆ 産業別の機能安全規格

- 米国DoD: MIL-STD-882D
- 英国防衛: Def-Stan-00-56
- 航空機: DO-178B
- 原子力: IEC61513
- プラント制御: IEC61511
- 鉄道: IEC62278、IEC62279(ソフトウェア関係)
- 自動車: ISO26262
- 医療機器: IEC62304

国際安全規格の基本構成

- ◆ 機械系はISO、電気系はIEC
- ◆ ISO/IECガイド51に準拠
- ◆ A規格:基本安全規格
 - ISO12100:基本概念、設計のための一般原則
 - ISO14121:リスクアセスメント原則
- ◆ B規格:グループ安全規格
 - ISO13849-1:制御システム安全規格
 - IEC61508:電气的安全機能規格
 - その他多数
- ◆ C規格:製品安全規格
 - 産業分野に応じて多数



機械安全規格: ISO12100 (JIS B 9700)

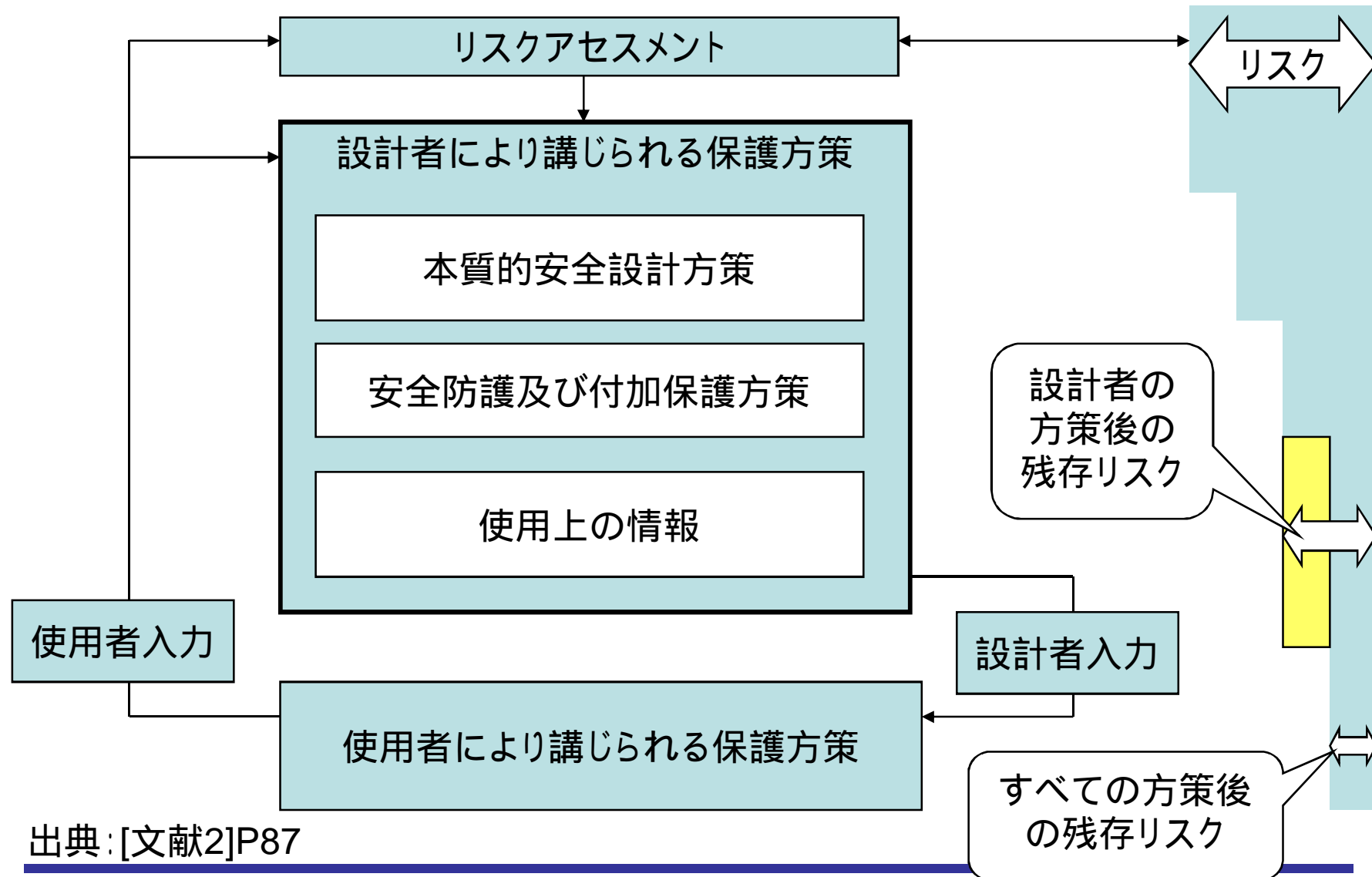
- ◆ 機械類の安全性に関する基本安全規格(A規格)
- ◆ 設計のための基本概念、一般原則を扱い、2部構成
 - 第1部: 基本用語、方法論
 - 第3章 用語及び定義
 - 第4章 機械類の設計時に考慮すべき危険源
 - 第5章 リスク低減のための方法論
 - 第2部: 技術原則
 - 第4章 本質的安全設計方策
 - 第5章 安全防護及び付加保護方策
 - 第6章 使用上の情報

安全に関する基本概念、リスク低減の方法論は、すべてに共通

用語及び定義

- ◆ 危害(harm)
 - 身体的傷害又は健康障害
- ◆ 危険源(hazard、又は潜在危険)
 - 危害を引き起こす潜在的根源
- ◆ 危険状態(hazardous situation)
 - 人が少なくとも一つの危険源に暴露される状態
- ◆ 不具合(障害、fault)
 - 要求される機能を実行できないアイテムの状態
- ◆ 故障(failure)
 - 要求される機能を遂行する能力がアイテムになくなること
 - 故障は事象であって、状態を意味する障害とは区別される
- ◆ リスク
 - 危害の発生確率と危害のひどさの組合せ
- ◆ リスクアセスメント
 - リスク識別、リスク見積り、リスク評価を含むすべてのプロセス

設計者による保護方策がより求められる

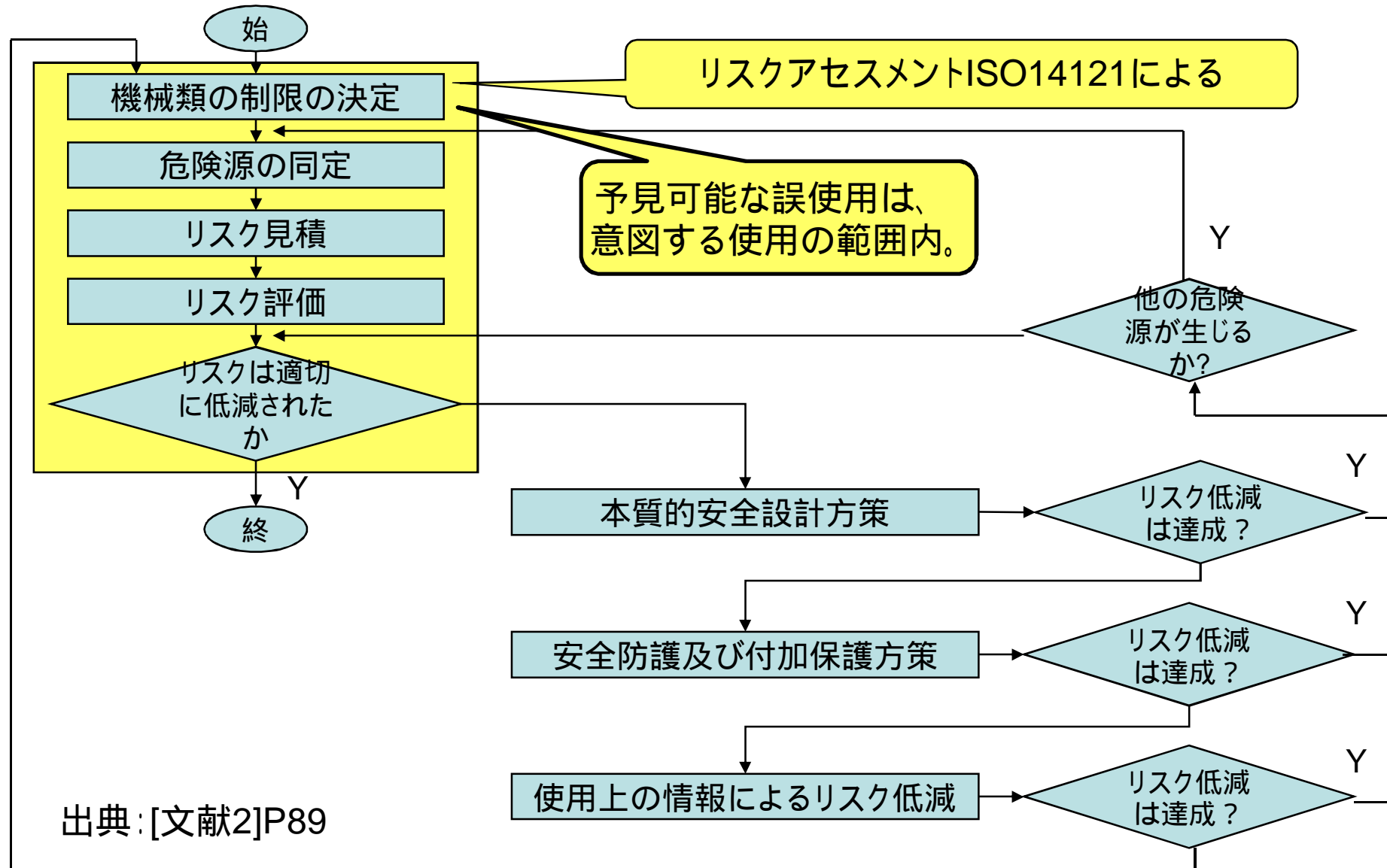


出典:[文献2]P87

本質的安全設計方策が優先する

- ◆ **本質安全性**：機械類をミスにしる故意にしる、どのように扱っても危険な状態にならない性質
- ◆ **本質安全化**には、安全防御を付加せずに、
 - **機械の運動部分に接しないようにする**(危害の発生確率を減らす)
 - 危険源を排除
 - 危険源を空間的に隔離
 - **接しても、障害が発生しないようにする**(危害のひどさを小さくする)
 - 運動要素の作動力を極小化
 - 故障時に安全側に動作するフェールセーフ設計

反復的にリスク低減を繰返さなければならない



リスク低減の達成基準

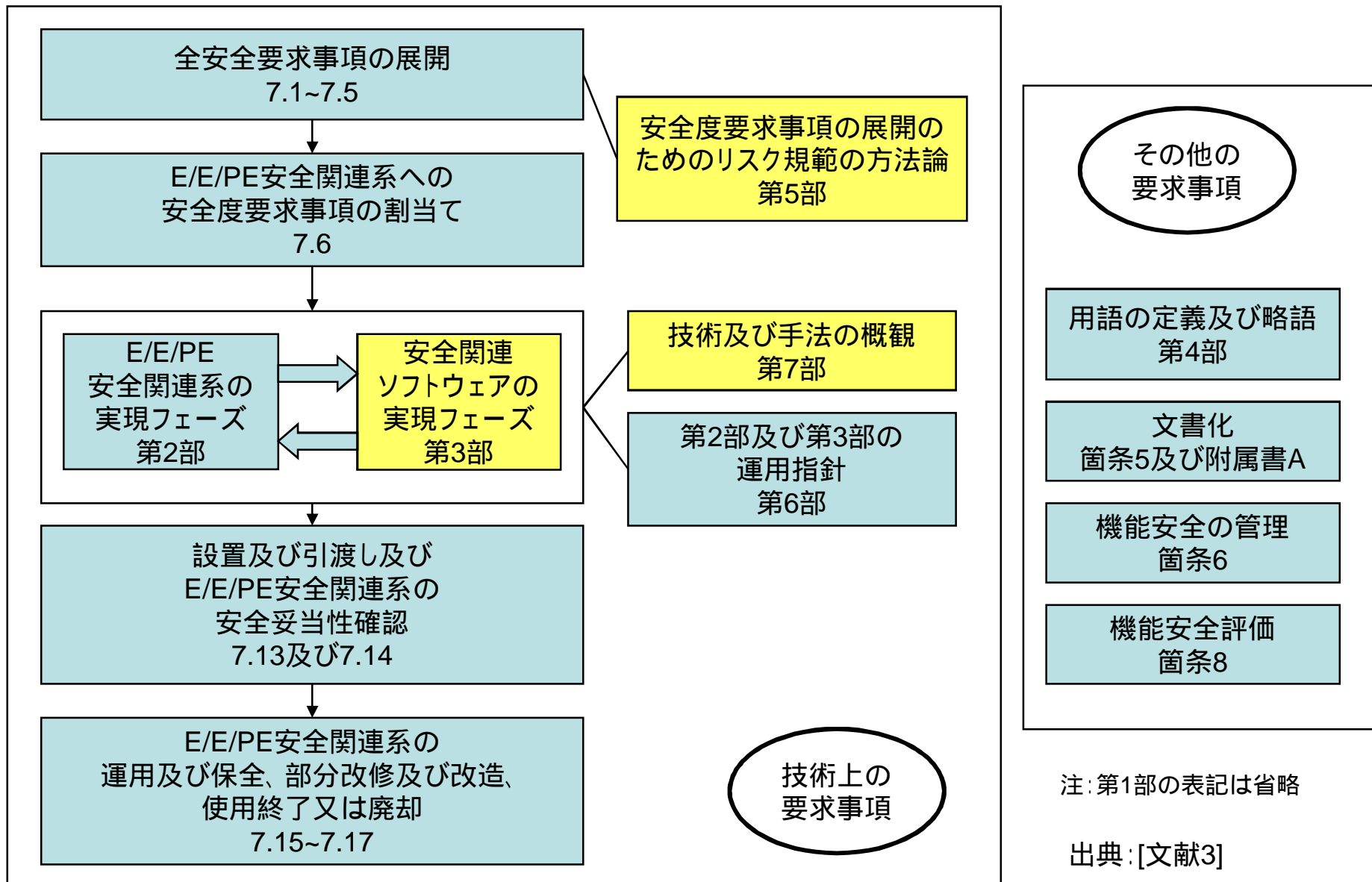
- ◆ 機械安全規格ISO12100第1部第5.5節から引用すると、次の質問にYesと回答できれば、達成できたと考えることができる
 - すべての運転条件及びすべての介入方法を考慮したか？
 - 保護法策はすべて実施したか？
 - 危険源は除去されたか、又はリスクは実現可能な最も低いレベルまで低減されたか？
 - 採用する方策によって新しく危険源が生じないのは確かであるか？
 - 使用者に残留リスクについて十分に通知し、勝つ警告しているか？
 - 保護方策の採用によってオペレータの作業条件が危うくないのは確かであるか？
 - 採用した保護方策は互いに支障なく成り立つか？
 - 専門/工業分野の仕様のために設計された機械が、非専門/非工業分野で使用されるとき、それらから生じる結果について十分配慮したか？
 - 採用した方策が機械の機能を遂行する上で機械の能力を過度に低減しないのは確かであるか？

機能安全規格：IEC61508(JIS C 0508)

- ◆ 1998年から2000年にかけて発行
- ◆ 電気・電子・プログラマブル電子安全関連系の機能安全を扱い、全7部構成 (JIS版で約350頁の分量)
 - 第1部：一般要求事項
 - 第2部：電気・電子・プログラマブル電子安全関連系に対する要求事項
 - 第3部：ソフトウェア要求事項
 - 第4部：用語の定義及び略語
 - 第5部：安全度水準決定方法の事例
 - 第6部：第2部及び第3部の適用指針
 - 第7部：技術及び手法の概観
- ◆ B規格であり、製品分野は特定しない
- ◆ 開発プロセスだけでなく、構想から廃棄までの全ライフサイクルにわたって、安全に対する要求事項を規定

リスク、安全度、設計技法の関係を学ぶ

規格群の全フレームワーク



機能安全に関する用語

- ◆ safety 安全
 - freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment
- ◆ functional safety 機能安全
 - part of the overall safety that depends on a system or equipment operating correctly in response to its inputs
- ◆ safety-related systems 安全関連系
 - systems that are required to perform safety functions
- ◆ safety functions 安全機能
 - functions to ensure risks are kept at an accepted level
- ◆ safety function requirements (what the function does) 安全機能要求事項
 - derived from the hazard analysis
- ◆ safety integrity requirements (the likelihood of a safety function being performed satisfactorily) 安全度要求事項
 - derived from a risk assessment

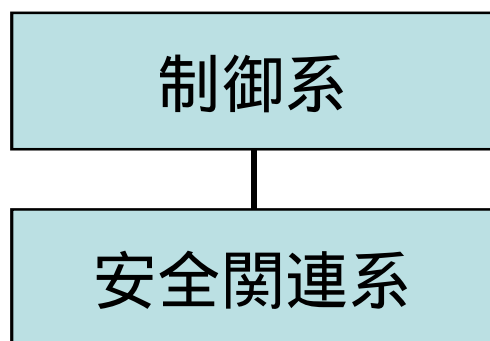
機能安全

- ◆安全関連系が正常に安全機能を実行することによって実現される安全性の一部。
 - ハードウェアだけでなく、ソフトウェアで実装された安全関連系も対象に入る(プログラマブル電子の意味)。
 - 安全機能は、リスクを許容範囲まで低減する。
 - 正常に安全機能を実行できる程度が、安全度。
- ◆リスクに応じて要求される安全機能と安全度が決まり、安全度要求を達成するには、推奨されている開発プロセス及び技法を採用しなければならない。

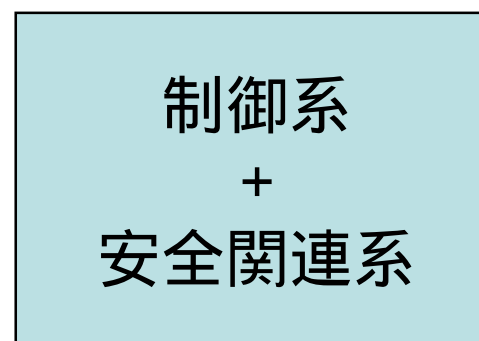
安全関連系

- ◆安全機能を実行するシステム
- ◆装置や製品の制御系と分離できない形態と、分離型に分けられる

分離型



非分離型



安全度水準

	1時間あたりの危険側故障確率 (連続モード又は高頻度作動要求運用の場合)
SIL4	10^{-9} 以上 10^{-8} 未満
SIL3	10^{-8} 以上 10^{-7} 未満
SIL2	10^{-7} 以上 10^{-6} 未満
SIL1	10^{-6} 以上 10^{-5} 未満

1年= 8760時間

11.4年= 10万時間

SIL: Safety Integrity Level

故障の分類

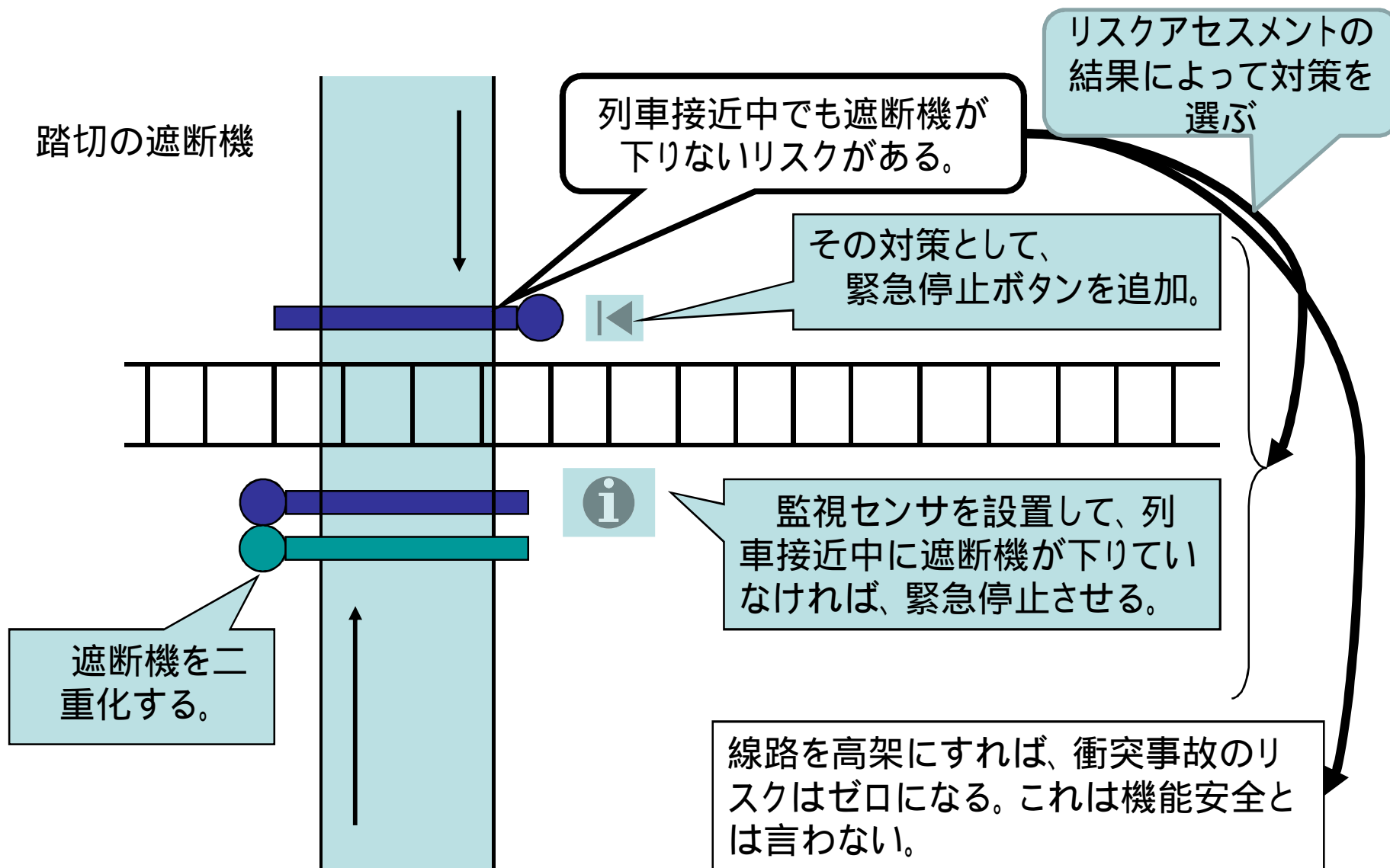
◆ 確率論的故障

- 部品や材料の劣化によって起こる故障
- ランダムハードウェア故障がその代表
- 多重化、冗長化が対策となる

◆ 決定論的故障

- 発生して初めてわかる性質の故障
- 仕様の誤りやバグがその代表
- 業務プロセスを定義して、その遵守を求めることが対策となる

機能安全の例



すべての安全要求事項フェーズの要求事項(抜粋)

- ◆ 同定された潜在危険のそれぞれに対して、要求される機能安全を確実なものにするために、必要な安全機能を定めなければならない。
- ◆ 明らかになった危険事象に対して、必要なリスク軽減を決定しなければならない。これは定量的及び/又は定性的方法で行ってもよい。
- ◆ 適用分野規格が存在し、必要なリスク軽減を直接決定する適切な方法論を提供する場合、その規格をこの箇条の要求事項に適合するように使用してもよい。
- ◆ EUC制御系による機能の失敗によって、1基以上のE/E/PE安全関連系、他技術安全関連系及び/又は外部リスク軽減施設に作動要求が生じ、かつ、EUC制御系が安全関連系としてみなされていない場合、次の要求事項のすべてを適用する。
- ◆ 前項に適合しないとき、EUC制御系を安全関連系とみなさなければならない。
- ◆ 安全度の要求事項を必要とされるリスク軽減という形式で、それぞれの安全機能に対して定めなければならない。
- ◆ すべての安全要求事項の仕様は、安全機能要求事項の仕様及び安全度要求事項の仕様で構成する。

出典:[文献3]

第3部 ソフトウェア要求事項

◆第6章 ソフトウェア品質管理システム

- 構成管理に関する規定。

◆第7章 ソフトウェア安全ライフサイクル要求事項

- フェーズごとに要求事項を規定。

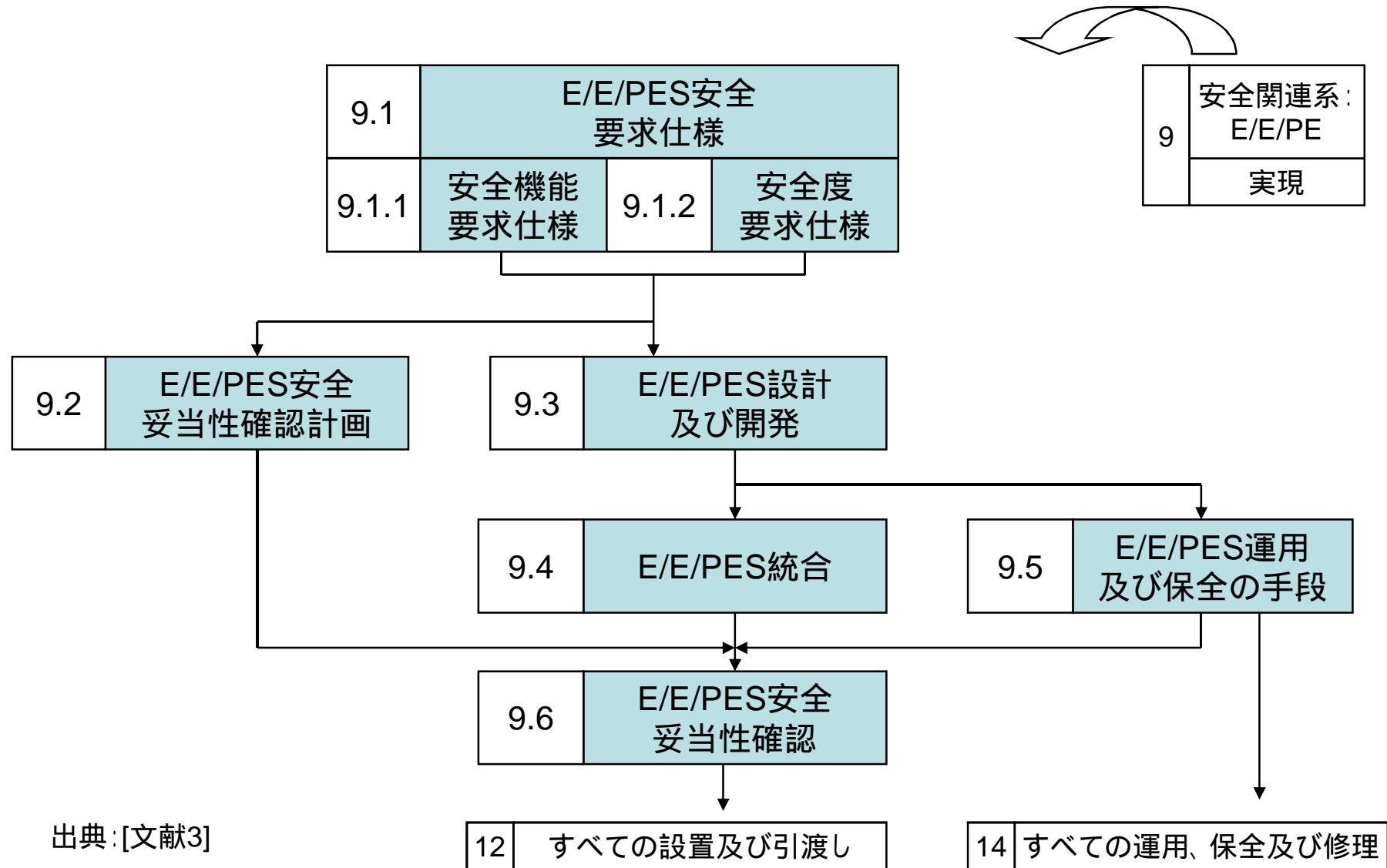
◆附属書A 技術及び手法選択の指針

- 安全度水準に対応する推奨法を一覧。
- 形式手法 (JISでは公式法と訳されている) がSIL4に推奨されている。

◆附属書B 詳細表

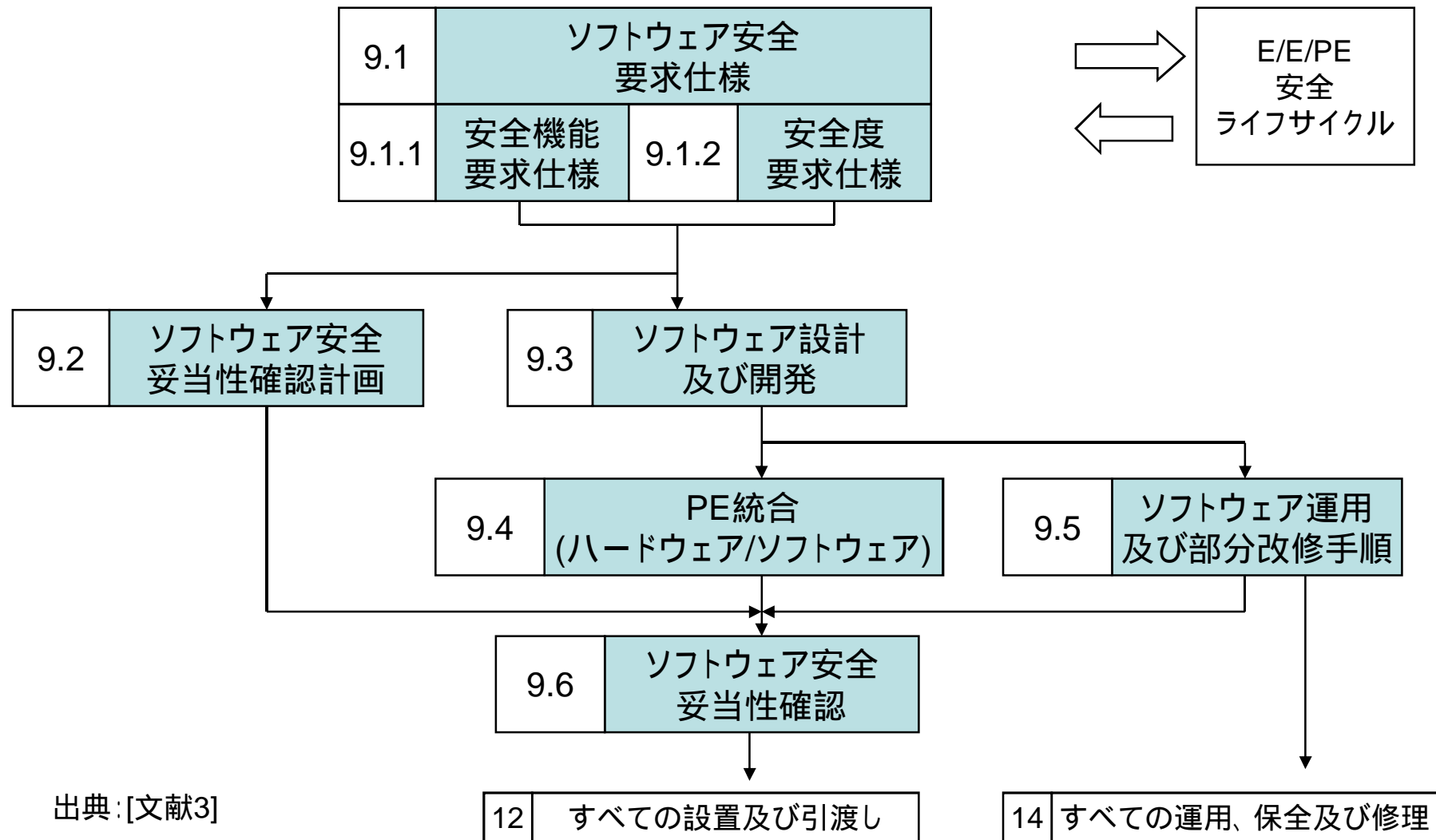
- 一部の技術及び手法の詳細版。

E/E/PES安全ライフサイクル



出典:[文献3]

ソフトウェア安全ライフサイクル



設計及び開発フェーズの要求事項(一部)

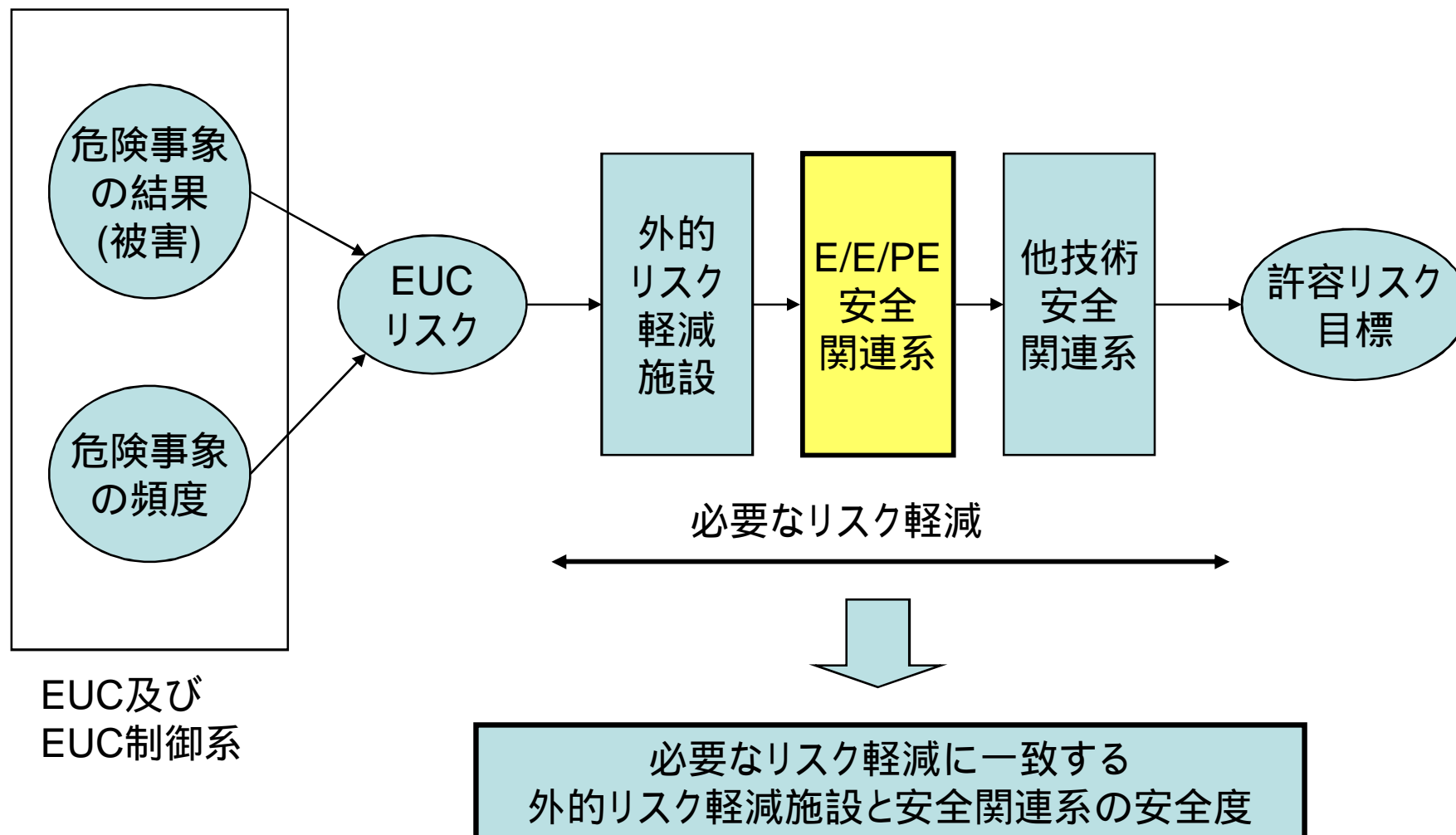
- ◆ 選択した設計法は、ソフトウェア修正を容易にする機能を持つこと。これらの機能には、モジュラー方式、情報秘匿及び要約が含まれる。
- ◆ 設計表現は明確に定義された、又は明確に定義された機能に限定した、表記法であること。
- ◆ ソフトウェアの安全関連部は、可能な限り設計によって最小限に抑えること。
- ◆ ソフトウェアが安全及び非安全機能の両方を実行する場合は、機能間の適切な独立性が設計に説明されていない限り、すべてのソフトウェアを安全関連として取り扱うこと。
- ◆ ソフトウェアが別の安全度水準の安全機能を実行する場合は、別の安全度水準の安全機能間の独立性が設計に説明されていない限り、すべてのソフトウェアはもっとも厳しい安全度水準に属するものとして取り扱うこと。
- ◆ ソフトウェア設計には、要求された安全度水準に見合った、制御及びデータの流れの自己監視を含むこと。異常検出に関して当該作動が取られること。
- ◆ 標準の、又は既に開発されたソフトウェアを設計の一部として使用する場合は、それを明確に示しておくこと。

出典:[文献3]

第5部 安全度水準決定方法の事例

- ◆ 附属書A リスクと安全度ー一般概念
- ◆ 附属書B リスクモデル(ALARP)及び許容リスクの概念
- ◆ 附属書C 安全度水準の決定:定量的方法
 - 許容リスクが数値で示されるときに有用。
- ◆ 附属書D 定性的方法によるSILの決定:リスクグラフ
 - リスク分析によってSILを決める方法のひとつ。
- ◆ 附属書E 定性的方法によるSILの決定:危険事象の過酷度マトリックス
- ◆ 附属書F 引用文献

リスク及び安全度の概念



出典:[文献3]

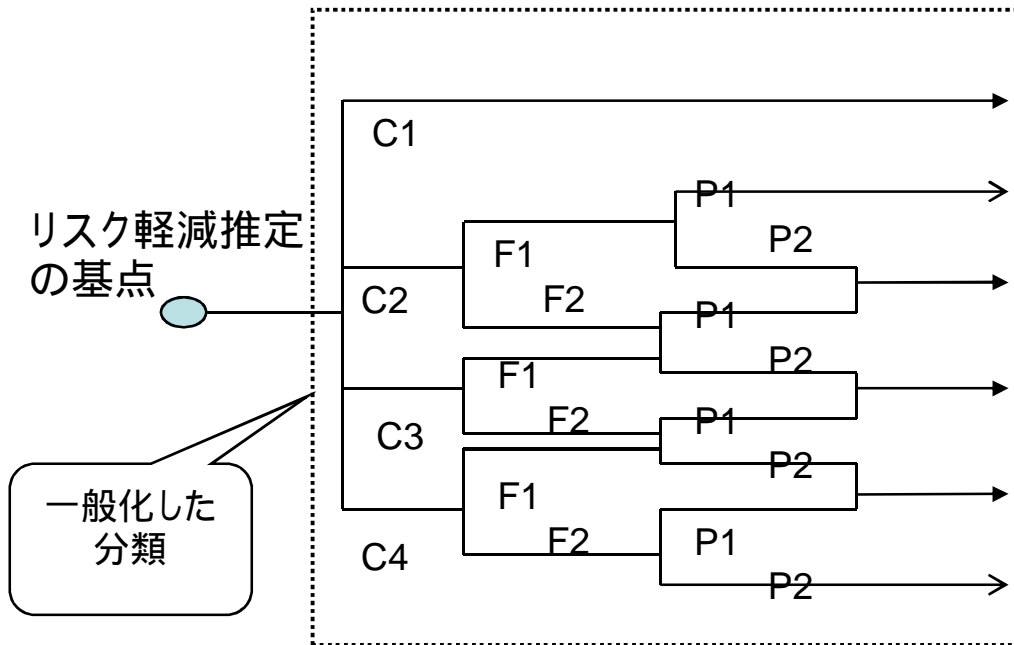
災害に関するリスクの等級化

頻度	結果			
	破局的な	重大な	軽微な	無視できる
頻繁に起こる				
かなり起こる				
たまに起こる				
あまり起こらない				
起こりそうもない				
信じられない				

リスク等級	説明
等級	許容できないリスク。
等級	好ましくないリスク。リスク軽減が非現実的すなわち、リスク軽減にかかる費用対効果費が著しく不均衡であるときだけ許容しなければならない好ましくないリスク。
等級	リスク軽減にかかる費用が得られる改善効果を超えるときに許容できるリスク。
等級	無視できるリスク。

出典:[文献3]

リスクグラフ: 定性的なSILの決定方法



	W3	W2	W1
	a	--	--
1	1	a	--
2	2	1	a
3	3	2	1
4	4	3	2
b	b	4	3

-- = 安全要求事項は全くない
a = 特別な安全要求事項はない
b = 単一のE/E/PE安全関連系では不十分
1,2,3,4 = SIL

C = 結果リスクパラメータ
F = 頻度と曝露時間リスクパラメータ
P = 潜在危険回避失敗可能性リスクパラメータ
W = 望ましくない事象の単位時間当たりの生起確率

出典:[文献3]

第7部 技術及び手法の概観

- ◆ 附属書は、第2部と第3部から引用される技術と手法を数行程度の解説で概観している。英文のまま。
- ◆ 附属書A E/E/PESにおける技術及び手法の概観：ランダムハードウェア故障の抑制
- ◆ 附属書B E/E/PESにおける技術及び手法の概観：決定論的原因故障の回避
- ◆ 附属書C ソフトウェアの安全度を達成するための技術及び手法の概観
- ◆ 附属書D 過去に開発されたソフトウェアの安全度を決定するための確率的アプローチ

MIL-STD-882D

- ◆表題： Standard practice for system safety
- ◆2000年に発行(882Cは1993年)
- ◆system safetyに関する要求事項を規定し、ガイダンスを説明している。
- ◆Appendix A: 実装のためのガイダンス

Def-Stan-00-56

- ◆表題： Safety Management Requirements
- ◆英国防衛システムのための安全管理に関する要求事項を規定
- ◆Part1:要求事項を規定
- ◆Part2:ガイダンスを説明
 - Annex BでALARPを解説。

DO-178B

- ◆ DO-178Bとは、航空無線技術委員会 (RTCA) によって作られた、米国における航空用ソフトウェアの開発用ガイドラインを定義しており、事実上の業界基準。
- ◆ DO-178Bは、主に、開発プロセスに関する規格。認証レベルは、A～Eまであり、ソフトウェアの不具合によって起こる結果をそれぞれ壊滅的、非常に危険、メジャー、マイナー或は影響なしと類別。
- ◆ ED-12Bはそのヨーロッパ版。

ISO26262

- ◆ IEC61508をベースとし、自動車を対象とする機能安全規格
- ◆ 作業中で、2008年に発行見通し
 - 04年から欧州(特に独、伊)中心に議論
 - 議長はBMW、自動車メーカーだけ
- ◆ MISRAがガイドライン(MISRA-SA)を提供する見通し

第3章 リスクアセスメント技法

- ◆ リスク識別、リスク見積及びリスク評価からリスクアセスメントは構成される。
- ◆ リスクアセスメント技法として、代表的なものに次の6種がある：
 - What-if
 - PreHA (Preliminary Hazard Analysis)
 - FMEA (Failure Mode and Effects Analysis)
 - HAZOP (Hazard and Operability Study)
 - FTA (Fault Tree Analysis)
 - ETA (Event Tree Analysis)

危険源と危険個所の違い

- ◆ リスク識別では、危険個所を抽出するのではなく、危険源を抽出しなければならない。
- ◆ 危険源は、機械類においては、人の行動と作業環境や取扱器物との組合せにより生ずる危険な状態と考えられる。
 - 自動切断装置を例にとれば、刃物は危険個所であり、異常停止時に人が刃物に触り、急に再回転した状態が危険源である。
- ◆ ISO12100では機械類の設計時に考慮すべき危険源を示し、機械的危険源として次のものを列記している：
 - 押しつぶし、せん断、切断、巻き込み、引き込み、衝撃、突き刺し、こすれ、噴出

What-if

◆特徴

- 非体系的なブレインストーミング手法
- 手順として、悪い事態を仮定し、それによって起きる事故とその安全防御を考察する
- 専門分野の異なるメンバーからなるチームで実施

◆利用分野

- 比較的単純な対象
- 体系的な手法と一緒に用いられることが多い

◆限界と弱点

- 網羅性に欠ける

PreHA

◆ 特徴

- 手順として、危険源を認識し、それが引き起こす事故の度合いとその安全防御を考察する
- 初期設計段階で弱点を取除くことが目的
- 一人又は二人で実施

◆ 利用分野

- 評価というよりリスクの分類
- 初期設計段階

◆ 限界と弱点

- 本格的なリスクアセスメントが必要となる
- 結果は実施者の力量に左右される

FMEA

◆ 特徴

- 手順として、部品の故障モードに焦点を当て、それから発生するシステム問題とその安全防御を考察する
- 個人でもチームでも実施できる
- 結果は定性的だが、故障率や重大度など、一部定量的

◆ 利用分野

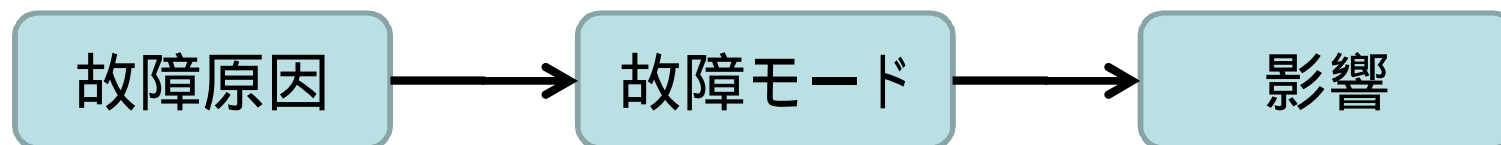
- 1950年代に軍用航空産業で開発された
- 機械系・電気系装置。特に、計画的な装置保守
- システム問題を解決するための情報収集

◆ 限界と弱点

- 故障モードを引き起こさない限り、人的エラーと外的影響を取り扱わない
- 単一の故障モードから発生する問題しか取り扱わない

故障モード

- ◆故障モードとは、部品や機器で発生する故障の状態又は故障の現象である。
- ◆故障モードには機能的、機械的、電氣的、化学的等の故障状態がある。機能的な故障モードは、たとえば次の通り：
 - 動作しない、停止しない、早く作動、遅く作動、大きすぎる値、小さすぎる値、定めた値にならない、誤操作等
- ◆故障モードは、何らかの故障原因で発生し、システムに影響を与える。



HAZOP

◆ 特徴

- 手順として、システム属性の設計意図からのずれ(逸脱)に焦点を当て、その原因、結果を双方向的に分析し、その安全防衛を考察する
- ガイドワードを用いて体系的にずれの洗い出しが可能
- 専門分野の異なるメンバーからなるチームで実施
- 結果は定性的、手法としては習得しやすい

◆ 利用分野

- 1960年代に化学産業で開発された
- 連続プロセス系、手続きや逐次処理の考察

◆ 限界と弱点

- 詳細な設計資料が必要
- すべてのずれを対象として、時間がかかる
- 単一の故障から起きる事故しか扱わない

FTA

◆特徴

- 特定の事故を装置故障、人的エラー及び外部事象の組合せとして原因究明する手法
- 表記に特殊は論理記号を用いる
- 一人で実施

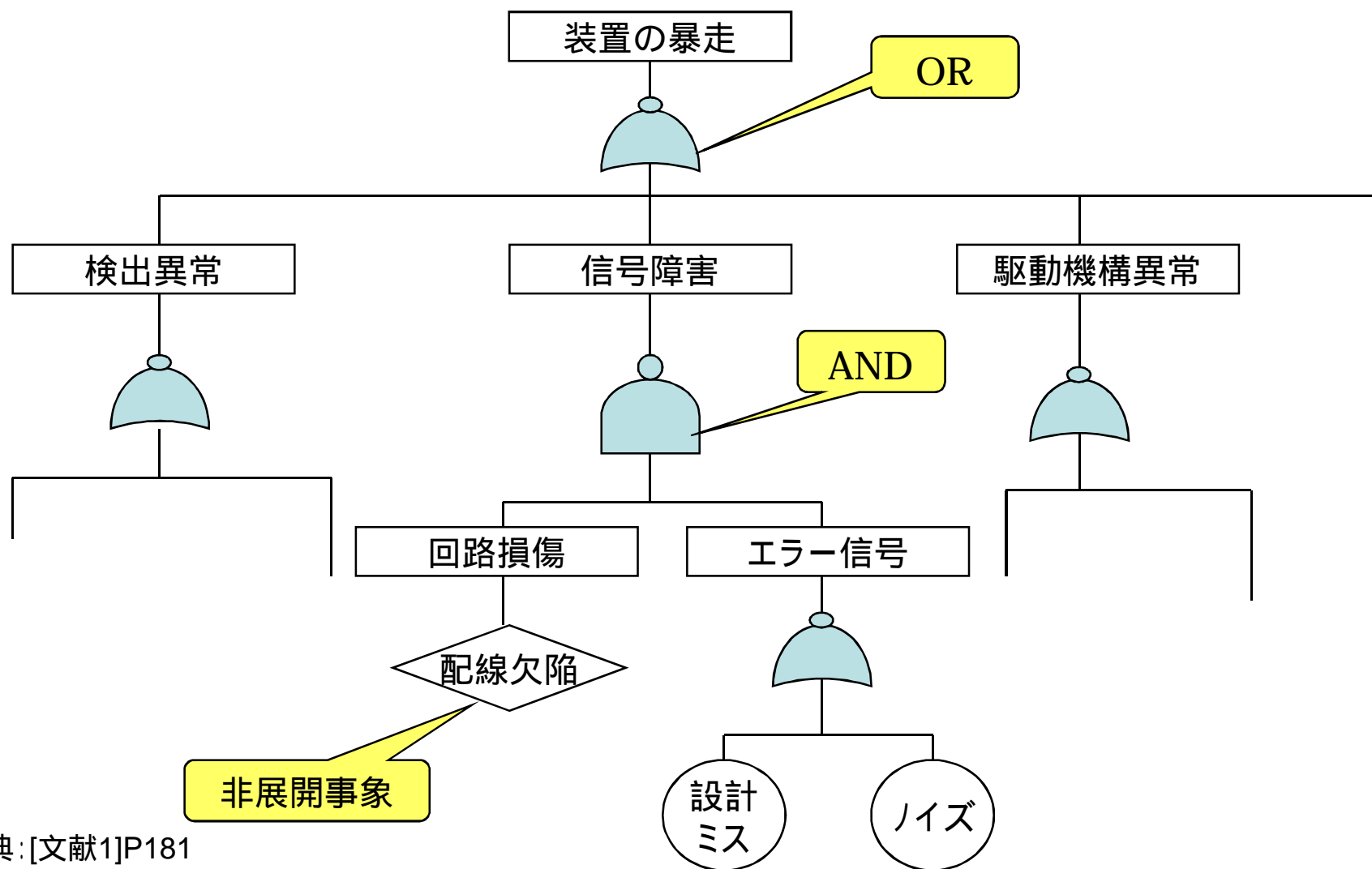
◆利用分野

- 複雑な事故の原因究明

◆限界と弱点

- ひとつの事故しか扱わない
- ツリーの作り方が分析者に依存しすぎる
- 容易に利用できる定量化は難しい

FTAによる分析例



出典:[文献1]P181

ETA

◆ 特徴

- 手順として、ある事象の発生を仮定し、その後の一連の事象を予想し、安全防御と外部影響の効果を考察する
- 一人で実施
- 多様な事故要因のタイミングやドミノ効果を扱うのに向いている

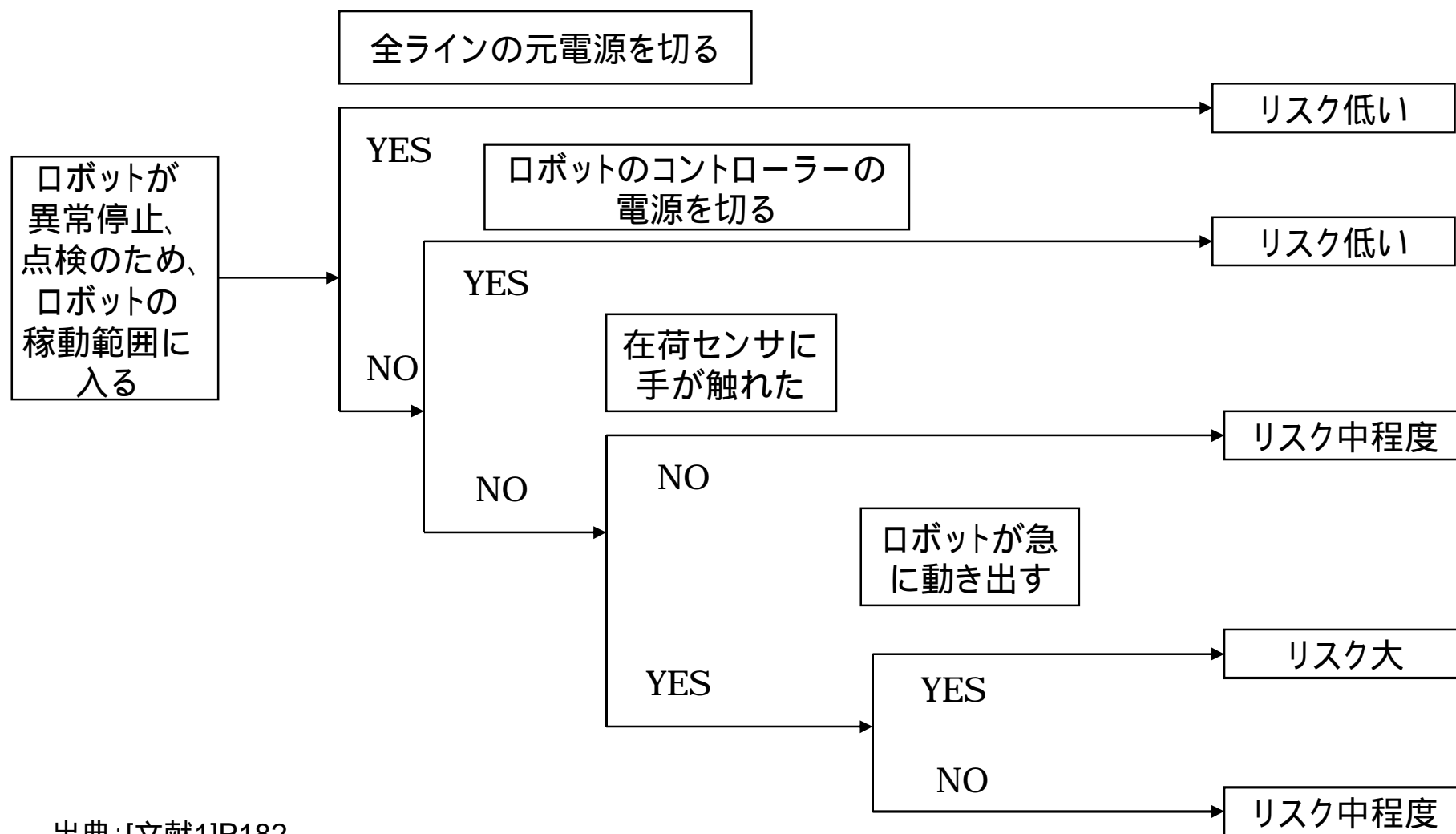
◆ 利用分野

- 複数の安全防御のあるシステムにおける事故の分析

◆ 限界と弱点

- ひとつの事象に限定され、事故原因を洗い出すことには向いていない
- 事象をたどることで条件が狭まり、リスクの洗い出しが楽観的になりやすい

ETAによる分析例



出典:[文献1]P182

リスクアセスメント技法の特徴比較

技法 比較項目	What-if	PreHA	FMEA	HAZOP	FTA	ETA
実施者	チーム	1人/2人	1人・ チーム	チーム	1人	
分析の起点	思いつき	危険源	部品の 故障	設計意図 のずれ	事故	事象
分析の目標	システムへの悪影響			原因と悪 影響	原因	悪影響の 連鎖
分析の方向	ボトムアップ			中間	トップダウ ン	ボトムアッ プ
設計資料	概略資料でも可能		詳細資料が必要			
評価基準	定性的				定量的・定性的	
表記法	特にない		表形式		論理記号	二者択一

HAZOPの手順

- ◆ 対象とするシステムと課題を定義する
- ◆ 事前準備
 - システムをいくつかの構成要素に分ける
 - 検討する設計意図からのずれを用意する
 - ワークシートを用意する
- ◆ ある構成要素のある設計意図からのずれに対して、それから引き起こされる事故を考える
- ◆ ずれの原因を考える(あるいは、その逆)
- ◆ 事故を防ぐ又は影響を緩和する安全防御を特定する
- ◆ リスク低減策等を推奨する
- ◆ すべての構成要素のすべての設計意図からのずれが終わるまで繰り返す

HAZOPのワークシート

構成要素				
ずれ	原因	結果	安全防御	リスク低減策

設計意図からのずれ

- ◆ ずれとは設計段階で想定している範囲を外れること
- ◆ システム属性とガイドワードの組として表現され、体系的に洗い出しができる
 - 例として、Flow/No

システム属性

◆ プロセス系に関する主要なものとして

- Flow
- Temperature
- Pressure
- Level
- Separate
- Composition
- React
- Mix
- Reduce
- Absorb
- Corrode
- Erode

◆ 操作性に関するものとして

- Isolate
- Vent(通気)
- Inspect
- Drain(排出)
- Purge(浄化)
- Maintain
- Start-up
- Shutdown

ガイドワード

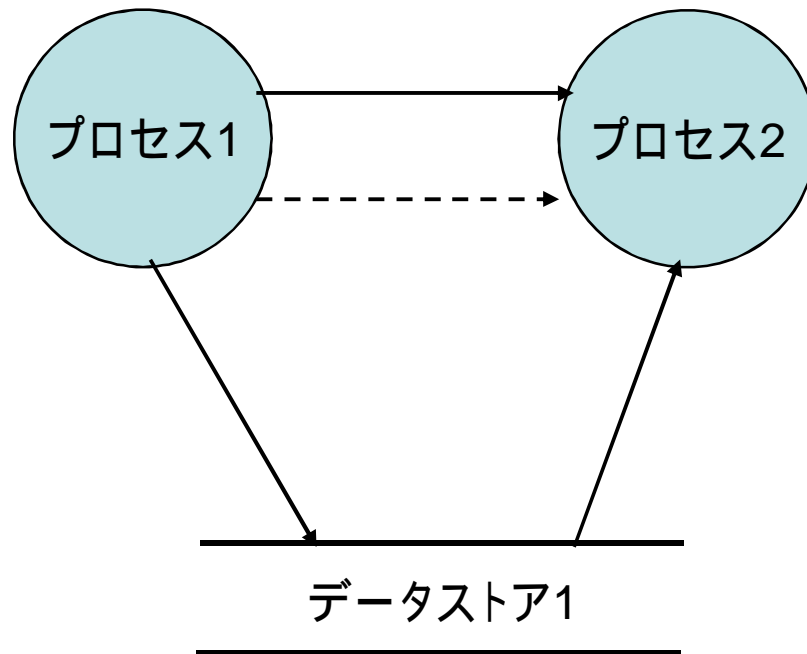
◆ 一般的属性(7種)

- No
- More
- Less
- As well as
- Part of
- Reverse
- Other than

◆ タイミング(4種)

- Early
- Late
- Before
- After

ガイドワードの解釈例



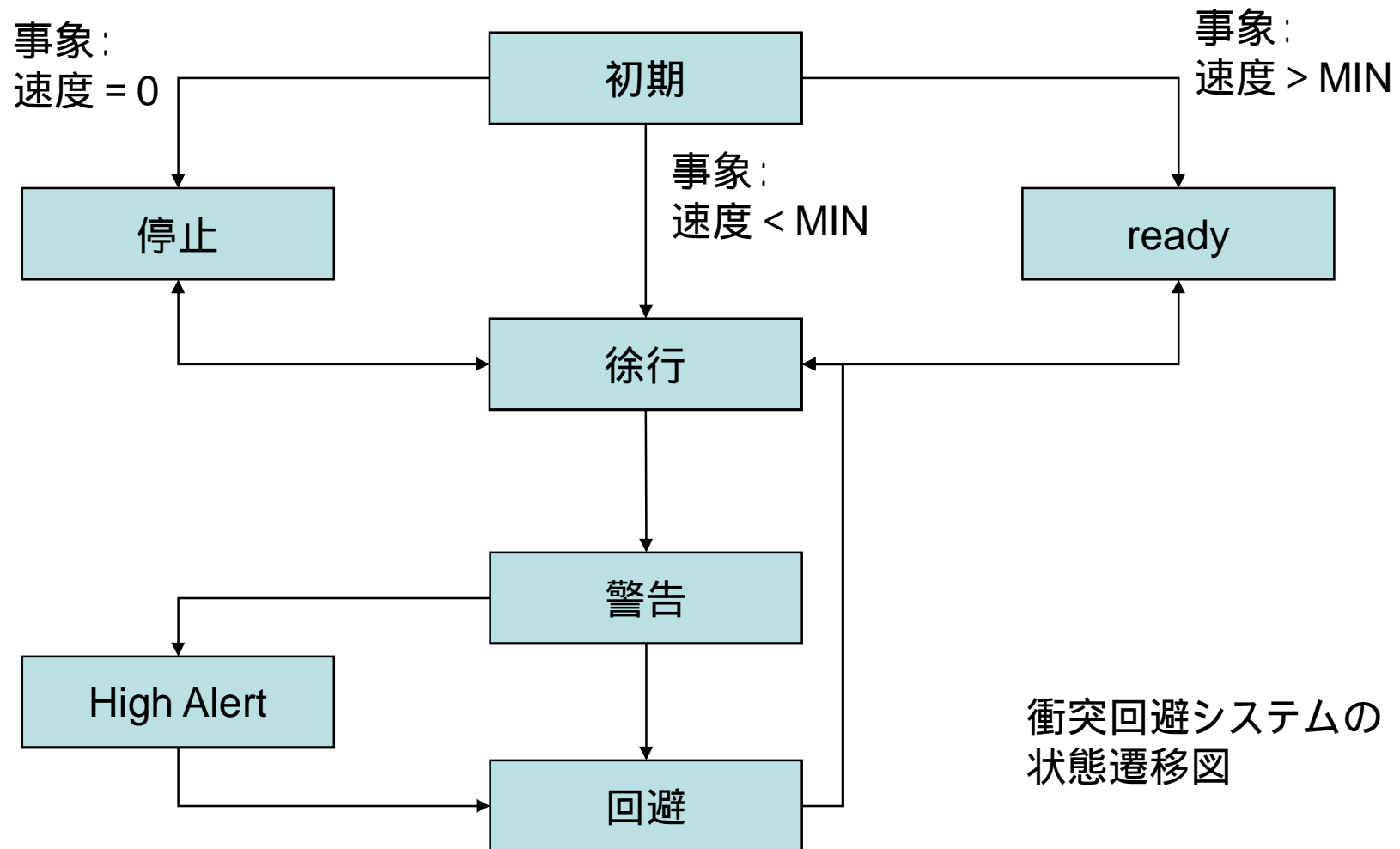
データフロー図で表現されたソフトウェア設計

属性: フロー、データ速度、データ値

ガイドワード	属性「フロー」の解釈
No	データが通過しない
More	期待以上にデータが通過
Less	
As well as	
Part of	流れる情報が未完成
Reverse	信用できない
Other than	情報が正しくない

出典: [文献4]

HAZOP解析例 (1/2)



出典:[文献4]

HAZOP解析例 (2/2)

項目	属性	ガイドワード	原因	結果
初期から徐行へ	事象： 速度 < MIN	No	速度計の故障	徐行せず、停止状態へ
			速度がゼロ	困惑し、動作は実装依存
		AS well as	惰力走行	初期化時間不足で、警告できない
		Other than	速度計が実際より低い速度を表示	アクセルの警告は危険になるかもしれない
			付加的なパルスで高い速度を表示	徐行状態に入れない
		Early/Late	初期化時間の変動	

出典:[文献4]

HAZOPに関する考察

◆ FMEAとの相違点

■ 着眼点

- (構成要素の)故障モード(FMEA)
- (構成要素間の相互作用に係る)設計意図からのずれ(HAZOP)

■ 分析手順

- 部品の故障モードを起点として分析を始め、最終的にシステムへの影響を導き出す(FMEA)
- 原因と結果の途中に位置する設計意図からのずれから分析を始め、システムへの影響とその原因を考察する(HAZOP)

◆ 連続プロセス系に適用するときの改善版

- ガイドワードによって体系的に危険源を洗い出すことができる
- 人的ミスを取り扱うことができる

◆ HAZOPの利点は、あらかじめ用意されたガイドワードを利用して、体系的に危険源を洗い出しできる点にある。ソフトウェア設計においても、データフロー図、状態遷移図、概念モデル等をもとにガイドワードを解釈すれば、適用可能である([文献4]を参照)。

第4章 リスク低減技法

- ◆ リスクアセスメントで抽出されたリスクの低減には、次の点を設計する必要がある：
 - 安全を確保するための機能(安全機能)
 - 安全機能の信頼性を向上させる手段
- ◆ 安全規格が要求する又は推奨する技法が、そのために活用できる。
- ◆ 故障やバグが多かった時代に普通に実施していた故障検出方法が、そのために有効。

安全規格が要求する設計技法

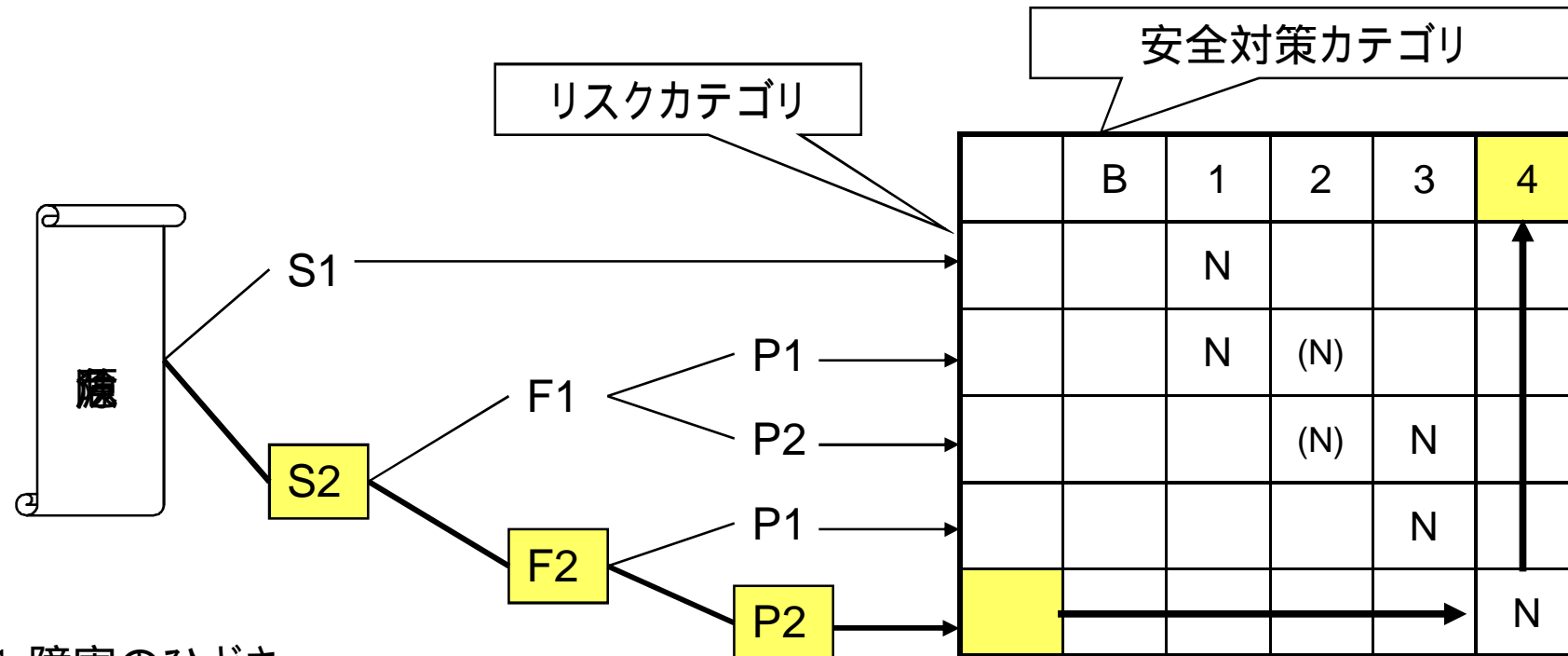
◆制御システム安全規格ISO13849-1

- リスクカテゴリに応じて安全カテゴリが決まり、設計要件を規定する。

◆機能安全規格IEC61508

- リスクの程度に応じて安全要求(安全機能と安全度水準)が決まり、その安全度水準に応じた設計技法の適用が求められる。

ISO13849-1に基づくリスク評価と安全対策



S: 障害のひどさ

F: 頻度

P: 回避可能性

出典:[文献1]P32,34

安全対策カテゴリ	要件の概要
B	安全関連部の目的機能を実現する
1	高信頼性の部品を使用する
2	安全機能が適当な間隔でチェックされる
3	安全機能が二重化される
4	安全機能が連続的に監視される

危険検出と安全検出の違い

	危険検出システム	安全検出システム
安全機能	危険な状態が発生すると、それを検出できる。	安全な状態にあることを検出できる。
安全機能の維持能力	事前にチェックできないので、欠陥時に安全機能が常に働く保証はない。	定期的にチェックすることによって、欠陥発生時に安全機能が働くことをある程度保障できる。
安全対策カテゴリ	レベル1に対応	レベル2に対応

フェールセーフ設計

- ◆安全対策カテゴリ4に対応できる技法
- ◆故障が発生しても、人には危害を加えないようにする設計。こういう故障を安全側故障と呼ぶ。
- ◆基本原理
 - 故障したときには必ず一方向に陥るようにする(非対称故障)
 - 安全情報の伝達は、必ず安全情報をもとにして行う。

非対称故障の例: 上にあるときが危険状態で、下にあるときが安全状態とすれば、故障すれば、重力によって必ず下に落ちる。

出典:[文献1]P57

IEC61508推奨の設計技法(一部)

ソフト方式設計での推奨技法	SIL1	SIL2	SIL3	SIL4
故障検出及び診断		R	HR	HR
エラー検出及びコード修正	R	R	R	HR
アサーションプログラミング	R	R	R	HR
安全バグ技術		R	R	R
ダイバースプログラミング	R	R	R	HR
リカバリブロック	R	R	R	R
後方修復	R	R	R	R
前方修復	R	R	R	R
故障修復機構の再試行	R	R	R	HR
実行作業の記録		R	R	HR
グレースフル デグラデーション	R	R	HR	HR
構造化手法	HR	HR	HR	HR
半形式手法	R	R	HR	HR
形式手法		R	R	HR
コンピュータ支援仕様ツール	R	R	HR	HR

安全度水準

R: 推奨

HR: 強く推奨

Assertion programming

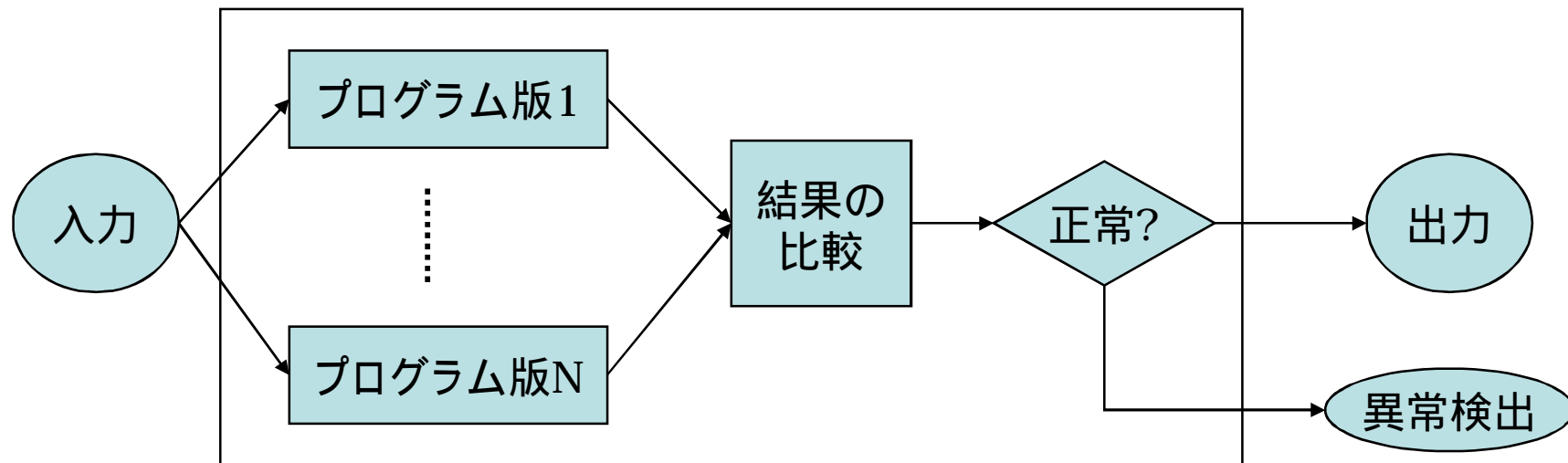
- ◆ プログラムの実行時に、その事前条件と事後条件をチェックする。
- ◆ プログラムの欠陥を実行時に検出できる。

For example,

```
assert < pre-condition>;  
action 1;  
  ⋮  
  ⋮  
action x;  
assert < post-condition>;
```

Diverse programming

- ◆設計と実装を変えて、同じ仕様に対して数本のプログラムを作成。同時に実行させて、その結果を比較する。
- ◆プログラムの欠陥を実行時に検出できる。



防衛的プログラミング

- ◆ 変則的な制御フロー、データフロー、データ値等を検出して、それに対処できるプログラムを作成する手法。具体的には：
 - 入力変数の確からしさをチェックする。
 - 出力変数の効果を、できれば関連するシステム状態の変化を調べて、チェックする。
 - 必要なハードウェアの存在、自身の完全性などソフトウェア構成をチェックする。
 - 手続きの入り口でそのパラメータの型、次元、値域をチェックする。
 - read-onlyとread-writeのパラメータを分離しておき、そのアクセスをチェックする。

設計及びコーディング規約

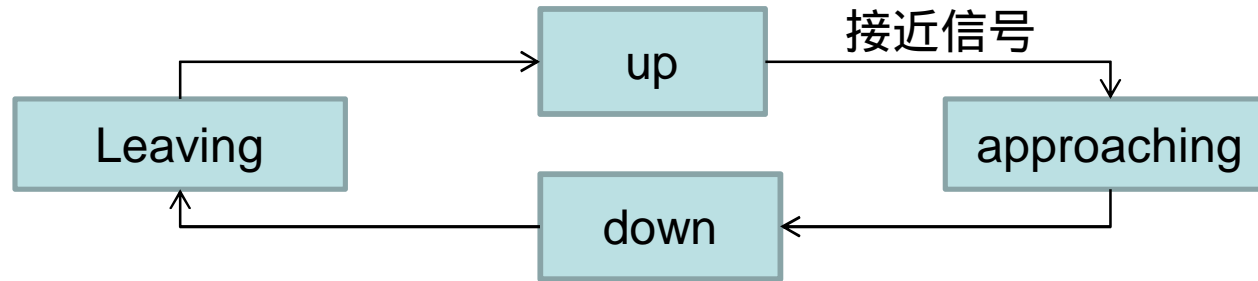
- ◆ソフトウェア詳細設計に関する推奨技法に取り上げられている。具体的には：
 - 動的オブジェクトを使わない。
 - 動的変数を使わない。あるいは、割当て時にチェックする。
 - 割込みの使用を制限する。
 - ポインタの使用を制限する。
 - 再帰呼出しの使用を制限する。
 - 無条件jumpを使用しない。

故障やバグが多かった時代には、

- ◆重要なデータ領域にはチェックサムをつける。
- ◆watch dog timerが正常に作動するかを定期的に確認する。
- ◆起動時に、実行周期がおかしくないかをチェックする。
終了時に、処理時間が異常でないかをチェックする。
- ◆下位モジュールが正常に機能しているかを定期的にチェックする。

練習問題:踏切の遮断機(リスク識別、見積)

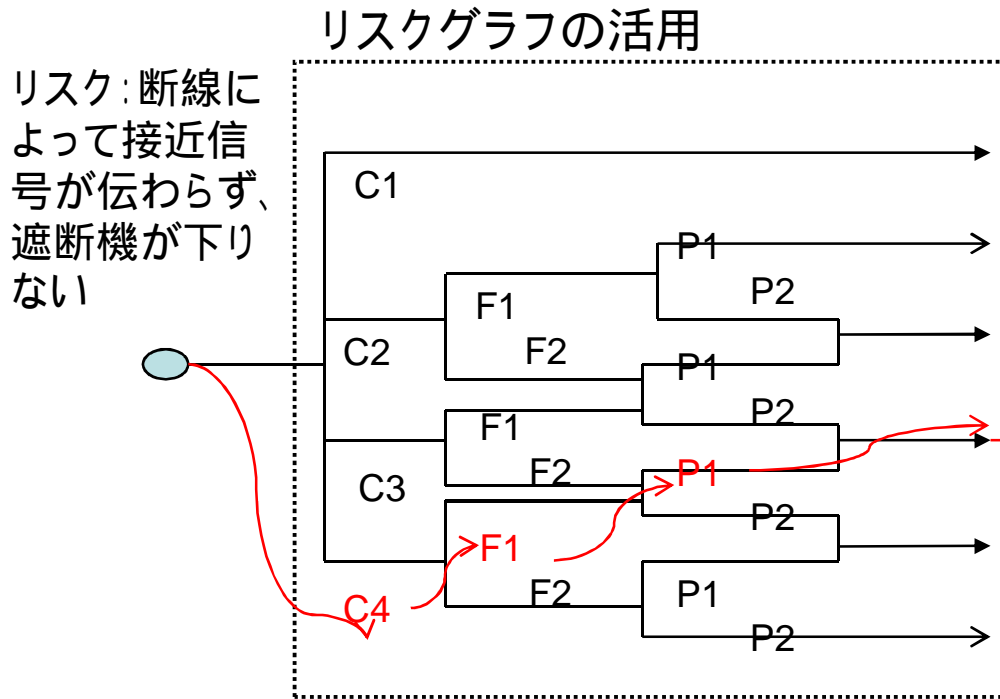
状態遷移図



HAZOP分析

項目	属性	ガイドワード	設計意図からのずれ	原因	結果
up から approaching への遷移	事象: 接近信号	No	接近信号が伝達されない	断線 電源断	遮断機が下りない
		More	接近信号が続けて伝達される		approachingでは接近信号を無視する
		Part of	接近信号が途中で切れる	信号機の出力量不足	遮断機が下りない
		Reverse	電車が接近していないのに受信	センサに異物付着	不必要に遮断機が下りる
		Other than	退去信号を受信		無視する

練習問題:踏切の遮断機(リスク評価)



W3	W2	W1
a	--	--
1	a	--
2	1	a
3	2	1
4	3	2
b	4	3

-- = 安全要求事項は全くない
 a = 特別な安全要求事項はない
 b = 単一のE/E/PE安全関連系では不十分
 1,2,3,4 = SIL

C = 結果リスクパラメータ
 F = 頻度と曝露時間リスクパラメータ
 P = 潜在危険回避失敗可能性リスクパラメータ
 W = 望ましくない事象の単位時間当たりの生起確率

第5章 安全設計への取組み方法

- ◆設計者個人の力量依存から体系的、組織的な取組みへの脱皮
- ◆規格認証を取得している部品、ツールの活用
- ◆ガイドライン、支援サービスの活用
- ◆既に発行、公開されている資料の調査活用

従来の設計と安全設計の相違

設計者が 考慮すべき事項	従来設計	安全設計
設計方法	個人的な工夫	体系的に進めなければならない
設計思想の基準	信頼性	安全に対するリスク
考慮すべき時期	操業、保全時	製造～試運転～操業～廃棄
安全対策	安全機器を付加的 につければよい	本質安全化
災害責任	使用者のみ	設計者も含まれる

出典:[文献1]P4

規格認証を取得している部品、ツール等

- ◆ 2005年2月、形式手法ツールSCADEの発売
 - DO-178B、IEC61508認証取得済み
- ◆ 2005年4月、セーフティネットワークの発売
 - IEC61508のSIL3に対応
- ◆ 2006年8月、温度伝送器が安全規格取得
 - IEC61508のSIL2に対応
- ◆ DO-178B認証取得済みのRTOS
 - 米国Wind River Systems、VxWorks(航空宇宙用)
 - 米国Green Hills Software、INTEGRITY
- ◆ 名古屋大学組込みシステム研究センター(NCES)とヴィッツが、TOPPERSをもとにIEC61508対応の車用のプラットフォームを3年計画で開発中(2006年現在)

ガイドライン、支援サービス

- ◆ MISRA安全性解析ガイドライン
 - 自動車用のISO26262用
 - 2006年6月、SESSAMEが英国から専門家を招き、セミナーを開催
- ◆ 株式会社日本機能安全の支援サービス
 - 2006年4月設立。東芝OBが関与。ガイアグループの一員。
 - 教育研修
 - IEC61508適合支援、認証支援
- ◆ 東洋エンジニアリングの潜在ハザード解析支援
- ◆ 千代田化工建設のリスク評価・低減サービス
- ◆ IDECのもの作り安全コンサルティングサービス

規格に関する書籍

国際規格等	JIS	日本規格協会からの出版物等
ISO12100-1/-2	B9700-1/-2	対訳本 ISO12100-1/12100-2:2003、¥2940(市販) JIS規格書、¥2500、¥2900 ISO原本、¥12295、¥11718
ISO14121	B9702	JIS規格書、¥1700 ISO邦訳、¥8400
ISO13849-1/-2	B9705-1	JIS規格書、¥2310 ISO邦訳、¥16170、¥23205
IEC61508	C0508	JIS規格書第1部から第7部まで、各部約3000円 IEC邦訳第1部から第7部まで、各部約2万円
MIL-STD-882D		邦訳、¥22575
IEC62304		邦訳、¥39900

規格に関する資料

◆ IEC

- IEC61508 Part-0のドラフト版。
- http://www.iec.ch/zone/fsafety/pdf_safe/hld.pdf

◆ 英国

- Def Stan 00-56
- <http://www.dstan.mod.uk/data/00/056/01000300.pdf>
- <http://www.dstan.mod.uk/data/00/056/02000300.pdf>

◆ 米国

- MIL STD 882D
- <http://www.safetycenter.navy.mil/instructions/osh/milstd882d.pdf#search=%22MIL%20STD%20882D%22>

安全設計技法に関する書籍

- ◆ グローバルスタンダード時代における実践FMEA手法、小野寺勝重著、日科技連出版社、¥3150
- ◆ 国際標準化時代の実践FTA手法、小野寺勝重著、日科技連出版社、¥3150
- ◆ FMEA・FTA実施法—信頼性・安全性解析と評価、鈴木順二郎著、日科技連出版社、¥2940
- ◆ Q&Aでわかるリスクベース設計のポイント、堀田源治他著、日刊工業新聞社、¥2200
- ◆ DesignWaveマガジン2006年12月号、CQ出版社、¥1257
- ◆ **System Safety: Hazop and Software Hazop**、F.Redmill他著、John Wiley & Sons Ltd、¥17290
 - 第7章、ソフト設計でのガイドワードの使い方
 - 第11章、FMEAとの使い分け
 - 第13章、医療診断システムの事例
 - 第15章、ソフト設計への適用例2件

関連団体(海外)

- ◆ IEC Functional Safety Zone
 - http://www.iec.ch/zone/fsafety/fsafety_entry.htm
- ◆ MISRA: The Motor Industry Software Reliability Association
 - <http://www.misra.org.uk/>
- ◆ RBDM: Risk-based Decision-making Guidelines
 - リスクアセスメントのツールを広く解説
 - <http://www.uscg.mil/hq/gm/risk/E-Guidelines/Tools.htm>
- ◆ Isograph
 - 信頼性に関するソフトの販売
 - <http://www.isograph.com/index.htm>
- ◆ PrimaTech
 - HAZOP等のソフトの販売、コンサル、トレーニング
 - <http://www.primatech.com/index.html>
- ◆ UK Defence Standardization
 - <http://www.dstan.mod.uk/>
- ◆ Green Hills Software
 - DO-178B対応のRTOS提供
 - <http://www.ghs.com/>

関連団体(国内)

- ◆ 安全工学会
 - 安全工学に関するNPO
 - <http://www.soc.nii.ac.jp/jsse3/index.html>
- ◆ 高度システム安全学研究室
 - 岡山大学の研究室、HAZOPを取り扱う
 - <http://syslab2.mech.okayama-u.ac.jp/safelab-j/index.htm>
- ◆ 東洋エンジニアリング
 - 潜在ハザード解析支援
 - <http://www.toyo-eng.co.jp/jp/Technology/safety/index.html>
- ◆ 化学工業会
 - 安全部会
 - <http://www2.scej.org/anzen/index.html>
- ◆ (株)日本機能安全
 - IEC61508適合支援、教育研修サービス
 - <http://www.jf-safety.co.jp/index.html>
- ◆ IDEC
 - ものづくり安全コンサルティングサービス
 - http://idec.com/jpja/technology_solution/safety/index.html

関連団体(国内、その2)

- ◆ ウィンドリバー
 - 規格準拠のRTOSを提供
 - http://www.windriver.com/japan/products/safety_critical/index.html
- ◆ SESSAME
 - 育成カリキュラム整備、方法論・ツールの開発
 - <http://www.sesame.jp/>
- ◆ 名古屋大学組込みシステム研究センター
 - RTOSの研究開発
 - <http://www.nces.is.nagoya-u.ac.jp/>
- ◆ 千代田化工建設
 - リスクアセスメント支援
 - <http://www.chiyoda-corp.com/biz/j/aes/mente/rrm/index.shtml>
- ◆ 信越化学工業
 - HAZOP採用
 - <http://www.shinetsu.co.jp/j/profile/kankyo.shtml>
- ◆ 日本防災システム協会
 - HAZOP研修会を開催
 - <http://www.bosai-system.jp/action.html>

引用文献

- ◆[文献1] Q&Aでわかるリスクベース設計のポイント、堀田源治他著、日刊工業新聞社
- ◆[文献2]ISO12100-1/12100-2機械安全の国際規格、日本規格協会
- ◆[文献3]JIS C 0508規格書、日本規格協会
- ◆[文献4] **System Safety: Hazop and Software Hazop**、F.Redmill他著、John Wiley & Sons Ltd

まとめ

- ◆安全とは、人体に危害を与えるリスクが許容限度まで低減されている状態である。
- ◆安全に関する国際規格として、機械安全ISO12100、機能安全IEC61508があり、安全に関する基本概念と方法論の習得に有益である。
- ◆安全設計とは、リスクを識別し、評価し、許容限度までリスクを低減することである。
- ◆リスクアセスメント技法の中でHAZOPは、ソフトウェア設計にも適用できる可能性がある。
- ◆リスク低減技法はまだ整備されていないが、安全要求度に応じて選択しなければならない。
- ◆安全設計には設計者個人の力量依存ではなく、体系的、組織的な取組みが必要である。