新たな安全設計手法を用いた
鉄道信号の設計安全性評価に関する取組

交通システム研究部　主任研究員　工藤　希

はじめに

交通安全環境研究所では、海外向け鉄道システムの設計安全性評価に関し、

- これまでの実績に基づき、国際規格との調和や規格適合性評価等との関連について検討してきた
- 複雑化した鉄道信号システムに対応するためには、従来の安全性評価手法に加え、近年提案された新しい評価手法の活用が有効と考えられるため、試行した

第三者安全性評価の位置づけ

- 鉄道システムの輸出に際し、その安全性を相手先に証明する方法として、機能安全関連の国際規格への適合性について第三者評価及び認証を受けることが一般化

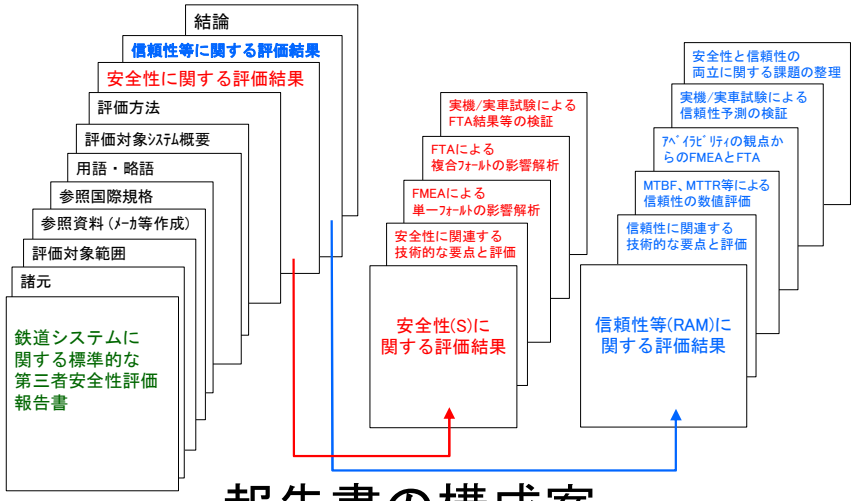
- 第三者評価には、規格適合性評価、認証と、本発表で述べる技術的な安全性評価に大別される
- 第三者による技術的な安全性評価も、機能安全性関連の国際規格を参照して行われることが多い

参照する国際規格の一例

規格番号	規格名・通称
IEC 62425	鉄道信号用安全関連電子装置の安全性証明
IEC 62278	鉄道におけるRAMS
IEC 62279	鉄道信号システムのソフトウェアの安全性
IEC 62280	鉄道信号システムの通信の安全性
IEC 62236	鉄道システムのEMC（電磁両立性）

設計安全性評価の位置づけ

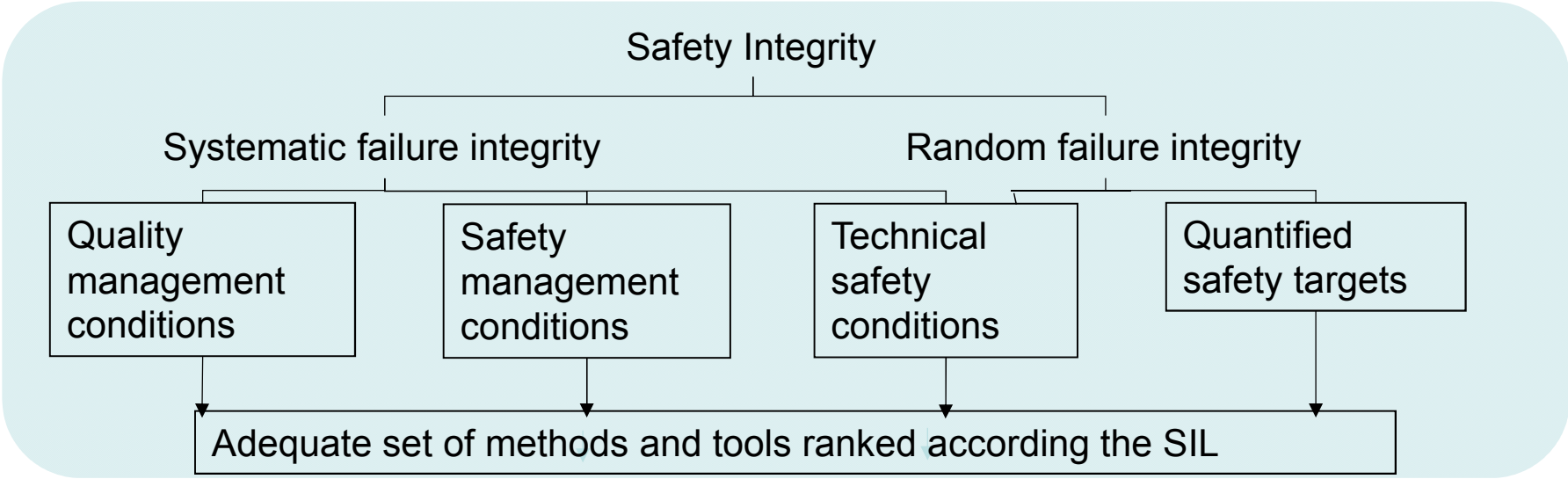
- 設計安全性評価は、システムの技術内容及び設計仕様等に対し、リスク分析に基づいた定量的評価や、システムの安全管理にかかわる定性的な評価などを行なうもの
- IEC 62425及びIEC 62278を重点的に参照し、これらの規格との整合を図った安全性評価報告書の構成案をこれまでの研究で提案してきた



報告書の構成案

安全度水準

- IEC 62425における安全度水準SIL（Safety Integrity Level）は4段階定義されており、そのうち最高水準のSIL4において定量的な必要要件とされる非安全事象の発生頻度は1×10^{-9}～10^{-8}/hとされている
- 一般的に鉄道の列車制御システム及び信号システムに対してはSIL4を達成することが要求されるため、各要素又はシステム全体における非安全事象の発生頻度がSIL4を達成するか否かを主要な判断基準とする



設計安全性評価で利用する評価手法

FMEA（Failure Mode and Effects Analysis）:
システムに起こりうる故障モードを予測し、考えられる原因や影響を事前に解析・評価する手法

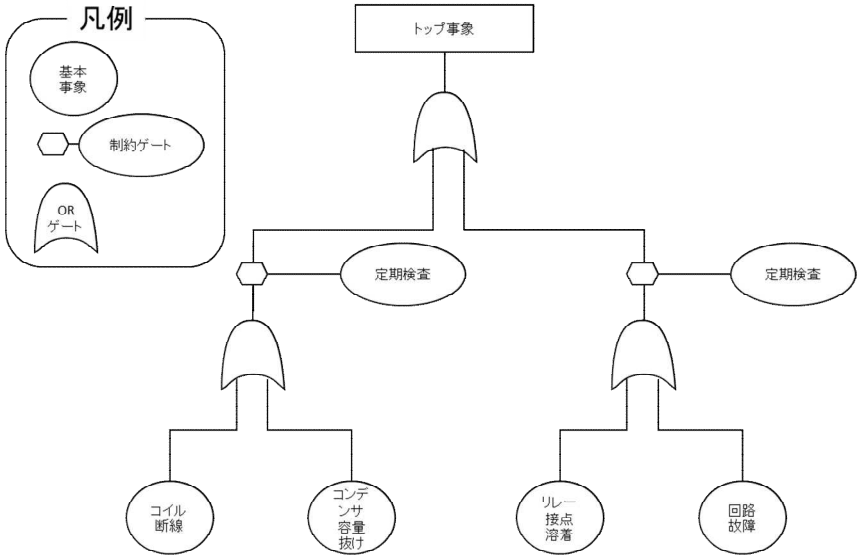
FMEAの例

アイテム	機能	故障モード	故障影響	故障原因	対策前			低減策	対策後		
					頻度	深刻度	リスクレベル		頻度	深刻度	リスクレベル

設計安全性評価で利用する評価手法

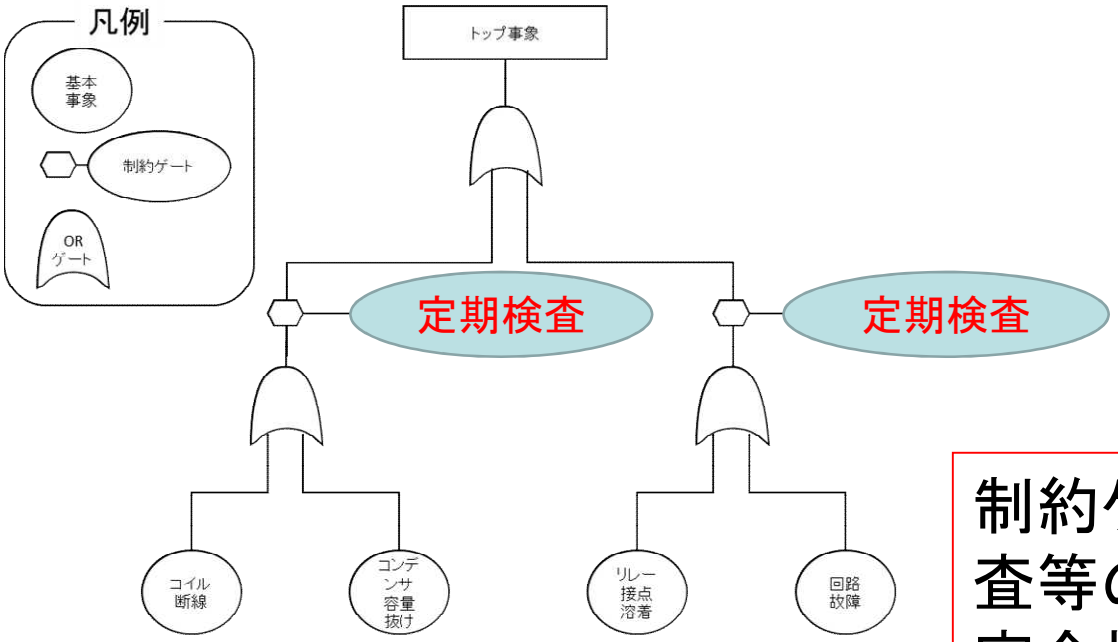
FTA（Fault Tree Analysis）:

発生が好ましくない事象に対して、その事象を引き起こす要因を連鎖的に展開し、因果関係を樹形図に図示し、対策を打つべき発生経路および発生要因、発生確率を解析する手法



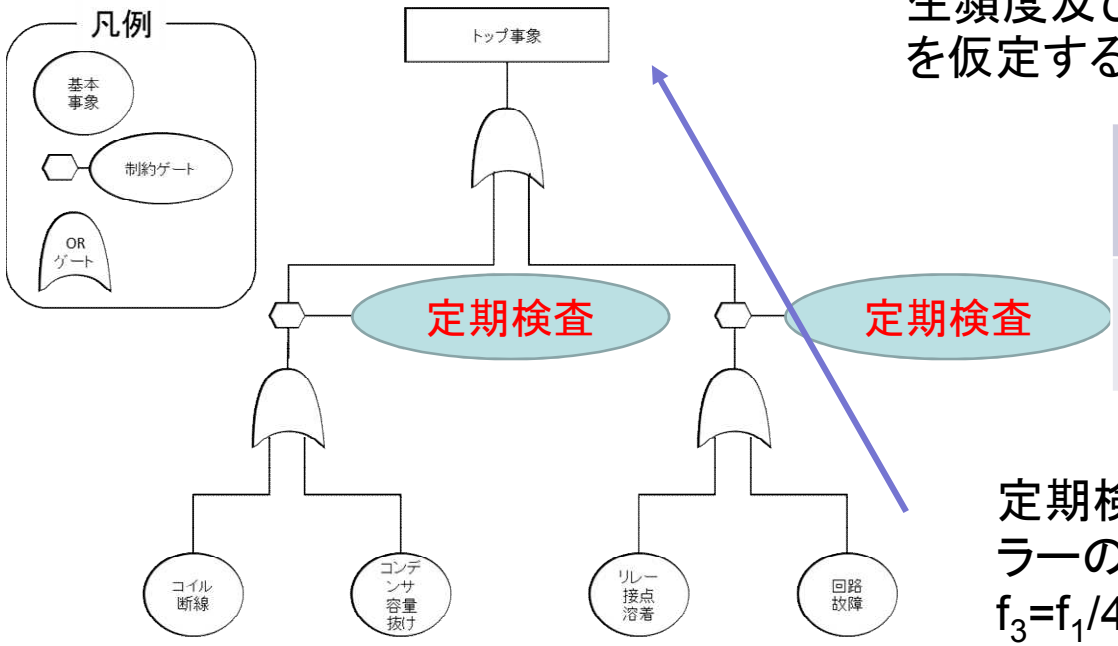
FTAの例

【FTAの例】定期検査におけるヒューマンエラー発生確率



制約ゲートとして、定期検査等の防護しなければ、安全性の水準を達成できないケースも

【FTAの例】定期検査におけるヒューマンエラー発生確率



仮に下表のように、基本事象の発生頻度及びトップ事象の発生頻度を仮定すると

トップ事象の発生頻度(f_1)	1×10^{-9}/h
基本事象の発生頻度(f_2)	1×10^{-6}/h

定期検査におけるヒューマンエラーの発生確率(f_3)は

$f_3=f_1/4f_2$

$=2.5\times10^{-4}$

以下に抑えることが求められる

【FTAの例】定期検査におけるヒューマンエラー発生確率

- 一方、一般的には定例作業時のエラー発生率は0.01～0.00001とされているので、前述の逆算により求めた結果は妥当と判断できる
- 但し、このエラー発生率は教育・訓練がきちんと行われていることが前提であり、特に海外向けの評価においては、この前提を明示しておくことが必要

意識のモード	生理的状態	エラー発生確率
正常、リラックスした状態	休息時、定例作業時	0.01～0.00001
正常、明晰な状態	積極的活動時	0.000001以下
興奮状態	慌てている時、パニック時	0.1以上

引用）中條武志，“人間信頼性工学：エラー防止への工学的アプローチ”，
http://www.indsys.chuo-u.ac.jp/~nakajo/open-data/Healthcare_Errorproofing2.pdf

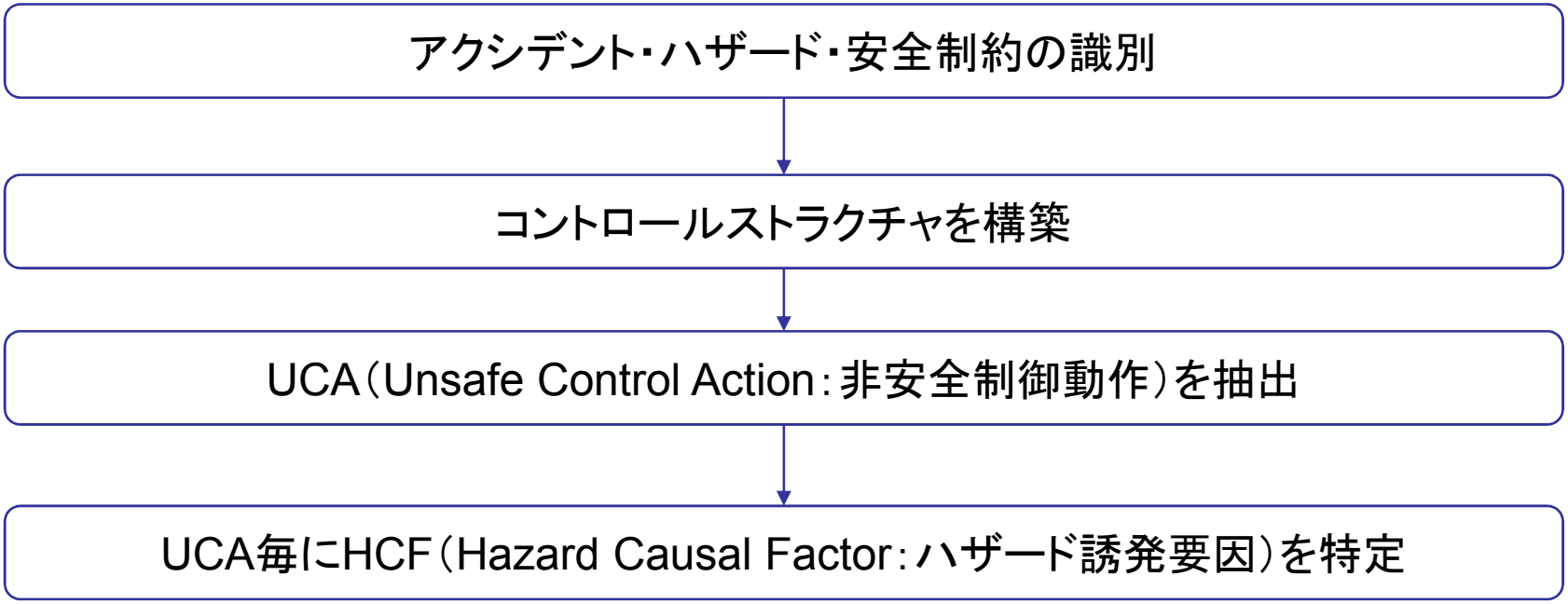
STAMP/STPA

- STAMPは2012年にマサチューセッツ工科大学のLeveson教授が提唱した安全解析手法
- これまでのFTA/FMEAでは機器の相互作用及び時間的遷移を伴うなどの複雑な事象の解析が難しい

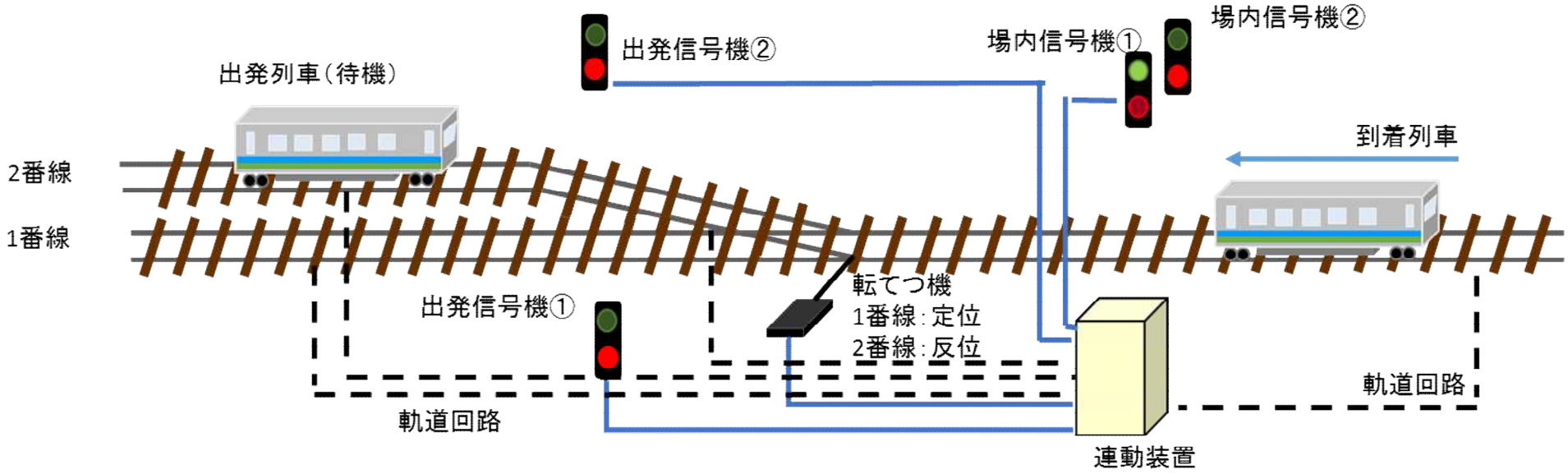
	FMEA/FTA	STAMP/STPA
手順	FMEAにより、システムに起こりうる故障モードを予測し、考えられる原因や影響を事前に解析・評価し、その結果、発生が好ましくない事象に対して、FTAにより評価する	ハザードはシステムの中で安全のための制御を行う要素（コントローラ）と制御される要素（被コントロールプロセス）の相互作用が働かないことによって起きるというアクシデントモデル
メリット	部品レベルまで細分化して分析できるため、深い分析が可能	機器の相互作用及び時間的遷移を含む解析を得意とする
デメリット	機器の相互作用及び時間的遷移を伴う等複雑な事象の解析に難	部品レベルの解析には解析が膨大となることが想定される

STAMP…System Theoretic Accident Model and Processes
STPA…STAMP based Process Analysis

STAMP/STPA実施手順



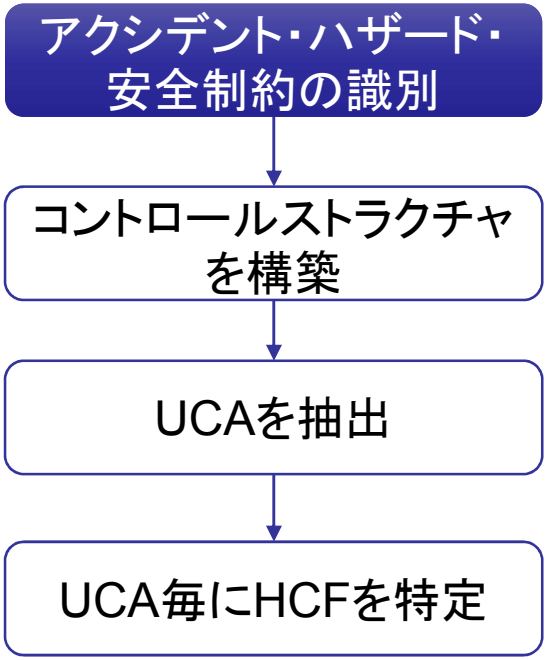
【STAMP/STPA試行】　対象装置



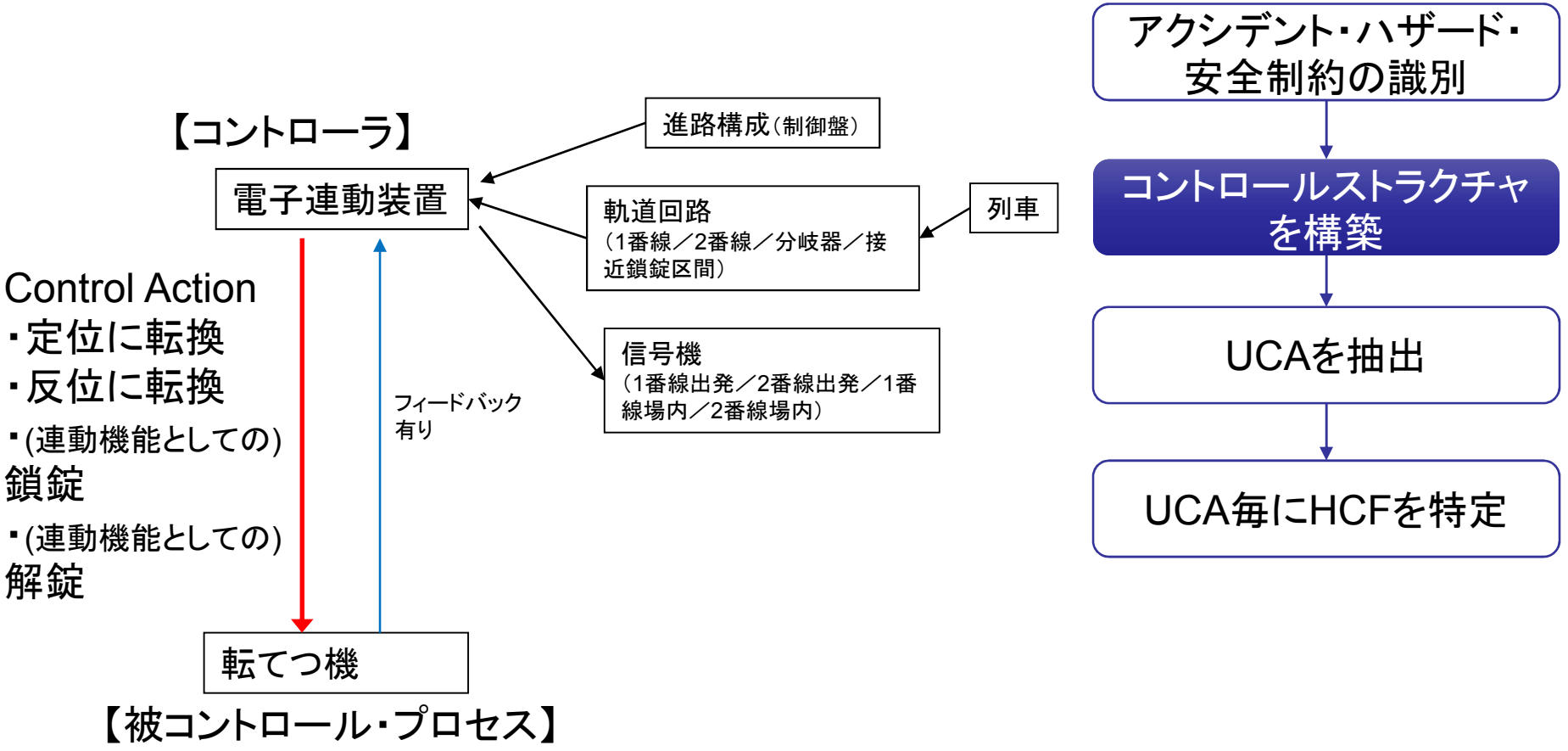
- 時間的遷移やタイミングの要素を含んだ制御を行う連動装置を試行対象として取り上げ、制御する要素を連動装置、制御される要素を転てつ機と仮定
- 連動装置から転てつ機への制御指示は、定位への転換、反位への転換、鎖錠及び解錠とし、各々の制御指示について連動装置へのフィードバック機能を有する
- それ以外の関係要素として、進路構成、軌道回路（4区間）及び信号機（出発／場内）を挙げた

【STAMP/STPA試行】アクシデント・ハザード・安全制約の識別

アクシデント	ハザード	安全制約
(A1)列車が分岐器上で脱線する	(H1)列車が分岐器上に在線中に不正転換する	(SC1)列車が分岐器上に在線中は転換してはならない
(A1)列車が分岐器上で脱線する	(H2)列車が分岐器上を走行中に鎖錠されない	(SC2)列車が分岐器上に在線中は鎖錠しなければならない
(A1)列車が分岐器上で脱線する	(H3)列車が非開通の分岐器を背向で通過する	(SC3)列車が背向で分岐器を通過する際に非開通であってはならない
(A2)列車同士が衝突する	(H4)到着列車の進路が駅在線列車と競合する方向に分岐器が開通している	(SC4)進路が競合するように分岐器を開通させてはならない

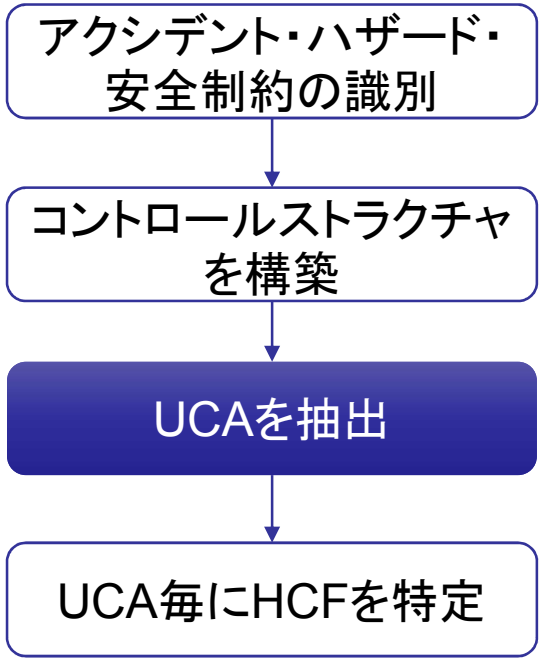


【STAMP/STPA試行】 コントロールストラクチャの構築



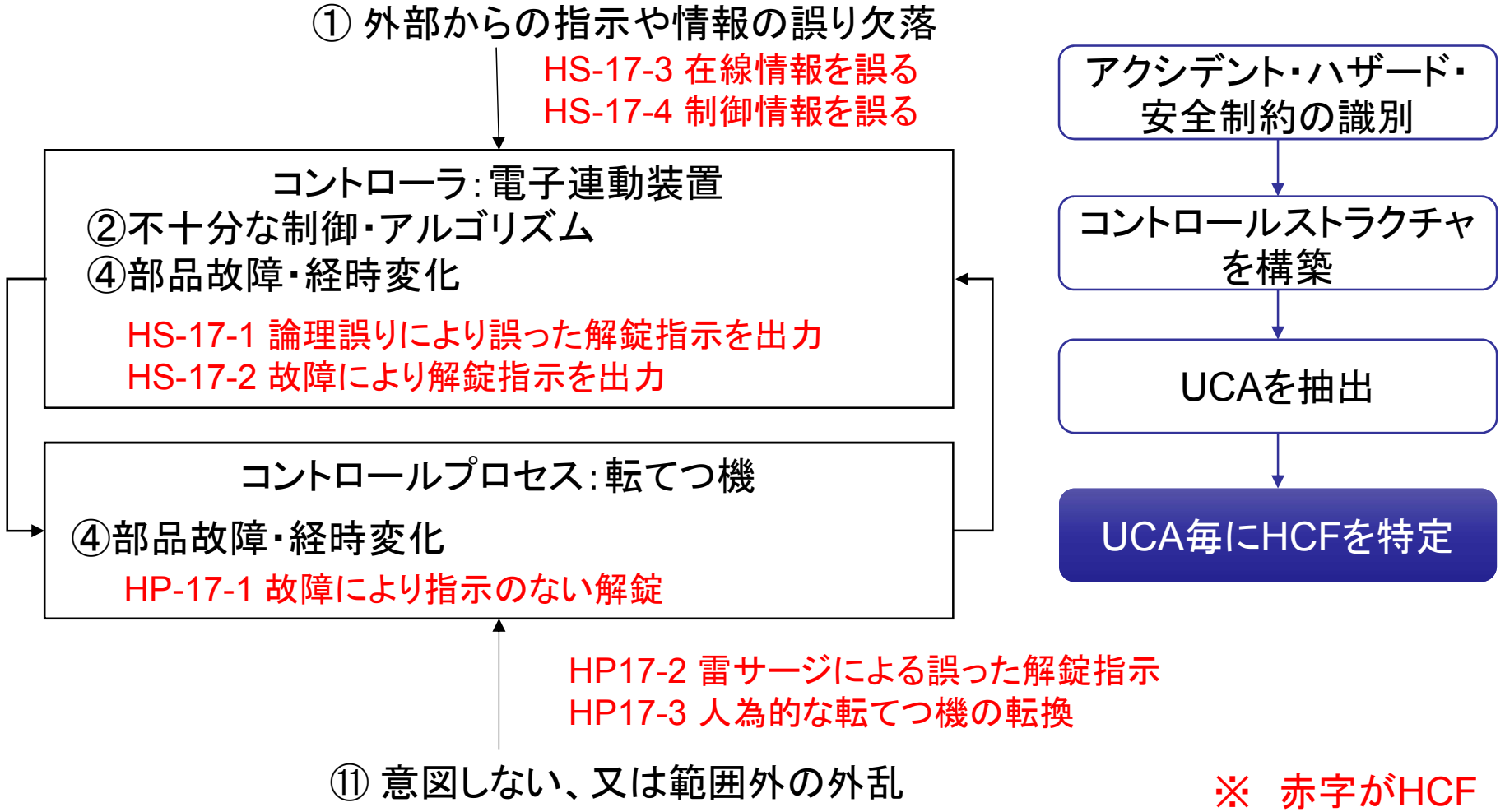
【STAMP/STPA試行】 UCAの抽出

コントロールアクション	与えられないとハザード	与えられるとハザード	早すぎ／遅すぎ／誤順序でハザード	早すぎる停止／長すぎる適用でハザード
解錠指示	転換が不可	（UCA16）車両が分岐器上を走行中だと脱線SC2違反	早すぎると・（UCA17）分岐器から進出前の車両が脱線SC2違反	早すぎる停止だと・解錠が不完全で次の転換が不可 長すぎる適用だと・次の鎖錠が不可



【STAMP/STPA試行】 HCFの特定

解錠指示　早すぎると
(UCA17)分岐器から進出前の車両が脱線 SC2違反

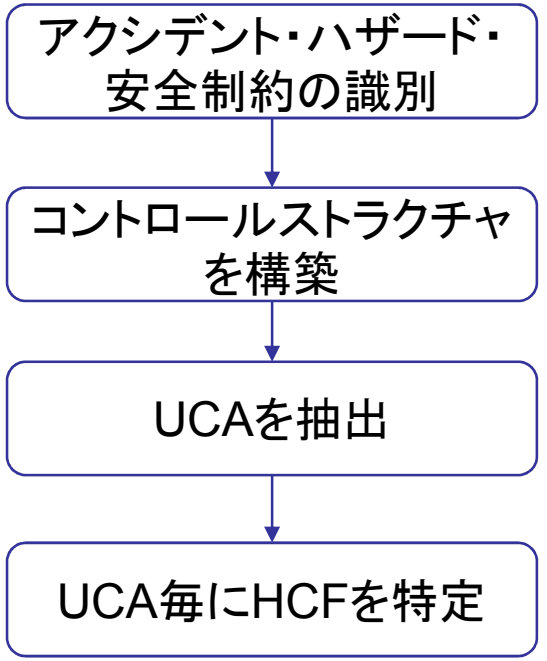


アクシデント・ハザード・安全制約の識別
↓
コントロールストラクチャを構築
↓
UCAを抽出
↓
UCA毎にHCFを特定

※　赤字がHCF

【STAMP/STPA試行】 解析例

- 同様に他のUCAに対しても解析を実施。抽出されたUCAに対して解析を行い、HCFとその対策を整理
- 以上より、STAMP/STPAを実施することで、相互作用及び時間的遷移も考慮に入れた安全性解析を行うことが可能であることを確認した
- なお、STAMP/STPAは現時点でIEC 62425に明確に記載された安全性評価手法ではないため、今後も試行を続け、規格への提案の可否についても検討していきたい



ハザード誘発要因	対策
HS-17-1 論理誤りにより誤った解錠指示を出力	設計段階・製造段階での検査
HS-17-2 故障により解錠指示を出力	定期検査
HP-17-1 故障により指示のない解錠	定期検査

まとめと今後の課題

- 海外向け鉄道システムの設計安全性評価に関し、複雑化した鉄道信号システムに対応するための評価手法について検討した
- これまでのFMEA及びFTAのような部品故障を対象とする考え方に加え、装置間の相互作用を解析するSTAMP／STPAの活用が有効なケースもあると考えられ、その一例として連動装置を例に検討を実施した
- 時間的遷移も考慮に入れた解析が可能なことから、その手法の有効性を確認した
- 今後は、FMEA及びFTAによる従来の安全性解析に加え、STAMP/STPAの適用実績を積み重ねていき、引き続き設計安全性評価に貢献していきたい