



STAMP / STPAを用いた ハザードログツールの提案

(A Proposal to Use a Hazard Log Tool in
Conjunction with STAMP/STPA)

2018年12月4日

株式会社京三製作所 開発センター
堺 将人 (Masato Sakai)



1. はじめに
2. 電子連動装置のSTAMP/STPA解析
3. リスク査定
4. リスク管理への展開
5. 対策の確認
6. まとめ

① 第1回Workshop
STAMP/STPAの解析結果



リスクの管理手法の
提案

② 第2回Workshop
踏切制御システムに対する
STAMP/STPA解析



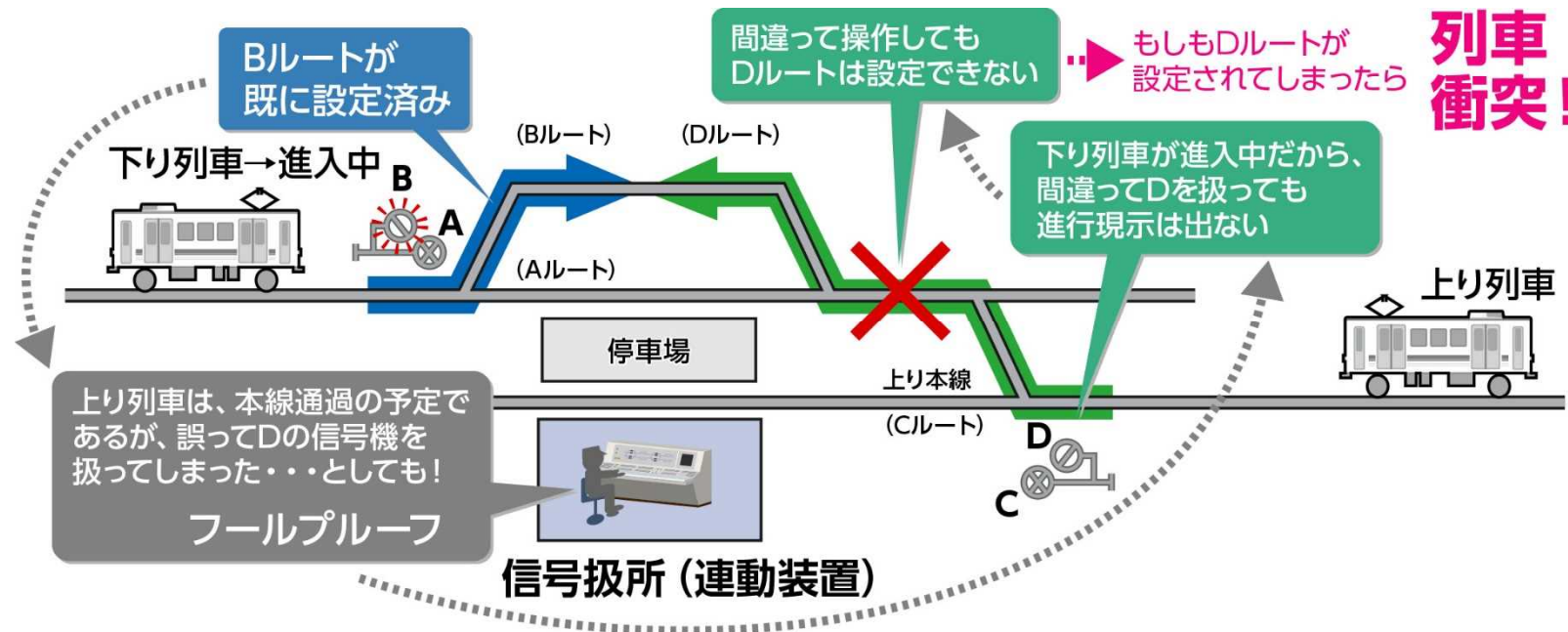
踏切事故調査結果



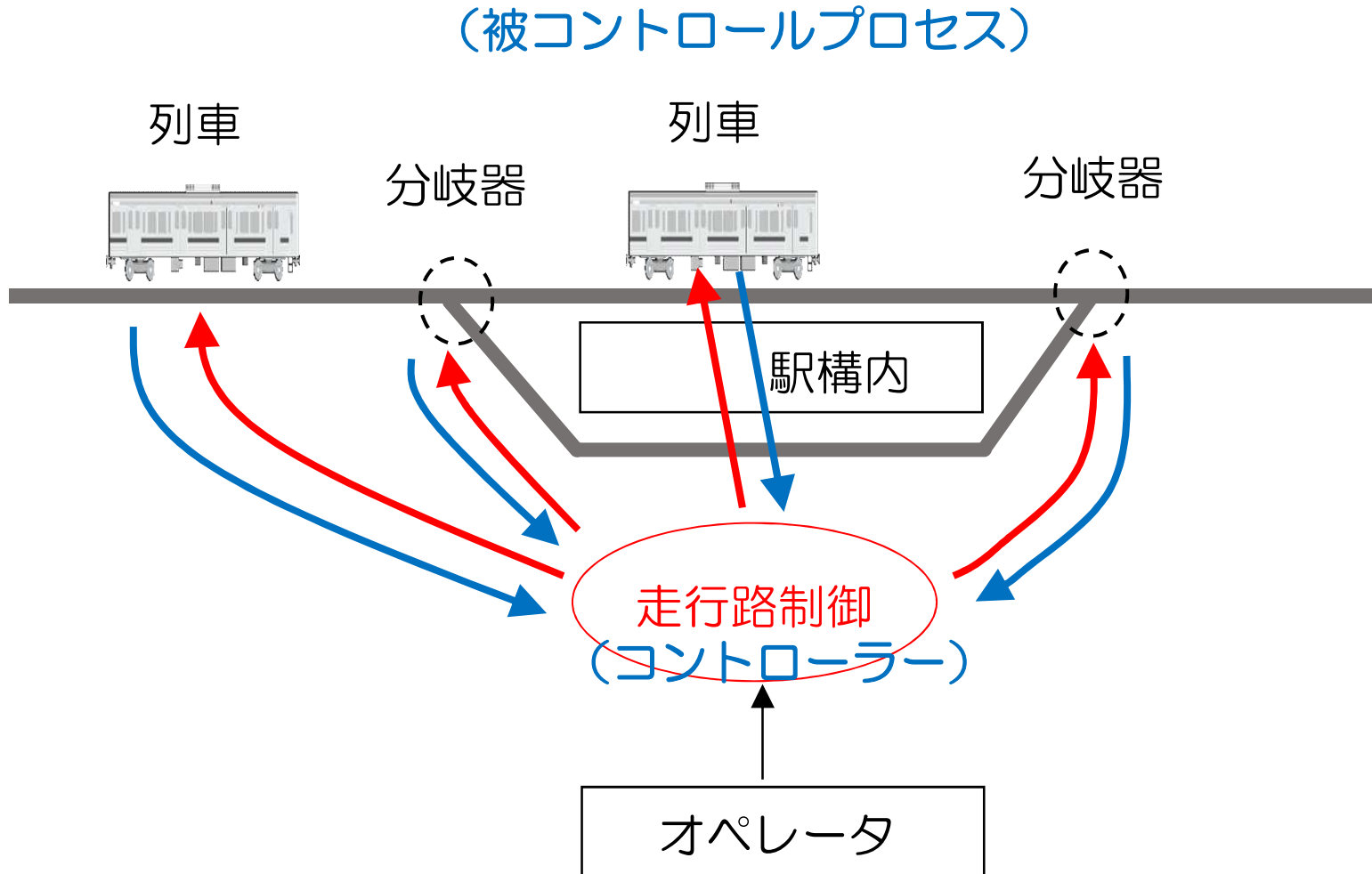
STAMP/STPAの
網羅性

③ 今回

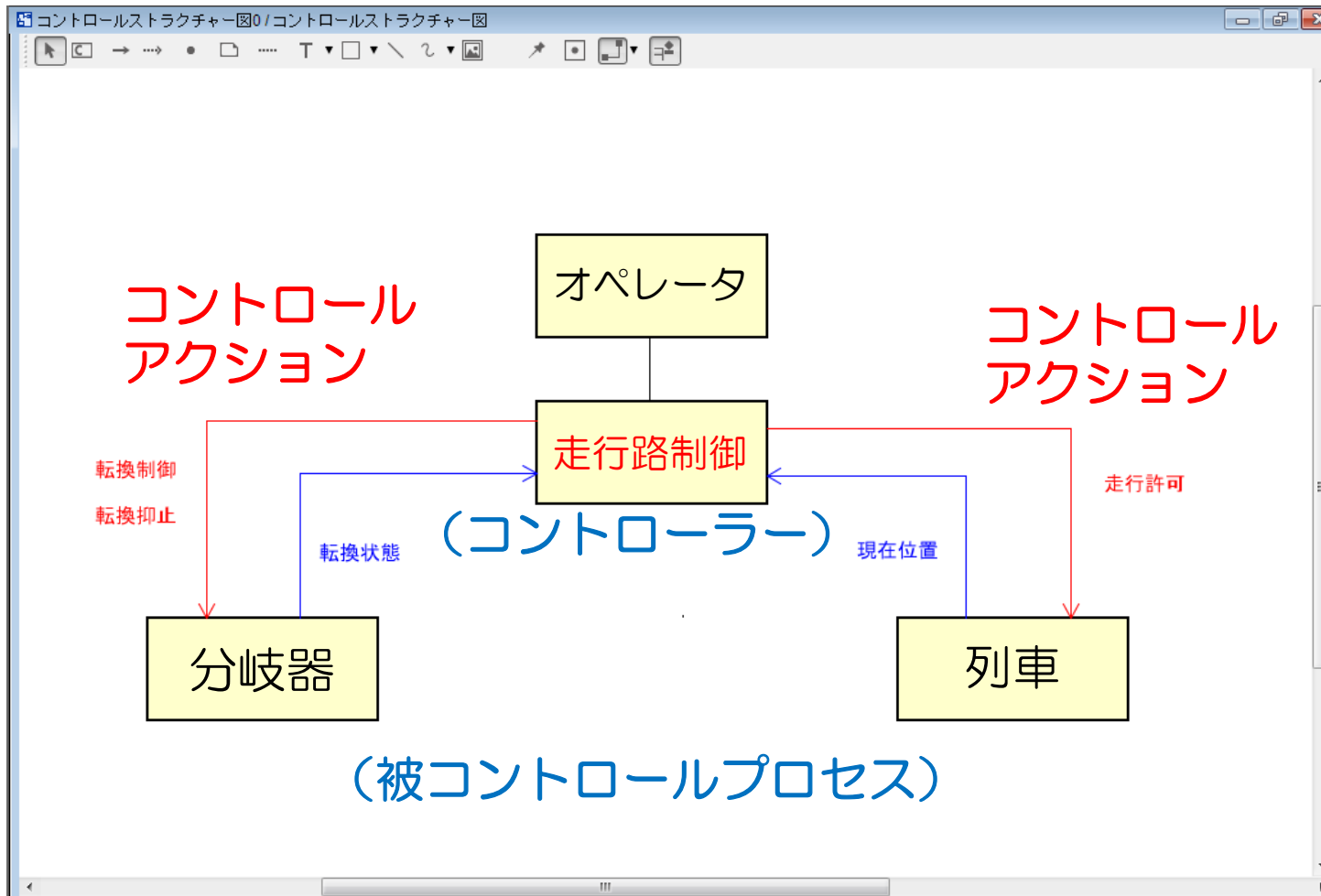
STAMP/STPAを用いたハザードログツールの提案



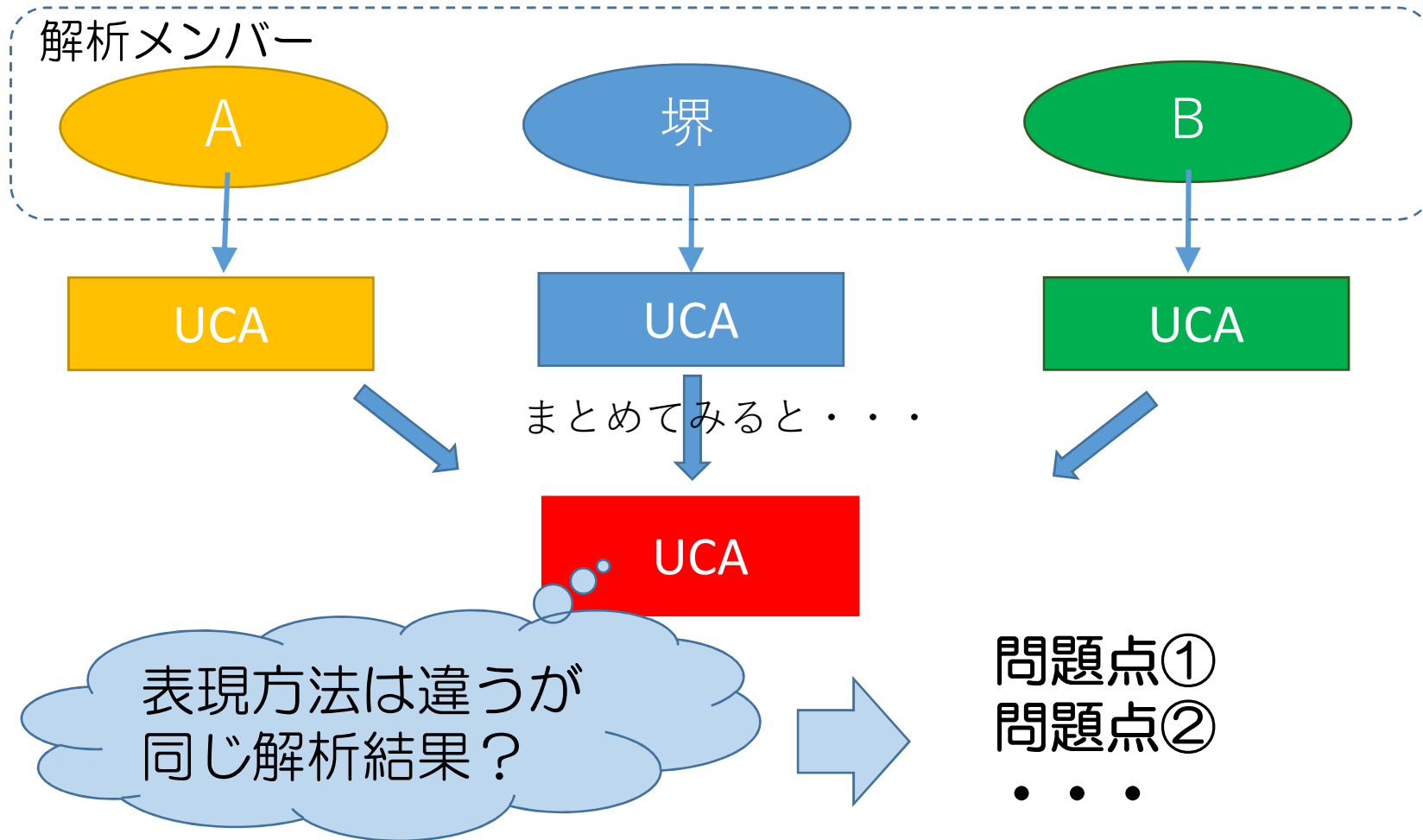
信号機、転てつ器等の制御または操作に一定の順序および制限を付して、相互に連鎖を設けた装置のことを連動装置と呼び、これをマイコンとソフトウェアで実現したものを電子連動装置と呼ぶ。



- 概念図をもとに、コントロールストラクチャを構築



- 複数のメンバーでUCAを解析すると

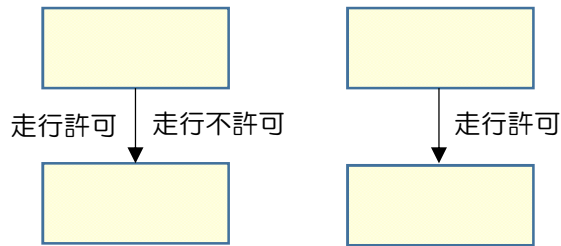


問題点① 同じ状態遷移に対し、相反する表現方法が存在

例) 走行許可 (コントロールアクション)

走行許可を与える

走行不許可を与えない



“コントロールアクション” 名を統一

問題点② 解析対象の状態の範囲を定義しないと解析結果が重複

例) 分岐器と列車の関係に関する表現

- 分岐器上を走行している列車に転換制御を与える
- 分岐器上を列車が通過完了する前に転換制御を与える
- 列車が分岐器にさしかかった時に転換制御を与える



“状態” を定義

誰が見てもわかるように “解析結果の状態” を明記

ガイドワード適用時の記述ルール (〇〇はコントロールアクション)

- ① Not Providing
 - **XXの状態**で、**〇〇**が与えられないとハザード
- ② Providing causes hazard
 - **XXの状態**で、**〇〇**が与えられるとハザード
- ③ Too early/too late,wrong order causes hazard
 - **XXの状態**になる前に、**〇〇**が与えられるとハザード
 - **XXの状態**になった後に、**〇〇**が与えられるとハザード
 - **XXの状態**で、順序を間違えて**〇〇**を与えるとハザード
- ④ Stopping too soon/applying too long causes hazard
 - **XXの状態**で、**〇〇**が停止するとハザード
 - **XXの状態**で、**〇〇**が継続するとハザード

STAMP/STPA

Step0
アクシデント、ハザード、安全制約
コントロールストラクチャ

Step1
UCAの抽出 網羅的に抽出可

Step2
HCFの特定



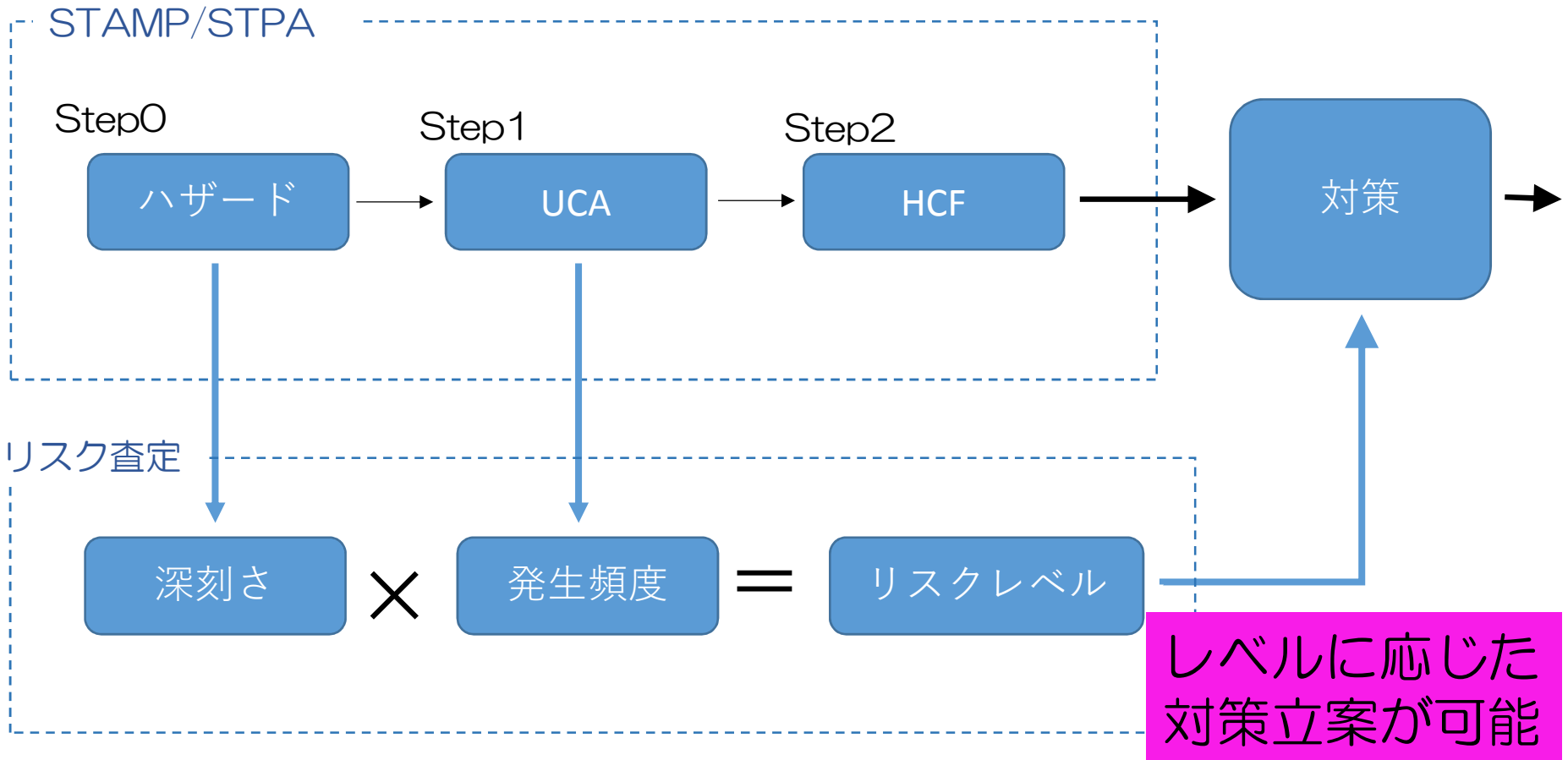
コスト
メンテナンス
etc 考慮が必要

リスクレベルに応じた適切な対策



UCAに対するリスク査定

リスク査定の考え方



リスク査定には、IEC62278（RAMS規格）を適用

①ハザード

②想定事象 (UCA)

③ハザードによる結果の深刻さレベル

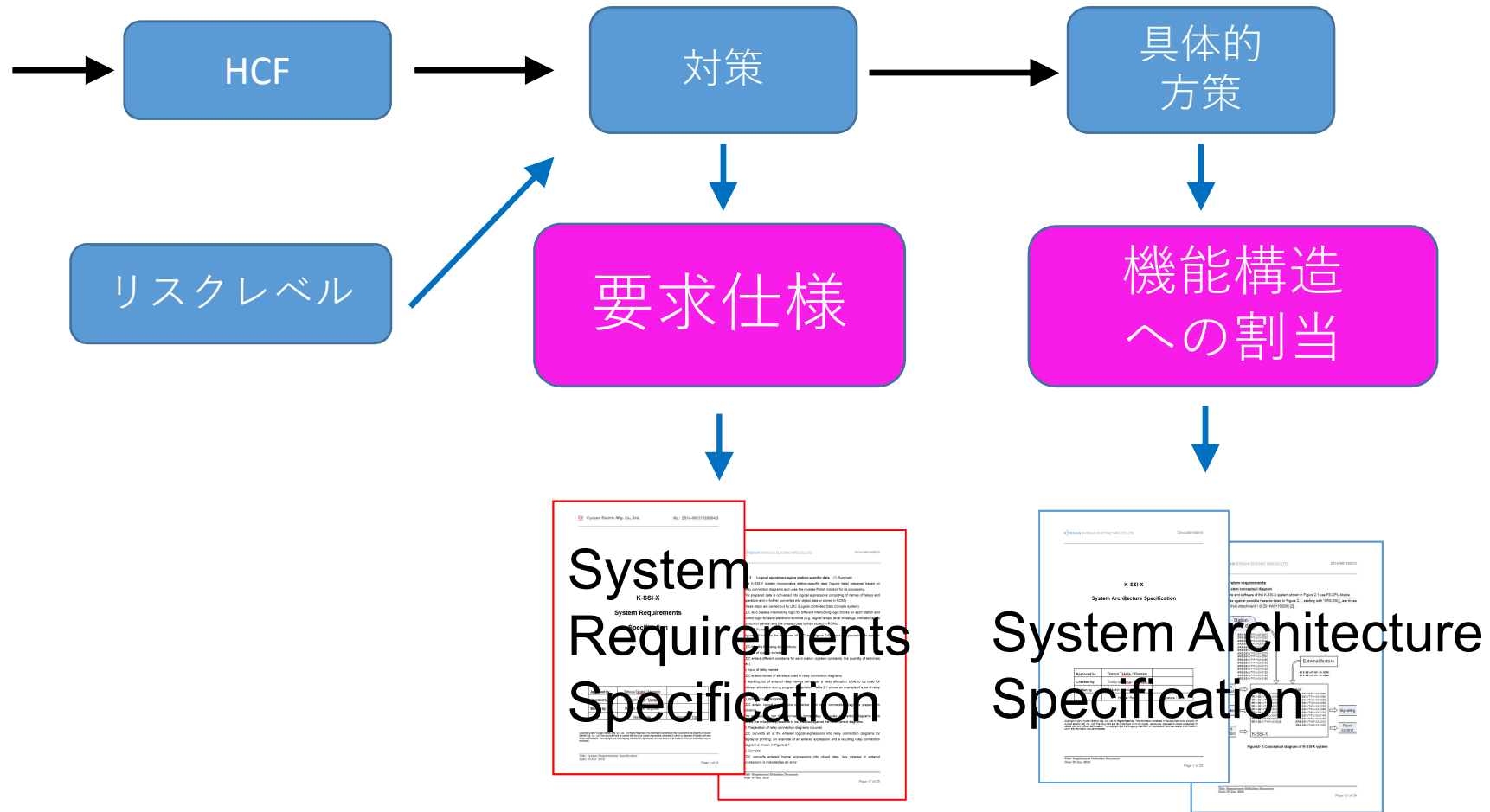
④UCAの発生頻度

⑤リスクレベル (③×④)

⑥ハザード要因 (HCF)

No.	ITEM (Name)	Hazard	Unsafe Control Action 安全ではない制御操作	Hazard Severity level (Select)	Frequency of Occurrence of hazardous event (Select)	Qualitative Risk categorie	Hazard Causal Factor ハザード要因	Determine 可能な対策	対策に対する具体的方策	Risk (RPN)
1	走行路制御装置	(HM) 列車の前方に列車がいる時に分岐路が転換された状態で、走行許可が与えられた列車が進行すると、列車が衝突(追突)する。	(UCA) 前方に列車がいる時に分岐路が転換された状態で、走行許可が与えられた列車が進行すると、列車が衝突(追突)する。	Catastrophic	Remote	Undesirable	① 転てつ機の転換方向を正しく認識できない(限り)			
2				Catastrophic	Remote	Undesirable	② 不適切な制御アルゴリズムが出力される			
3				Catastrophic	Remote	Undesirable	③ 列車の位置情報を正しく認識できない(不完全)			
4				Catastrophic	Remote	Undesirable	④ 列車を把握できない。(欠)			
5				Catastrophic	Remote	Undesirable	⑤ 列車を正しく認識できない。(欠如)			
6				Catastrophic	Remote	Undesirable	⑥ 進行許可を出力していないのに進行表示が出力された。			
7				Catastrophic	Remote	Undesirable	⑦ 進行許可を出力していないのに進行表示が出力された。			
8			(UCA) 走行許可が出て列車が走行している状態で、走行許可を解除すると、不許可域に進入してしまう。(不許可域に列車が着いた衝撃・脱線。)	Catastrophic	Improbable	Tolerable	② 不適切なアルゴリズムにより列車が止まらない状況で急に走行許可を解除される。			
9				Catastrophic	Improbable	Tolerable	③ 列車の位置の状態を正しく認識できない。(不完全)			
10				Catastrophic	Improbable	Tolerable	④ 列車の位置の状態を正しく認識できない。(不完全)			

Intolerable	受け入れ不可
Undesirable	望ましくない
Tolerable	許容可
Negligible	無視できる



No.	ITEM (Name)	Hazard	Unsafe Control Action 安全でない制御動作	Hazard Severity level (Select)	Frequency of Occurrence of hazardous event (Select)	Qualitative Risk categorie	Hazard Causal Factor ハザード要因	Determine possible actions 可能な対策	Method 対策に対する具体的方策	Risk (RPN)
1	北行発車制御装置	(H1) 列車の前方に列車がある状態で、走行許可が与えられ列車が進行すると、列車が衝突(衝突)する。	(UCA3) 前方に列車がある状態で、走行許可が与えられ列車が進行すると、列車が衝突(衝突)する。	Catastrophic	Remote	Undesirable	① 転てつ機の転機方向を正し、認識できない。(誤り)	① 転てつ機の転機方向の入力回路は検定であることを常に監視し、異常時は転機できない状態とすること。	入力回路の健全性：FS CPU Block 異常時処理：運動処理 → 処理はIEC62279に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする。	Negligible
2					Remote	Undesirable	② 不適切な制御プログラムにより走行許可が出力される。	② アルゴリズムの検証は十分に実施すること。	検証はIEC62279に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする。	Negligible
3					Remote	Undesirable	③ 列車の位置情報を正し、認識できない。(不完全)	③ プロセスすること。	検証はIEC62279に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする。	Negligible
4				Catastrophic	Remote	Undesirable	④ 列車を把握できない。(欠陥)	④ 列車の位置情報を正し、認識できない。(不完全)	④ 列車の位置情報を正し、認識できない。(不完全)	Negligible
5				Catastrophic	Remote	Undesirable	⑤ 列車を正し、認識できない。(欠陥)	⑤ 列車を正し、認識できない。(欠陥)	⑤ 列車を正し、認識できない。(欠陥)	Negligible
6				Catastrophic	Remote	Undesirable	⑥ 走行許可を出力していないのに進行表示が出力された。	⑥ 走行許可制御を監視し、異常時は安全側に制御すること。	監視：運動処理 運動処理はIEC62279に準拠したSIL4の要件を満たす最上位レベルの機能をサポートする。安全側制御：FS-CPU (安全側の規定は運動処理に基づき定義する)	Negligible
7										Negligible
8										Negligible
9										Negligible
10										Negligible

対策に対する
具体的方策

A方式
K5形

No.	ITEM (Name)	Hazard	Unsafe Control Action 実安全ではない制御動作	Hazard Severity Level (Select)	Frequency of Occurrence of hazardous event (Select)	Qualitative Risk category	Hazard Causal Factor ハザード要因	Method 対策に対する具体的方策	Risk (RPH)
1	走行制御	① 列車の速度超過	① 列車の速度超過を抑制する機能を確保する。速度超過を抑制する機能を確保する。	Catastrophic	Remote	Undesirable	① 列車の速度超過を抑制する機能を確保する。	① 列車の速度超過を抑制する機能を確保する。	Negative
2				Catastrophic	Remote	Undesirable	② 列車の速度超過を抑制する機能を確保する。	② 列車の速度超過を抑制する機能を確保する。	Negative
3				Catastrophic	Remote	Undesirable	③ 列車の速度超過を抑制する機能を確保する。	③ 列車の速度超過を抑制する機能を確保する。	Negative
4				Catastrophic	Remote	Undesirable	④ 列車の速度超過を抑制する機能を確保する。	④ 列車の速度超過を抑制する機能を確保する。	Negative
5				Catastrophic	Remote	Undesirable	⑤ 列車の速度超過を抑制する機能を確保する。	⑤ 列車の速度超過を抑制する機能を確保する。	Negative
6				Catastrophic	Remote	Undesirable	⑥ 列車の速度超過を抑制する機能を確保する。	⑥ 列車の速度超過を抑制する機能を確保する。	Negative
7				Catastrophic	Remote	Undesirable	⑦ 列車の速度超過を抑制する機能を確保する。	⑦ 列車の速度超過を抑制する機能を確保する。	Negative
8				Catastrophic	Remote	Undesirable	⑧ 列車の速度超過を抑制する機能を確保する。	⑧ 列車の速度超過を抑制する機能を確保する。	Negative
9				Catastrophic	Improbable	Tolerable	⑨ 列車の速度超過を抑制する機能を確保する。	⑨ 列車の速度超過を抑制する機能を確保する。	Negative
10				Catastrophic	Improbable	Tolerable	⑩ 列車の速度超過を抑制する機能を確保する。	⑩ 列車の速度超過を抑制する機能を確保する。	Negative

System Architecture Specification

① 既存電子運動

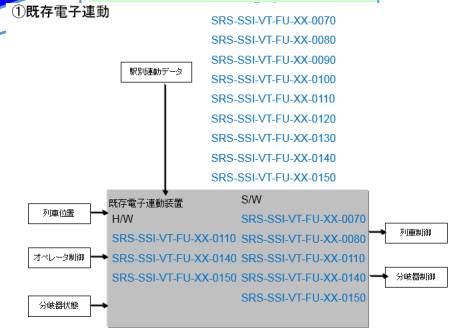
- SRS-SSI-VT-FU-XX-0070
- SRS-SSI-VT-FU-XX-0080
- SRS-SSI-VT-FU-XX-0090
- SRS-SSI-VT-FU-XX-0100
- SRS-SSI-VT-FU-XX-0110
- SRS-SSI-VT-FU-XX-0120
- SRS-SSI-VT-FU-XX-0130
- SRS-SSI-VT-FU-XX-0140
- SRS-SSI-VT-FU-XX-0150

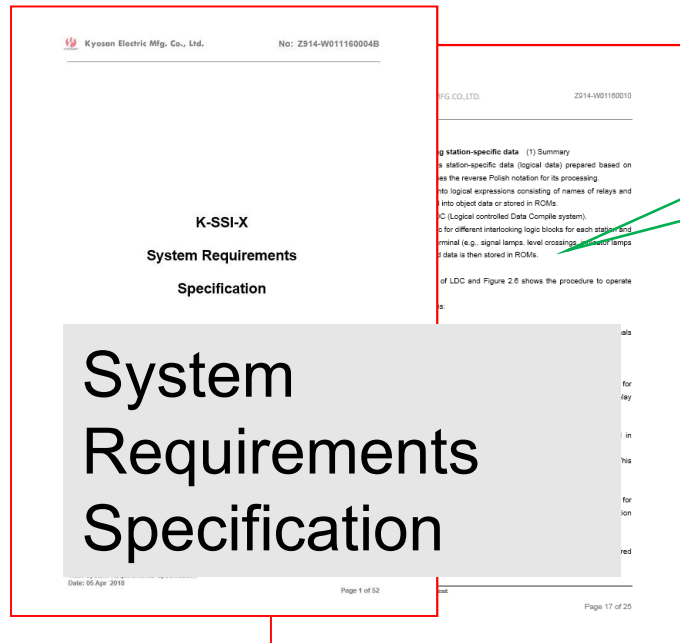


No.	ITEM (Name)	Hazard	Unsafe Control Action 実安全をしない制御動作	Hazard Severity level (Select)	Frequency of Occurrence of hazardous event (Select)	Qualitative Risk category	Hazard Causal Factor ハザード要因	Identify possible actions 可能な対策	Method 対策に対する具体的方策	Risk (RPN)
1	走行制御 制動機能	(1)列車位置検出機能 (2)列車位置検出機能 (3)列車位置検出機能 (4)列車位置検出機能 (5)列車位置検出機能	(USA)前方に列車がいるのに制動が解除される状態 が実行される。列車が衝突 する。	Catastrophic	Remote	Undesirable	① 軌道の軌道方向を正し誤差を なくし、誤り	軌道の軌道方向の入力部 にエラーを発生させない。衝突 しない状態を維持する。	方軌の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
2				Catastrophic	Remote	Undesirable	② 不適切なアルゴリズムにより列車 が検出されない。(不完全)	アルゴリズムの検証は十分 なことを確認する。	誤検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
3				Catastrophic	Remote	Undesirable	③ 列車の位置情報を正し誤差を なくし、誤り	位置情報の検出は十分 であることを確認する。	位置情報の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
4				Catastrophic	Remote	Undesirable	④ 列車を正しく認識できない。(欠陥)	列車の検出を正しく 検出することを確認する。	列車の検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
5				Catastrophic	Remote	Undesirable	⑤ 列車を正しく認識できない。(欠陥)	列車の検出を正しく 検出することを確認する。	列車の検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
6				Catastrophic	Remote	Undesirable	⑥ 列車を正しく認識できない。(欠陥)	列車の検出を正しく 検出することを確認する。	列車の検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
7				Catastrophic	Remote	Undesirable	⑦ 列車を正しく認識できない。(欠陥)	列車の検出を正しく 検出することを確認する。	列車の検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
8				Catastrophic	Remote	Undesirable	⑧ 列車を正しく認識できない。(欠陥)	列車の検出を正しく 検出することを確認する。	列車の検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
9			(USA)走行制御が解除された 状態で列車が検出されない状態 が実行される。列車が衝突 する。(不完全)	Catastrophic	Improbable	Tolerable	① 不適切なアルゴリズムにより列車 が検出されない。(不完全)	アルゴリズムの検証は十分 なことを確認する。	誤検出の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible
10				Catastrophic	Improbable	Tolerable	② 列車の位置情報を正し誤差を なくし、誤り	位置情報の検出は十分 であることを確認する。	位置情報の発生性：FB CPU Block 発生確率：低動機 発生レベルに達しない条件を満 足させることとする。	Negligible

対策に対する
具体的方策

A方式
K5形





- 2. 安全要求
 - 2.1 分岐器上に列車がいる場合、その間は分岐器を転換できないようにする。
 - 2.2 進行を指示する現示から停止現示にすると常に一定時分経過するまで転轍機を鎖錠する。
 - 2.3 接近区間に列車が在るとき、信号機を停止現示にしても一定時分経過するまでは転てつ機を鎖錠する。
 - ⋮
 - ⋮



電子連動装置の安全機能が全て網羅出来ていることを確認

- ① 解析時に入カルールを設けることで、解析結果の重複を低減できることが確認できた。
- ② STAMP/STPAの解析結果をハザードログツールでまとめると鉄道の国際規格RAMS（IEC62278）におけるリスク分析の記録と追跡を行う上での手段として展開できる事が確認できた。
- ③ 電子連動装置のSTAMP/STPA解析結果から、電子連動装置の安全機能要求が全て導き出せたことで、STAMP/STPA解析がハザードを網羅的に解析できることが示せた。

ご静聴ありがとうございました