










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）




KYOSAN KYOSAN ELECTRIC MFG.CO.,LTD.

目次

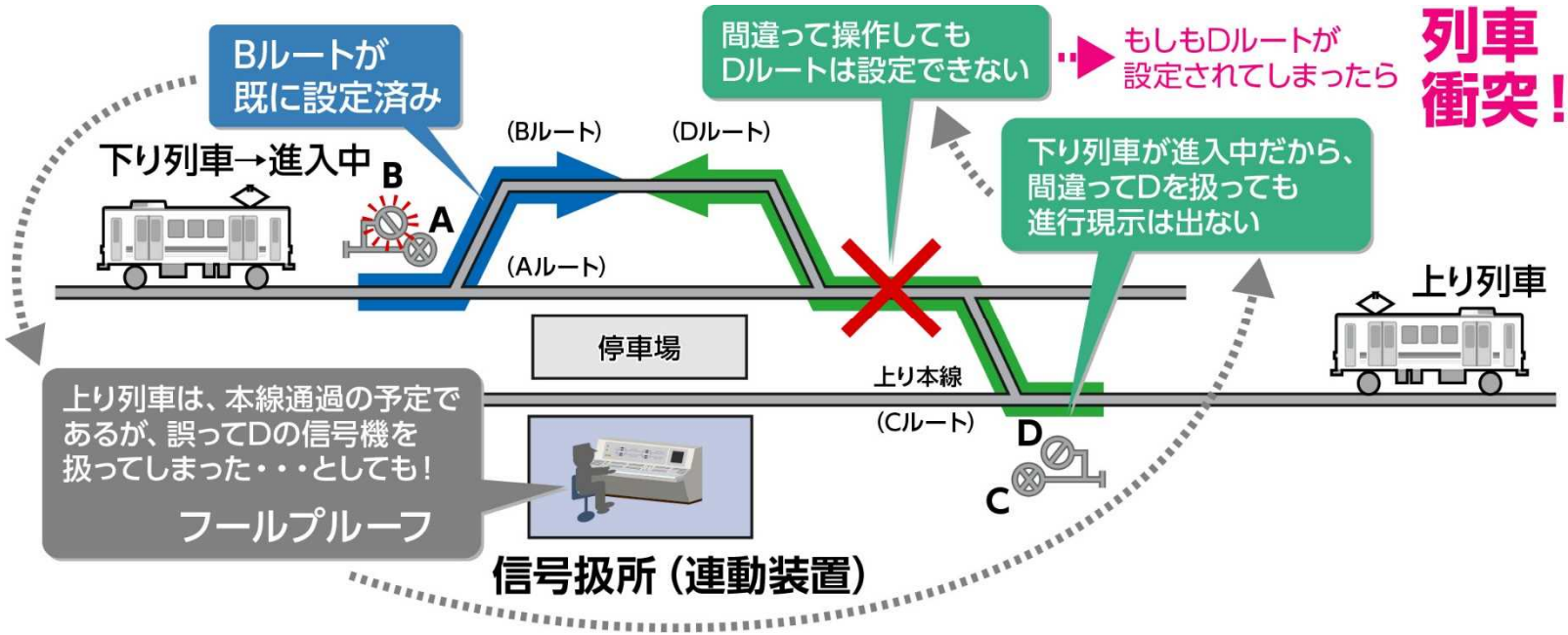
はじめに

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

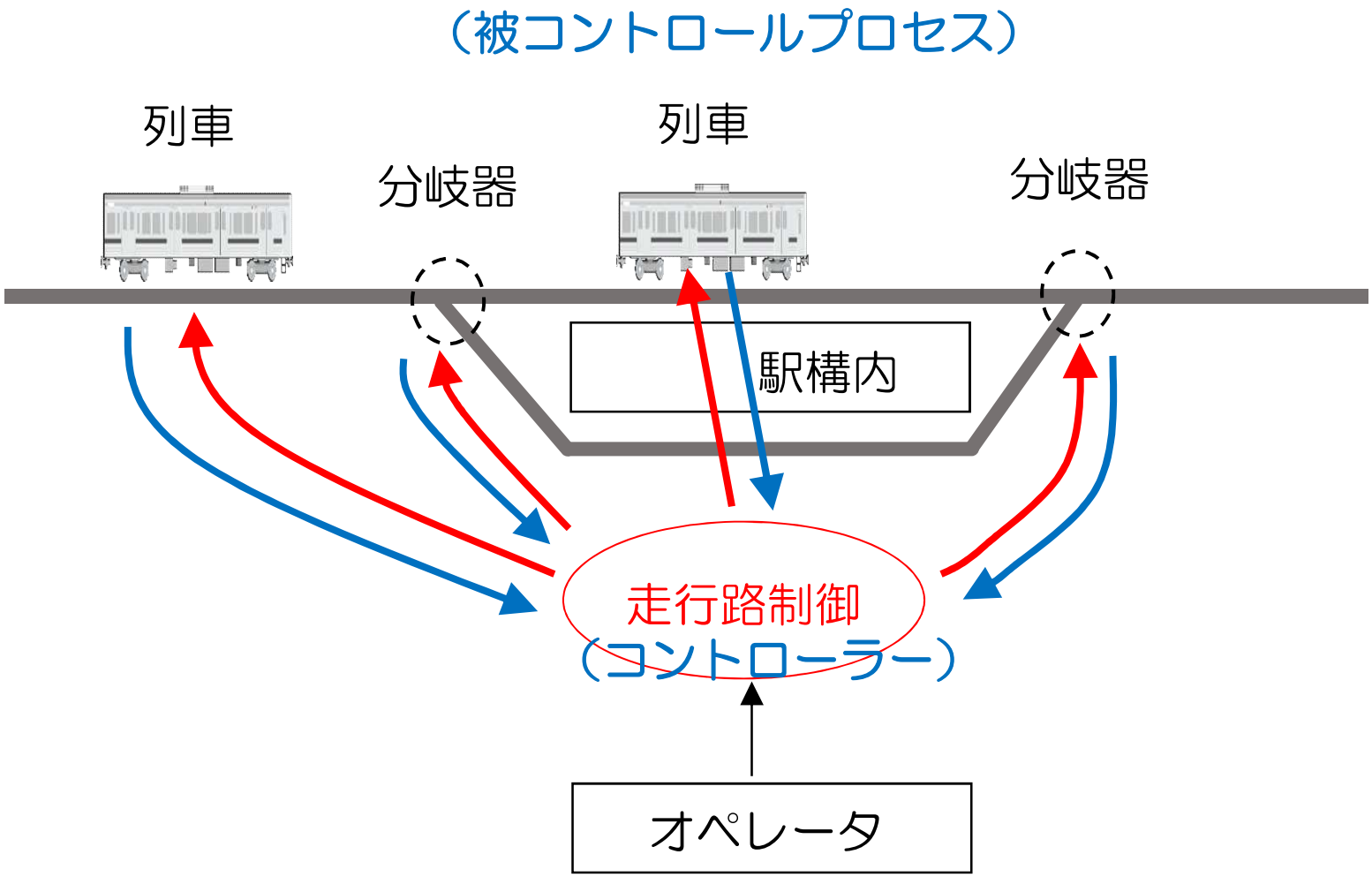
③ 今回
STAMP/STPAを用いたハザードログツールの提案

電子連動装置とは



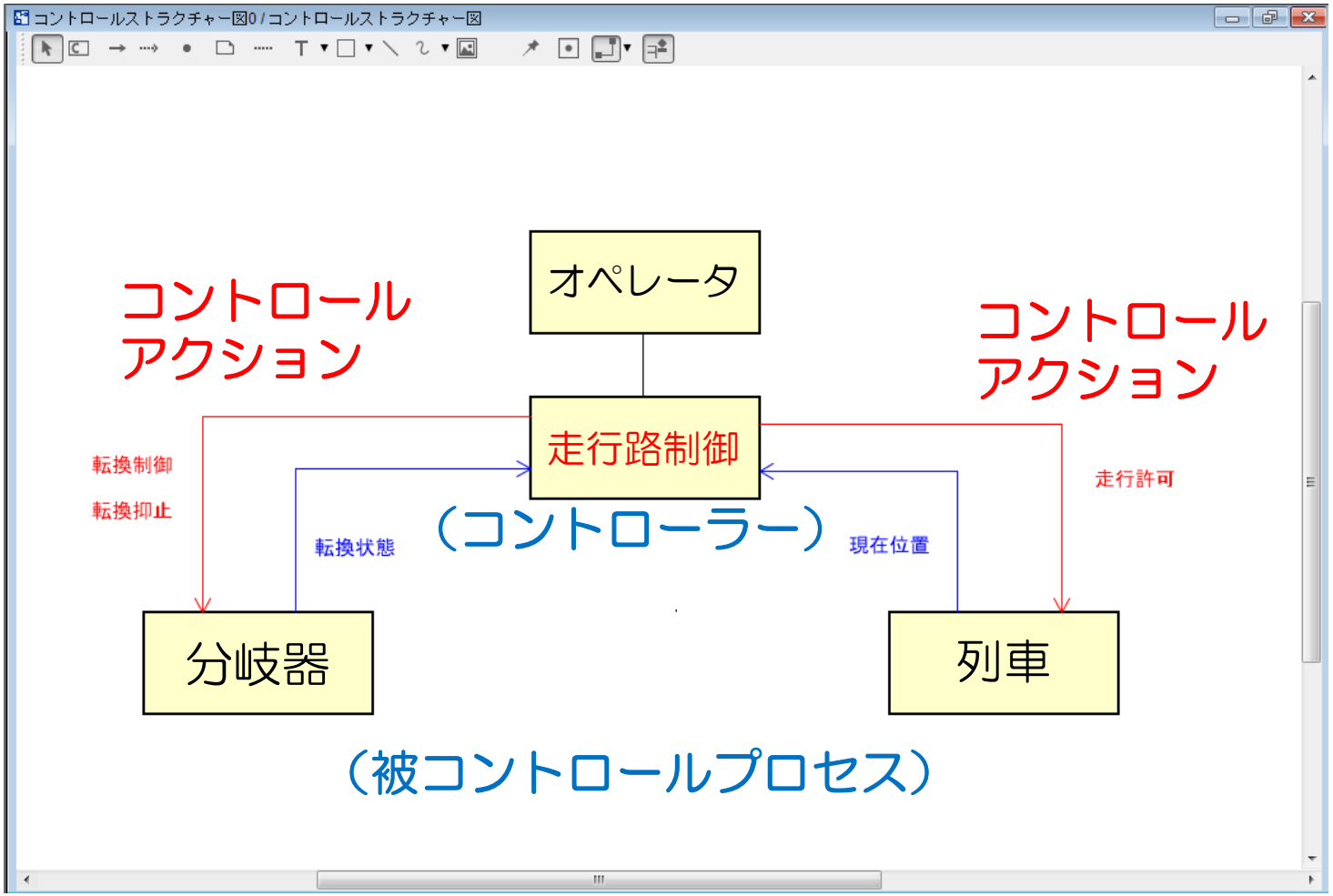
信号機、転てつ器等の制御または操作に一定の順序および制限を付して、相互に連鎖を設けた装置のことを連動装置と呼び、
これをマイコンとソフトウェアで実現したものを電子連動装置と呼ぶ。

概念図の検討



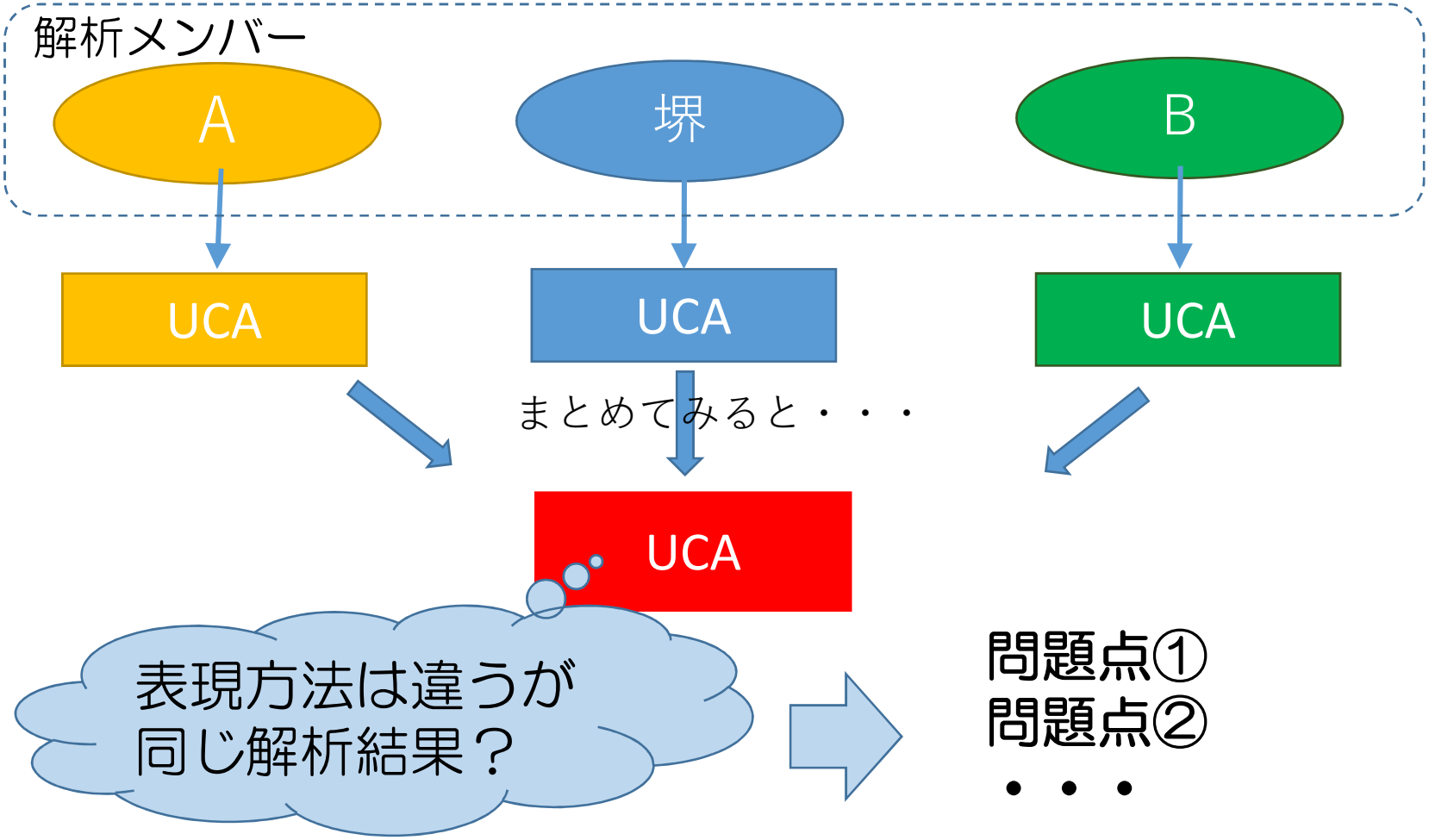
コントロールストラクチャの構築

- 概念図をもとに、コントロールストラクチャを構築



UCA抽出時の問題点

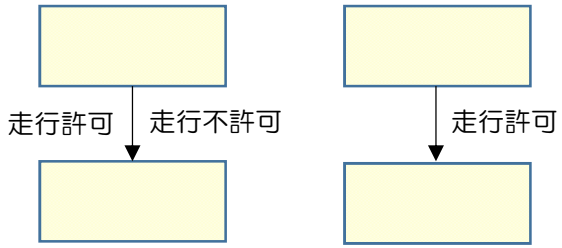
- 複数のメンバーでUCAを解析すると



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

UCA　入力ルールの検討（3）

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

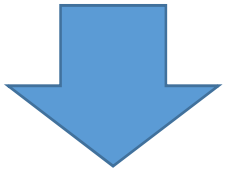
STAMP/STPA

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

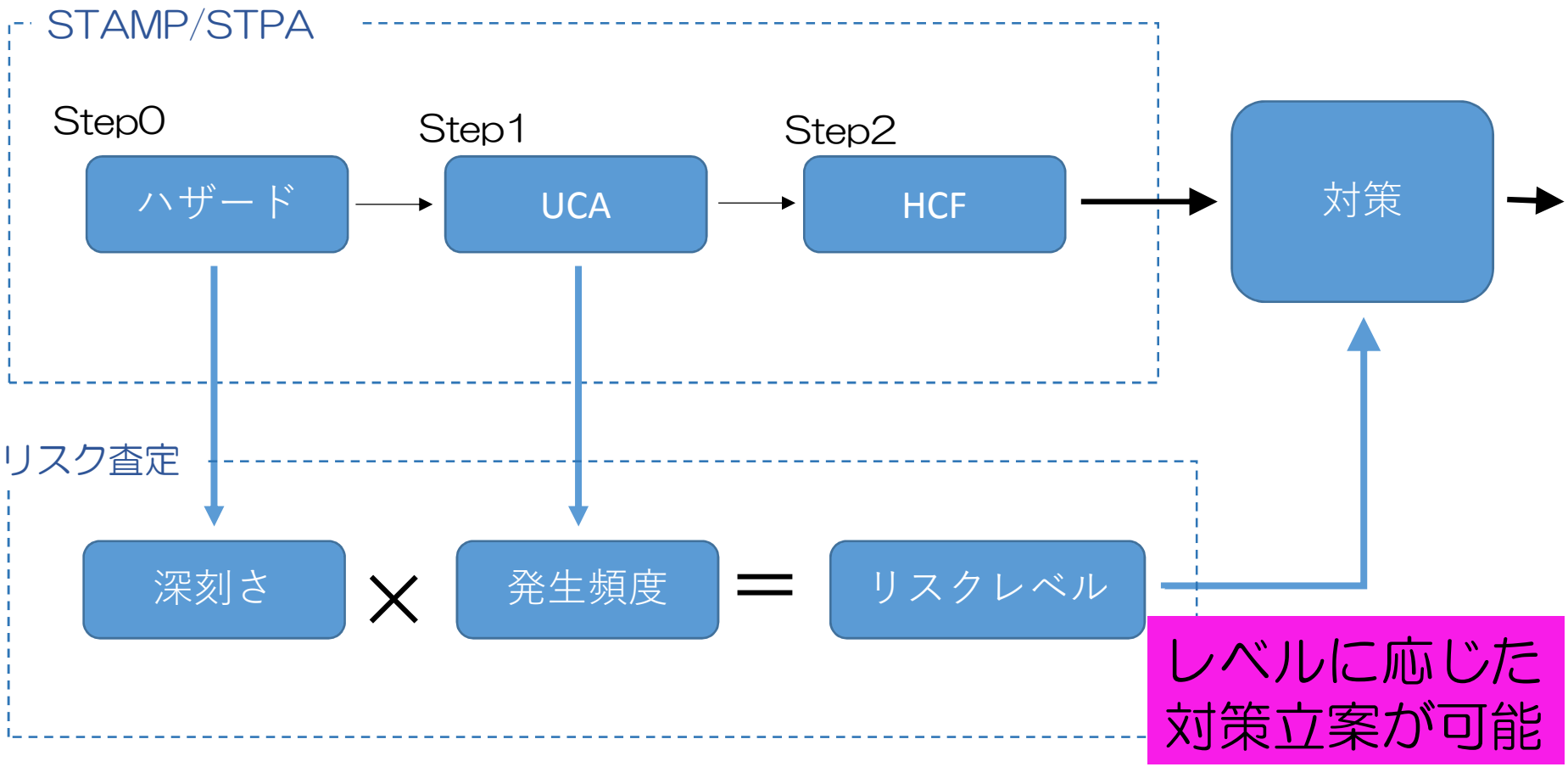
Step2
　HCFの特定

リスクレベルに応じた適切な対策



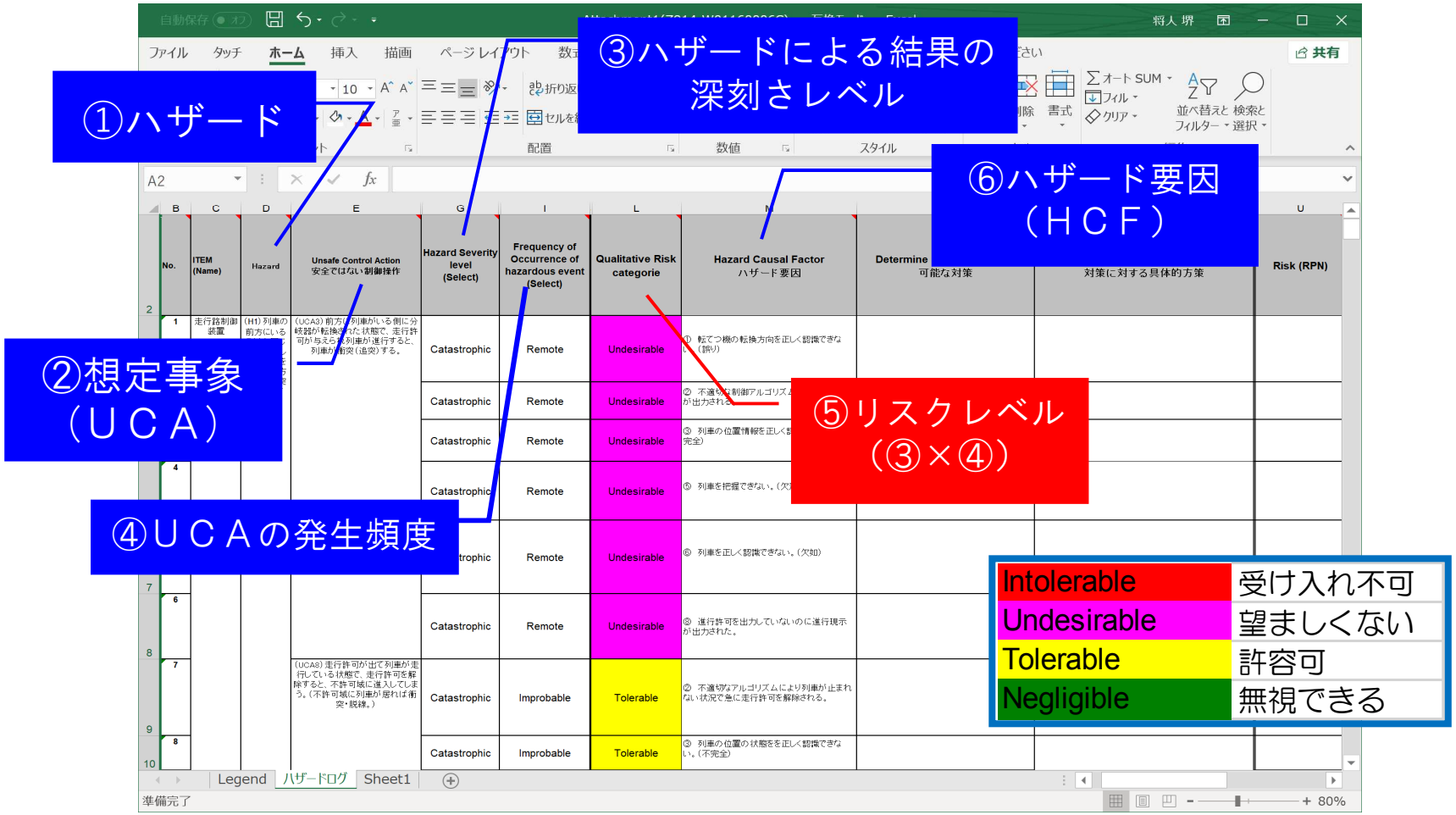
UCAに対するリスク査定

リスク査定の考え方



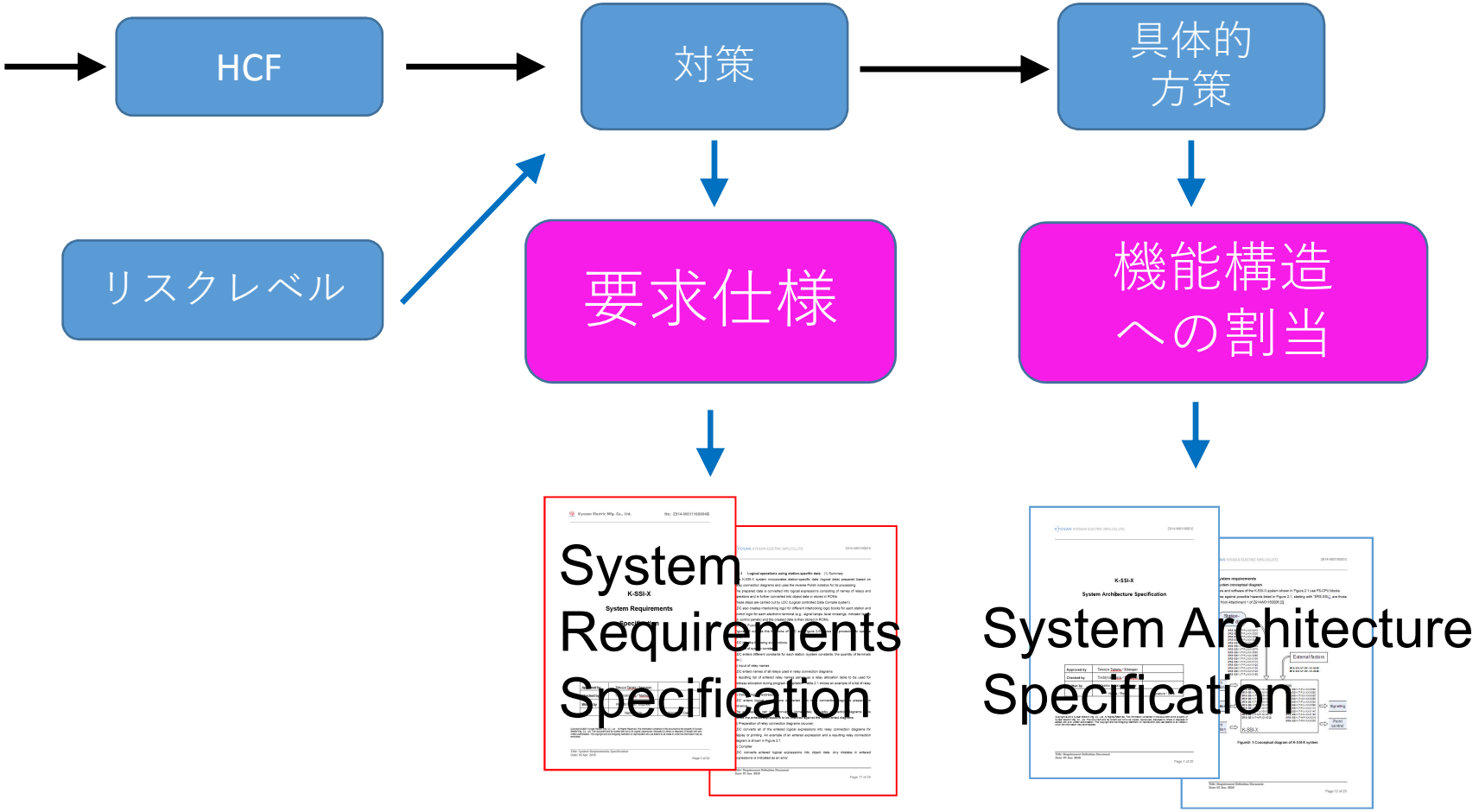
リスク査定（2）

リスク査定には、IEC62278（RAMS規格）を適用

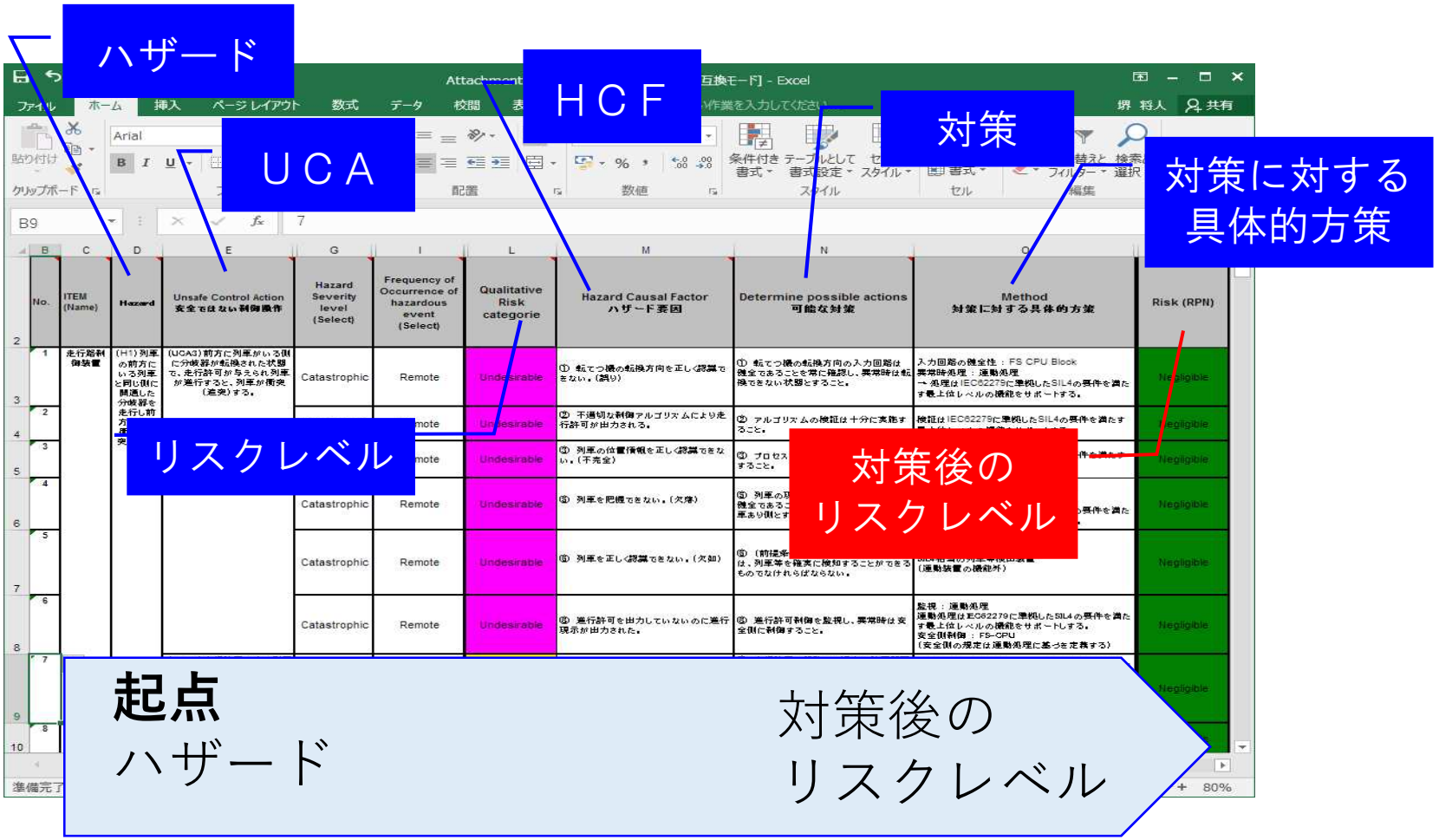


No.	ITEM (Name)	Hazard	Unsafe Control Action 安全ではない制御操作	Hazard Severity level (Select)	Frequency of Occurrence of hazardous event (Select)	Qualitative Risk categorie	Hazard Causal Factor ハザード要因	Determine 可能な対策	対策に対する具体的方策	Risk (RPN)
1	走行路制御装置	(H1) 列車の前方にいる	(UCA3) 前方に列車がいる側に分岐器が転換された状態で、走行許可が与えられ列車が進行すると、列車が衝突（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（誤り）			
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。（欠如）			
7				trophic	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現示が出力された。			
8	7		(UCA8) 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。(不許可域に列車が居れば衝突・脱線。)	Catastrophic	Improbable	Tolerable	② 不適切なアルゴリズムにより列車が止まれない状況で急に走行許可を解除される。			
9	8			Catastrophic	Improbable	Tolerable	③ 列車の位置の状態をを正しく認識できない。(不完全)			
10										

対策の検討と仕様書への展開



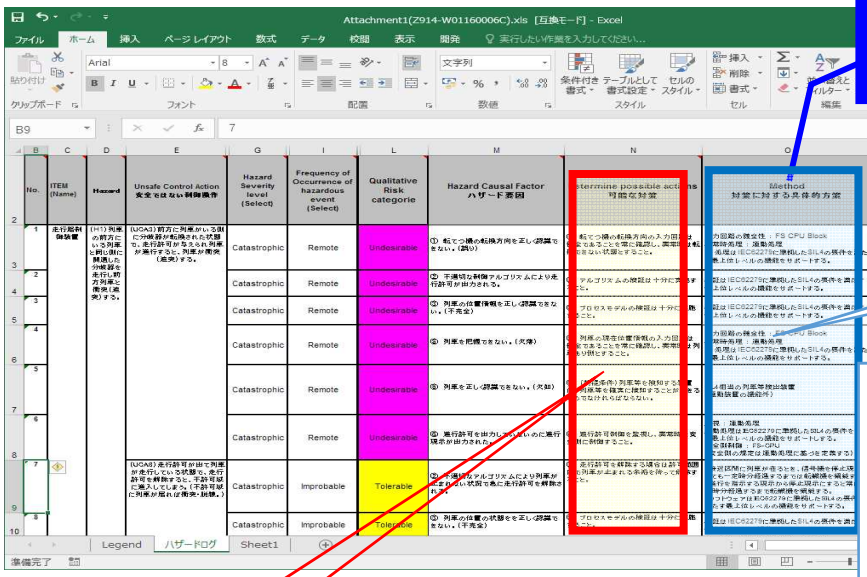
リスク管理

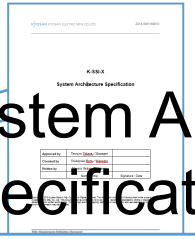


対策に対する具体的方策

対策に対する
具体的方策

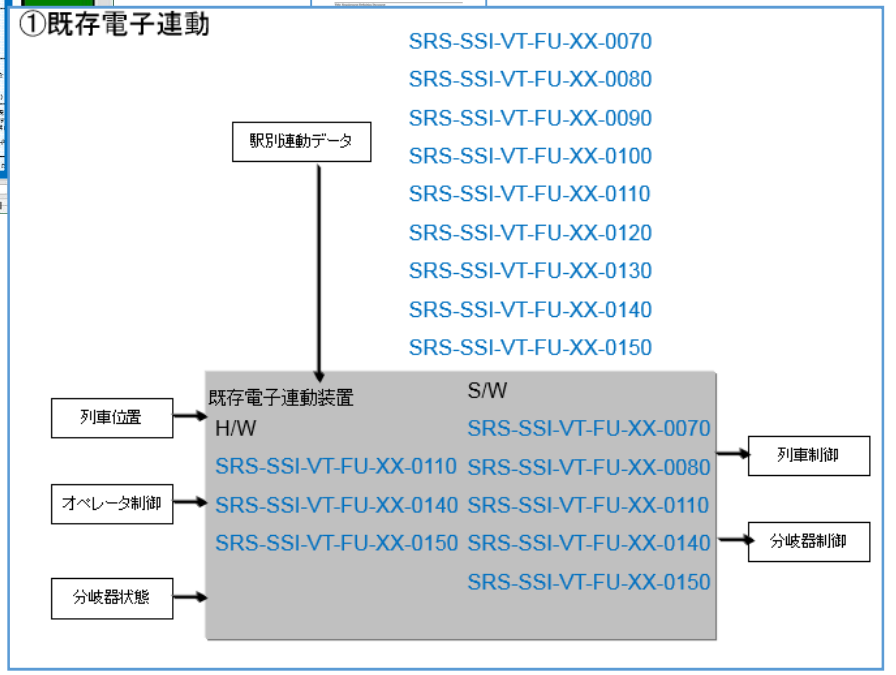
A方式
K５形



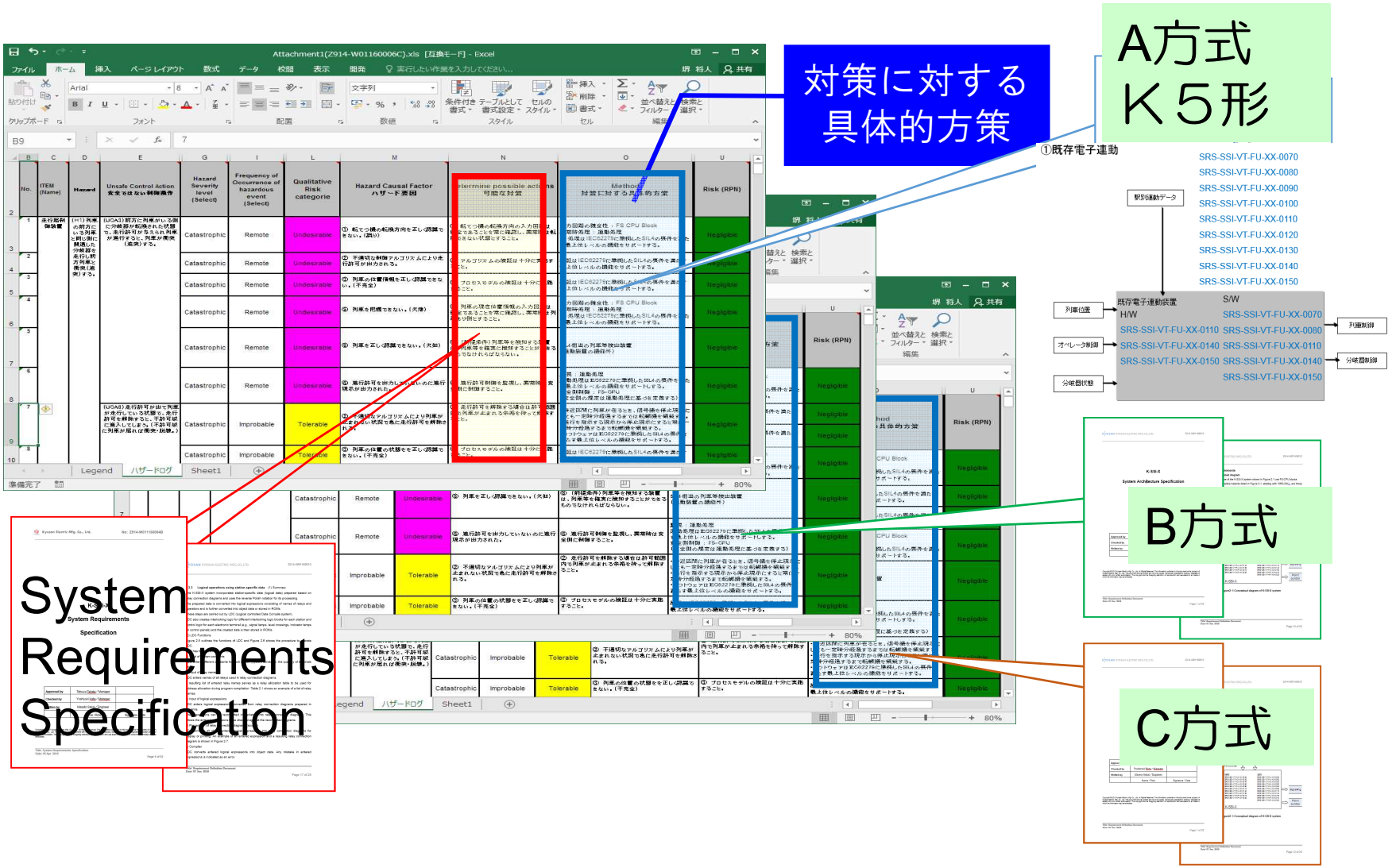


System Architecture Specification

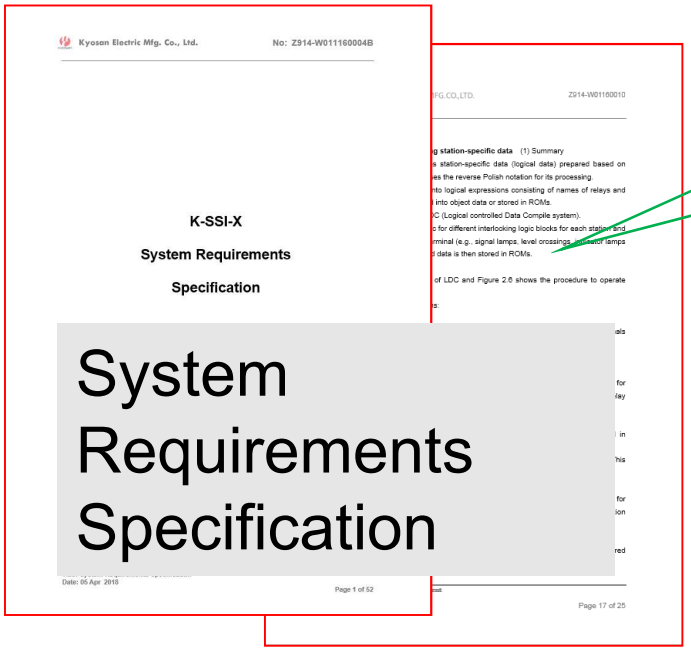
System Requirements Specification



対策に対する具体的方策



対策の確認



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

まとめ

① 解析時に入力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