STAMPトライアル
～踏切に関する人間が絡むシステム事例～
とりこ検知

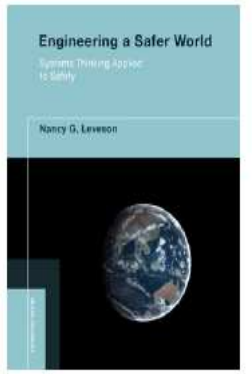
2022年１０月５日

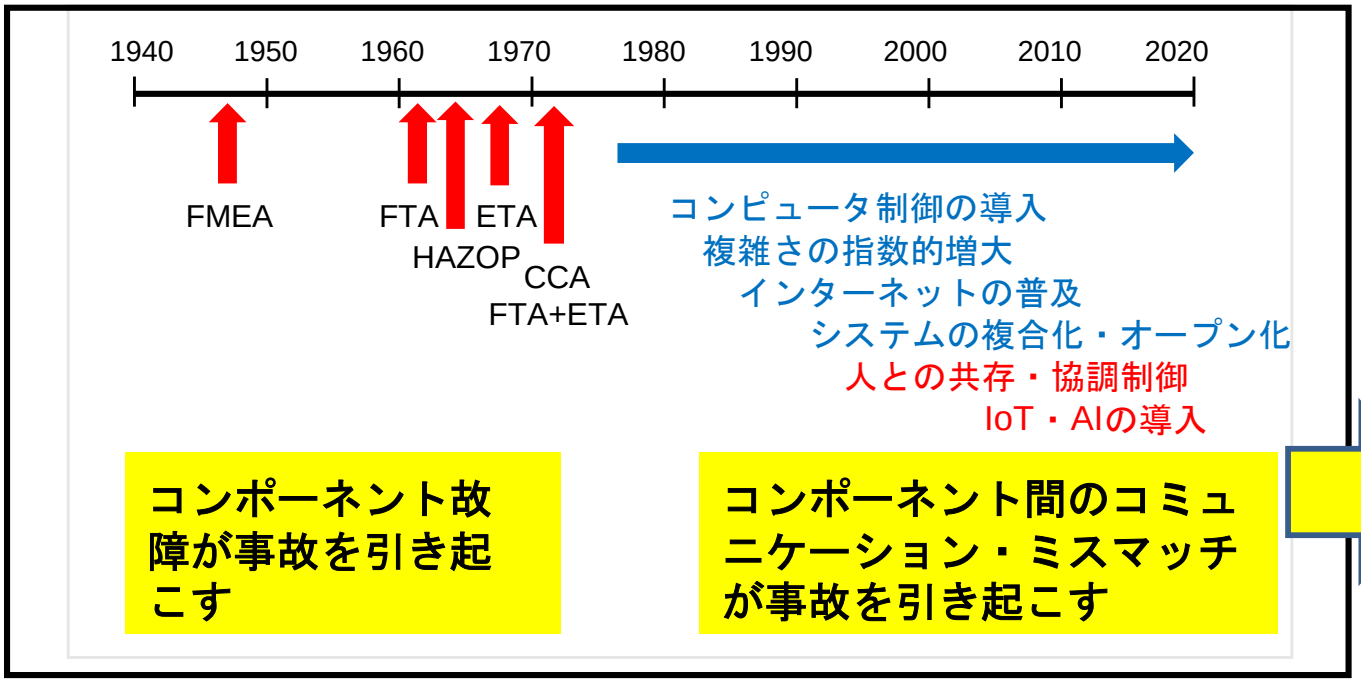
安全性向上委員会
三原　幸博

IoT時代の環境変化と新しい安全解析法　STAMP

Sec-Seminar(2015.6.18) Lecture by Nancy Leveson

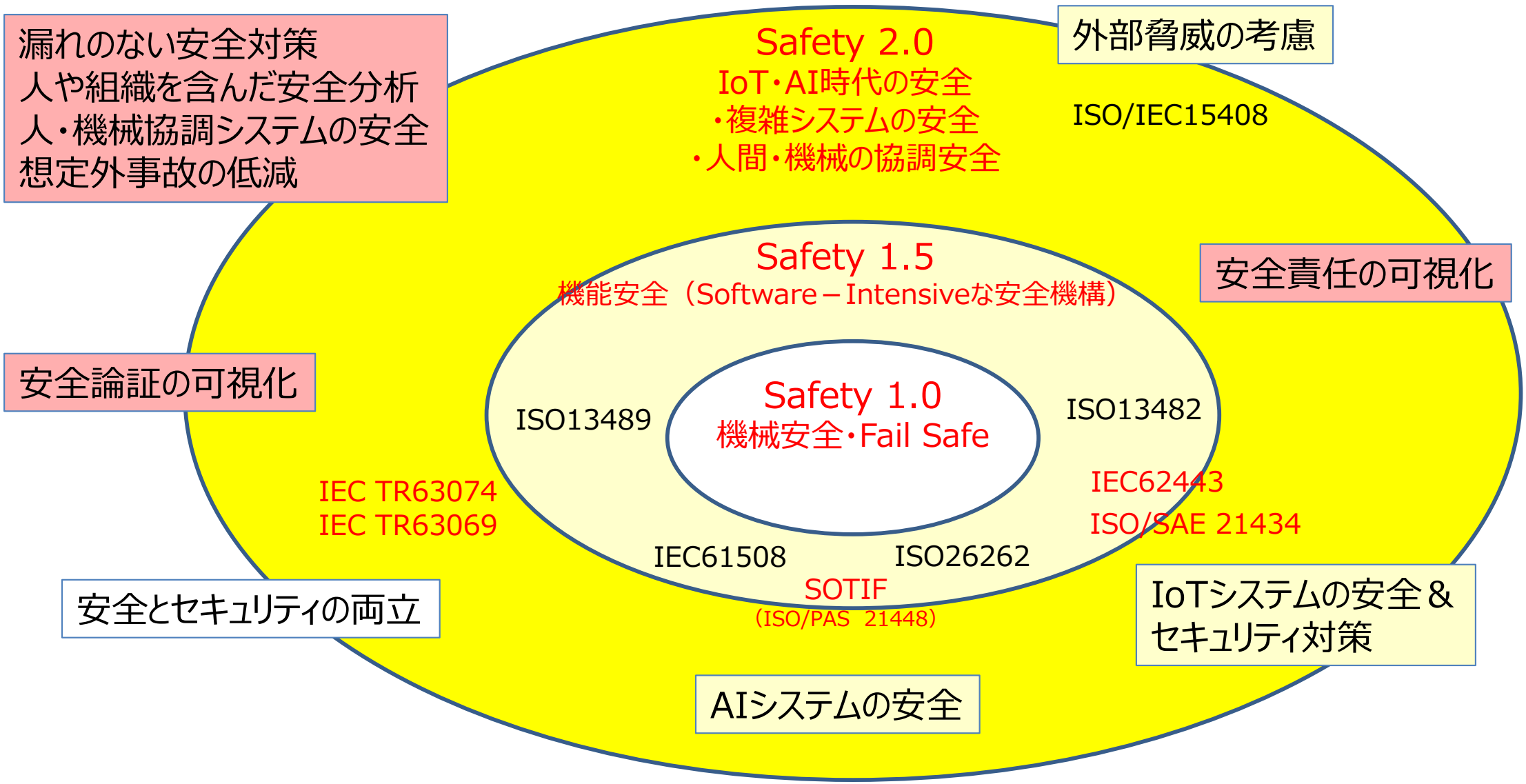
現状の安全分析ツールは、40-65年も昔に開発されたものであり、現代の新しい技術の入った複雑な工学システムの安全分析には限界がある
安全分析のパラダイムシフトが必要　→　***STAMPの登場***





故障がなくても事故は起こる。
◇要求仕様の欠陥
◇コンポーネントの性能限界
◇Worst Caseの想定不足

複雑システムでの安全分析（規格）の発展



京浜急行踏切事故（2019年9月5日11時40分）

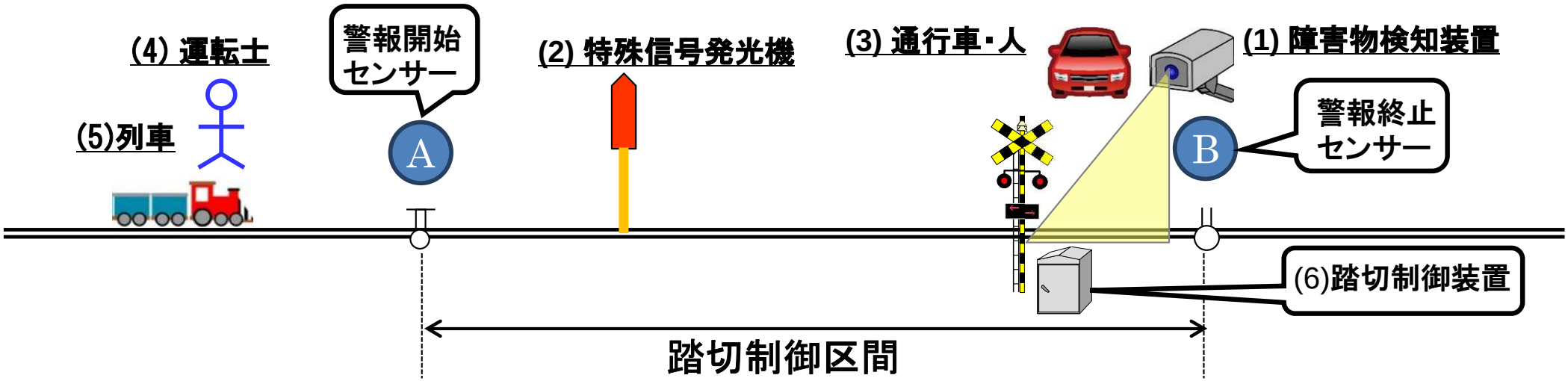
神奈川新町～仲木戸間の踏切で大型トラックと衝突

踏切に設置した**障害物検知装置**で停止信号を点灯
- カーブがあるが、570m手前で確認可能
- 時速120kmで走行時の制動距離は517.5m（空走距離は33m／秒）
- 社内規定では、信号機点滅を確認した場合、「**速やかに停止**」としていたが、今後、「**直ちに非常ブレーキ**」に変更するとのこと
- 運転士は、「速やかに停止」の場合、常用ブレーキか非常ブレーキ併用かの判断が必要

対象システム

■とりこ検知システムの登場人物

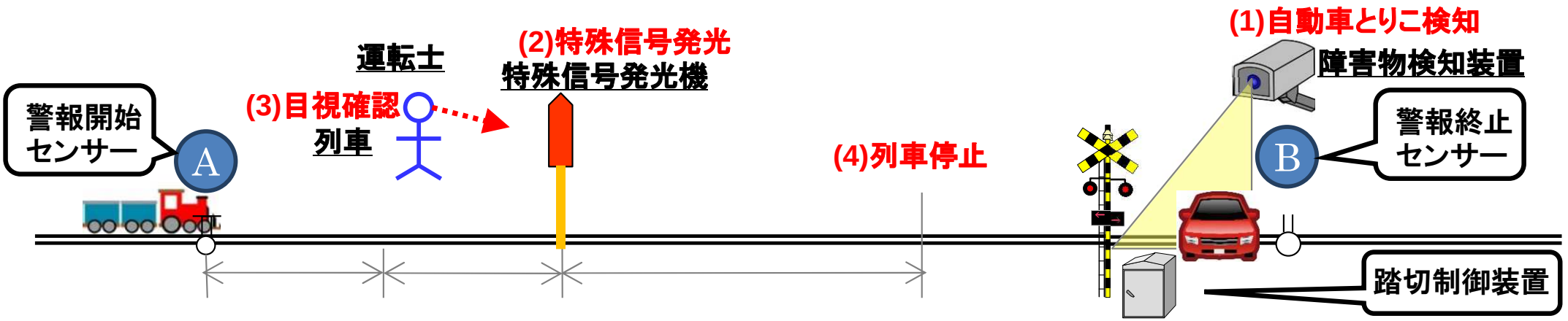
	登場人物	役割(安全関連責任)	備考
1	障害物検知装置	踏切遮断中に通行車・人があるか否か検知し、検知すると特殊信号発光機に点灯指示を出す。“とりこ”解消時に特殊信号発光機に消灯指示を出す。	
2	特殊信号発光機	障害物検知装置からの指示を受けて点灯・消灯する。	
3	通行車・人	踏切を通行する車・人。踏切遮断開始時に、踏切に進入してはならない。また踏切から退出しなければならない。退出できずに滞留すると“とりこ”という。	
4	運転士	特殊信号発光機の発光を確認(視認)するとブレーキをかけて列車を緊急停止させる。(“とりこ”との衝突回避)	目視
5	列車	運転士に制御されて踏切に向かって進行中の列車	
6	踏切制御装置	列車の接近をセンサーで検知して踏切を遮断するとともに障害物検知装置に動作開始を指示する。また列車通過完了をセンサーで検知して踏切を開通するとともに障害物検知装置に動作終了を指示する。	



とりこ検知

	手順	機械の動き	人の動き	備考
1	開始	踏切遮断動作開始	・通行車、人が踏切から退避	
2	開始	検知開始	・通行車、人が踏切内に滞留	
3	発生	踏切道上の通行車を検知	ー	
4	対応	特殊信号発光機が発光	• 運転士が特殊信号を認識	目視による
5	対応	ー〃ー	• 運転士が列車にブレーキをかける	マニュアルブレーキ

“とりこ検知”とは、障害物検知装置が列車の運転士に“とりこ”を知らせてブレーキをかけさせることで踏切の安全を守るシステム（機能）である。



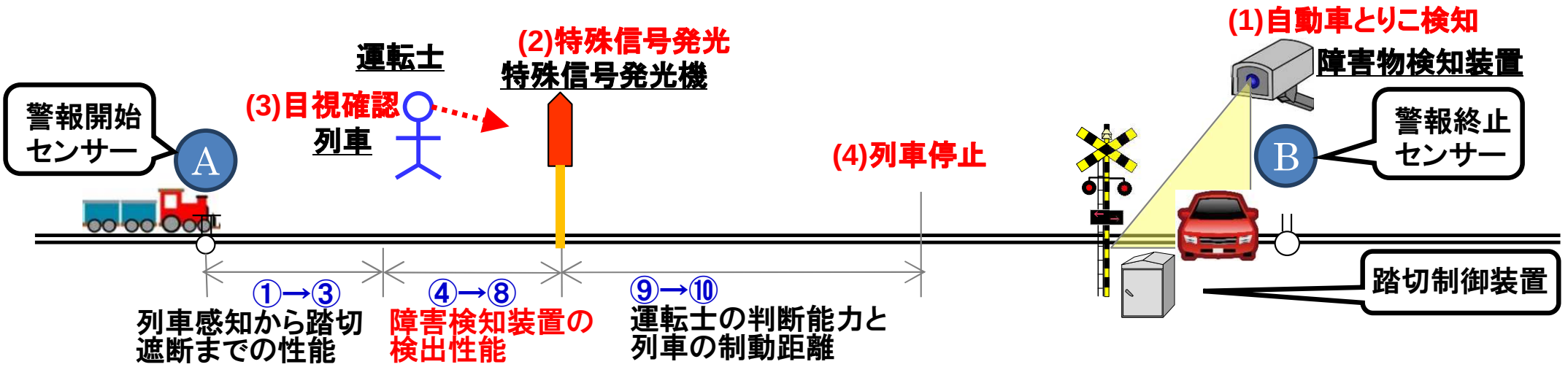
とりこ検知　前提条件

1. 踏切遮断機・警報機は正常に機能するものとする
2. 分析範囲は、とりこ発生（踏切が遮断後）から列車停止までとし、列車停止後に乗客が線路に降りる、線路上を歩く、ことによるアクシデントは分析対象外とする
3. 障害検知装置はカメラと画像診断装置によるものとする

以下、分析の過程で追加した前提条件

4. 障害検知は、踏切が遮断後に作動する（障害物検知装置は障害物になることの予測機能を持たない）
5. とりこ状態が解消されると特殊信号発光機を消灯する
6. 特殊信号発光機、警報開始センサー、踏切の設置場所と各装置の性能の関係は次頁メモの通りとする

メモ：各装置の設置位置と役割



今回の分析範囲は④から⑨

障害検知システムの動作シーケンス（仕様）

① 開始センサーが列車到達を感知
- 相互作用：センサー→制御装置

② 踏切制御装置が遮断指示を送出
- 相互作用：制御装置→遮断機

③ 遮断機が遮断完了
- 相互作用：遮断機→制御装置→検知装置

④ 障害検知装置が検知開始

⑤ 障害検知/障害解消検知

⑥ 信号発光指示/消灯指示
- 相互作用：検知装置→信号発光機

⑦ 信号発光/消灯

⑧ 運転士が目視確認
- 相互作用：信号発光機→運転士

⑨ 停止判断、マニュアルブレーキ作動開始
- 相互作用：運転士→列車

⑩ 列車停止

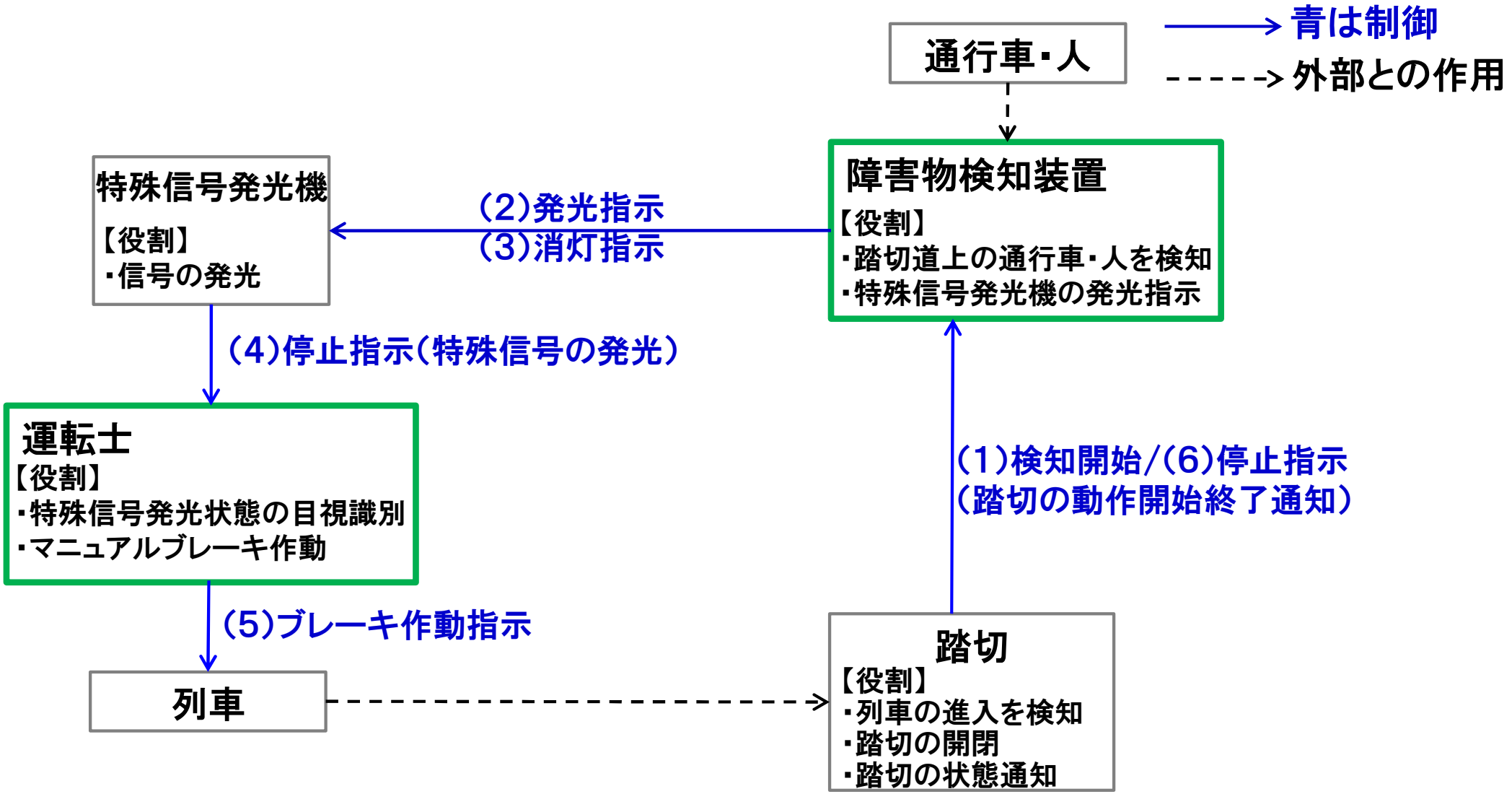
準備1　安全制約の識別

■ アクシデント、ハザード、安全制約の識別

アクシデント(Loss)	ハザード(Hazard)	安全制約(Safety Constraints)
(A1)列車が“とりこ”状態の車と衝突する。 ・通行中の人、車の運転手が死傷する ・列車の乗員、乗客が死傷する	(H1-1)“とりこ”発生時に特殊信号発光機が発光しない	(SC1-1)“とりこ”発生時に特殊信号発光機が発光すること
	(H1-2)“とりこ”発生中に特殊信号発光機の発光が停止する	(SC1-2)“とりこ”発生中は特殊信号発光機の発光が停止しないこと
	(H1-3)特殊信号発光機の発光を乗務員が目視確認できない	(SC1-3)特殊信号発光機の発光を乗務員が目視確認できること
(A2)特殊信号発光機が発光し続けて列車が走行できない	(H2-1)“とりこ”が発生していないのに特殊信号発光機が発光	(SC2-1)“とりこ”が発生していない時は特殊信号発光機は発光してはならない
	(H2-2)“とりこ”対応処理完了後特殊信号発光機の発光停止できない	(SC2-2)対応処理完了後特殊信号発光機の発光停止できなければならない

A2は、人命・財産喪失という重大アクシデントではないため、分析対象外にした。

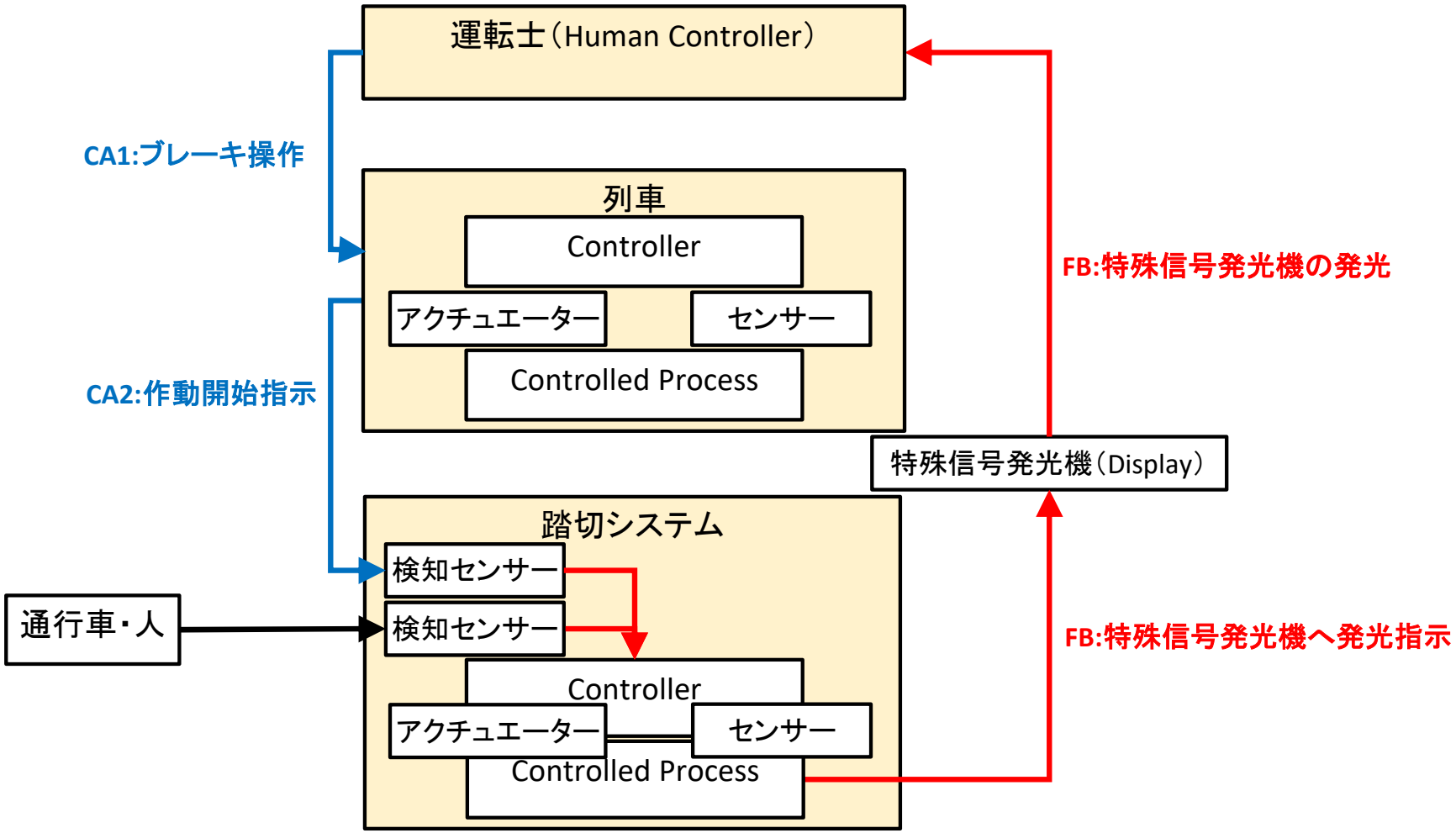
準備2　コントロールストラクチャの構築



“とりこ検知”の流れに沿ったコントロールストラクチャー

準備2　コントロールストラクチャの構築

指示系統の上下関係を階層的に表現している

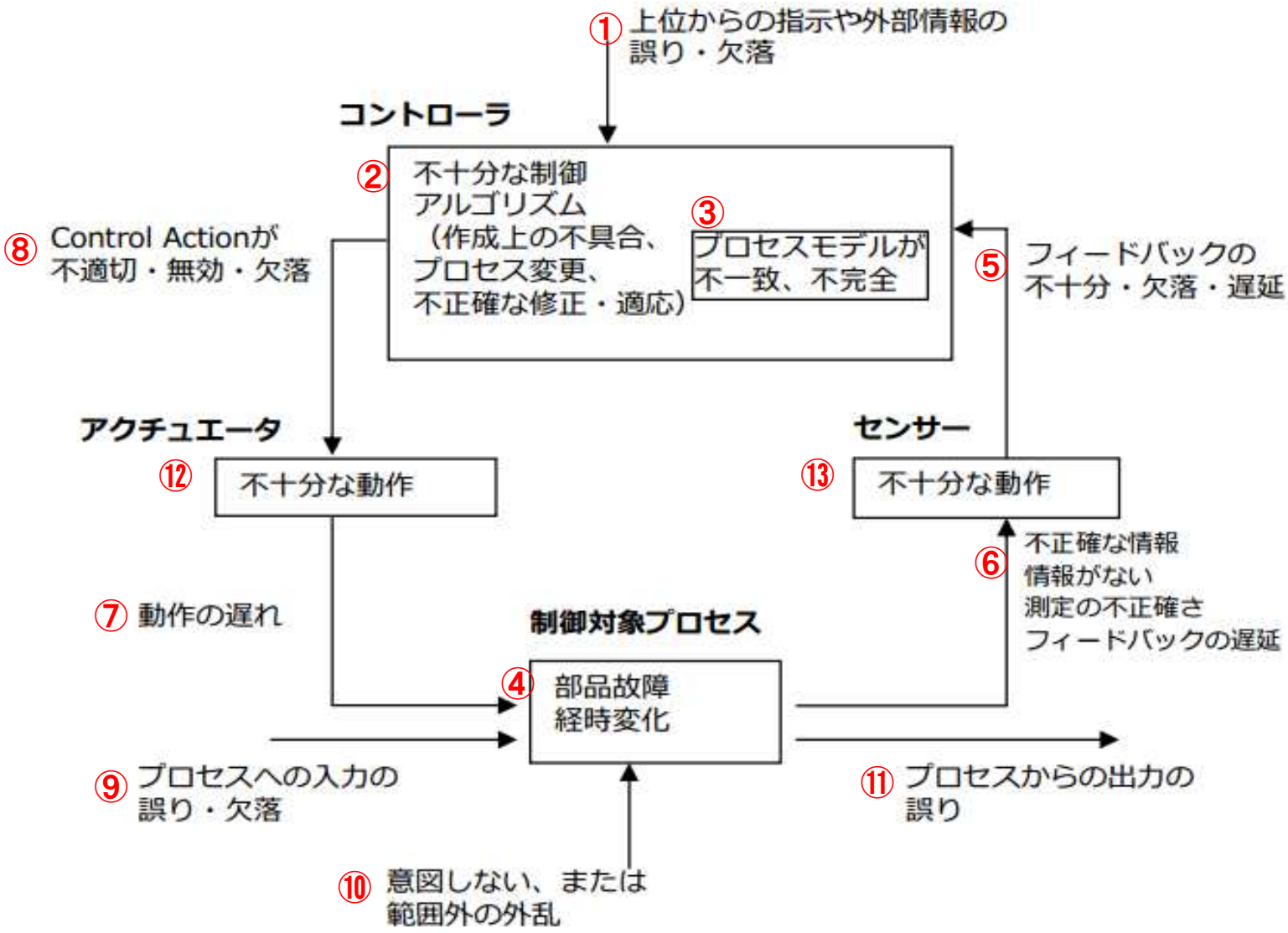


運転士を中心にしたコントロールストラクチャー

Step1　UCAの識別

#	コントロールアクション	Not Providing	Providing causes hazard	Too early / Too Late	Stop too soon / Applying too long
1	(踏切→検知装置)検知開始指示(踏切の動作開始通知)	(UCA1-N)検知開始指示が出ないので検知できないので発光せず　SC1-1違反	踏切開状態で特殊信号発光機を発光する	(UCA1-T)Too Lateで検知開始が遅れ、特殊信号発光機の発光が遅れるので検知できない時間がある SC1-1違反 Too earlyで“とりこ”でない車を検知し発光指示する可能性あるがハザードにはならない	ー
2	(検知装置→特殊信号発光機)発光指示	(UCA2-N)とりこがあっても発光せず列車を停止させない　SC1-1違反	“とりこ”がないのに発光して列車を停止させる	(UCA2-T)Too lateで発光開始が遅れ、列車が停止できない(ブレーキをかけるのが遅れる)　SC1-1違反	ー
3	(検知装置→特殊信号発光機)消灯指示	“とりこ”解消しても特殊信号発光機消灯せず	(UCA3-P)“とりこ”中に特殊信号発光機消灯SC1-2違反	(UCA3-T)Too early　同左	
4	(特殊信号発光機→運転士)停止指示(特殊信号の発光)	(UCA4-N)“とりこ”があっても発光せず列車を停止しない　SC1-1違反	“とりこ”がないのに発光し列車を停止させる	(UCA4-T)Too lateで発光開始が遅れ、列車が停止できない(ブレーキをかけるのが遅い)　SC1-1違反	ー
5	(運転士→列車)ブレーキ作動指示	(UCA5-N)運転士が特殊信号発光機の発光を認識できず列車を停止しない SC1-3違反	“とりこ”がないのに停止する	(UCA)Too lateで列車停止が間に合わない(ブレーキをかけるのが遅い) →今回対象外とする	(UCA)Too soonで列車停止が間に合わない(ブレーキを途中で解除)　→今回対象外とする
6	(踏切→検知装置)検知停止指示(踏切の動作停止通知)	“とりこ”がないのに発光し列車を停止させる	(UCA6-P)列車が在線中に検知停止指示が出ると“とりこ”があっても発光せず列車を停止させない　SC1-2違反	(UCA6-T)Too earlyで“とりこ”があっても発光せず列車を停止させない　SC1-2違反	ー

HCF導出のための11個のガイドワード



①上位からの指示や外部情報の誤り・欠落

②不適切な制御アルゴリズム（作成時の欠陥、プロセス変更、誤った修正・適用）

③プロセスモデルが不一致、不完全、不正確。不適切な操作

④部品故障、経年変化

⑤フィードバックの不十分・欠落・遅延

⑥不正確な情報、情報の欠如。測定の不正確性。フィードバック遅延

⑦動作の遅れ

⑧Control actionが不適切・無効・欠落

⑨制御行動の衝突。プロセス入力の誤り・欠落

⑩意図しない、または範囲外の外乱

⑪プロセス出力の誤り

次頁以降では、前ページのCSDの中にあるコントロールループ毎に、上記ガイドワードを適用して、HCFを導出する。

人対人 のHCF導出のためのヒント

指示主体(人)

(C1)指示が必要と思っていない
(C2)指示を知っていたが忘れる
(C3)指示内容を間違える
(C4)指示したつもり
(C5)思い出す(遅れる)
(C6)指示内容を勘違い(取り違える)
(C7)違う相手に指示を出す
(C8)確認せずに見込みで指示を出す

指示(口頭・電話・メイル・FAXなど光、音、旗)

(A1)指示が伝わらない(悪環境で阻害/伝達手段故障)
(A2)指示手段が不適切など
(A3) 指示が遅れる
(A4)間違った指示の混入

悪環境の例
発光を認識できない理由
・雪、雨、霧による視界不良
・逆光が強い
・線路が大きくカーブしている
・途中にトンネルがある
・途中に遮蔽物(木など)がある
・不適切な装備(サングラスなど)
・騒音で聞こえない

被指示主体(人)

(P1)指示が来たが受け取らない
(P2)指示を誤解して実行する
(P3)指示どおりの実行ができないまたは遅れる(不適切な環境やスキル不足のため健康状態不良)
(P4)実行結果のフィードバックを忘れる
(P5)思い出す(遅れる)

フィードバック(口頭・電話・メイル・FAXなど)

(F1)フィードバックが伝わらない(悪環境で阻害/伝達手段故障)
(F2)指示手段が不適切
(F3)フィードバックの遅れ
(F4)間違ったフィードバック

人対機械 のHCF導出のためのヒント

指示(操作:SW,KB)

(A1)指示が伝わらない(故障)
(A2)指示が遅れる(故障)
(A3)間違った指示の混入

指示主体(人)

(C1)指示が必要と思っていない
(C2)指示を知っていたが忘れる
(C3)指示内容を間違える
(C4)指示したつもり
(C5)思い出す(遅れる)
(C6)指示内容を勘違い(取り違える)
(C7)違う相手に指示を出す
(C8)確認せずに見込みで指示を出す

被指示主体(機械)

(P1)指示が来たが受け取れない(故障)
(P2)指示どおりの実行ができないまたは遅れる(故障又は不適切なアルゴリズム)
(P3)間違った指示で対応できない

フィードバック(口頭・電話・メイル・FAXなど)

(F1)フィードバックが伝わらない(悪環境で阻害、指示手段が不適切など)
(F2)フィードバックの遅れ
(F3)間違ったフィードバック

悪環境の例
発光を認識できない理由
・雪、雨、霧による視界不良
・逆光が強い
・線路が大きくカーブしている
・途中にトンネルがある
・途中に遮蔽物(木など)がある
・不適切な装備(サングラスなど)
・騒音で聞こえない

機械対人 のHCF導出のためのヒント

指示主体(機械)

(C1)プロセスモデルの誤り
(C2)不適切なアルゴリズム
(C3)故障による不指示
(C4)性能不足による遅れ

指示(メッセージ、警報)

(A1)指示がでない(故障)
(A2)指示が伝わらない(悪環境で阻害)
(A3)指示手段が不適切など
(A4)指示が遅れる
(A5)間違った指示

被指示主体(人)

(P1)指示が来たが受け取らない
(P2)指示を誤解して実行する
(P3)指示どおりの実行ができないまたは遅れる(不適切な環境やスキル不足のため健康状態不良)
(P4)実行結果のフィードバックを忘れる
(P5)思い出す(遅れる)

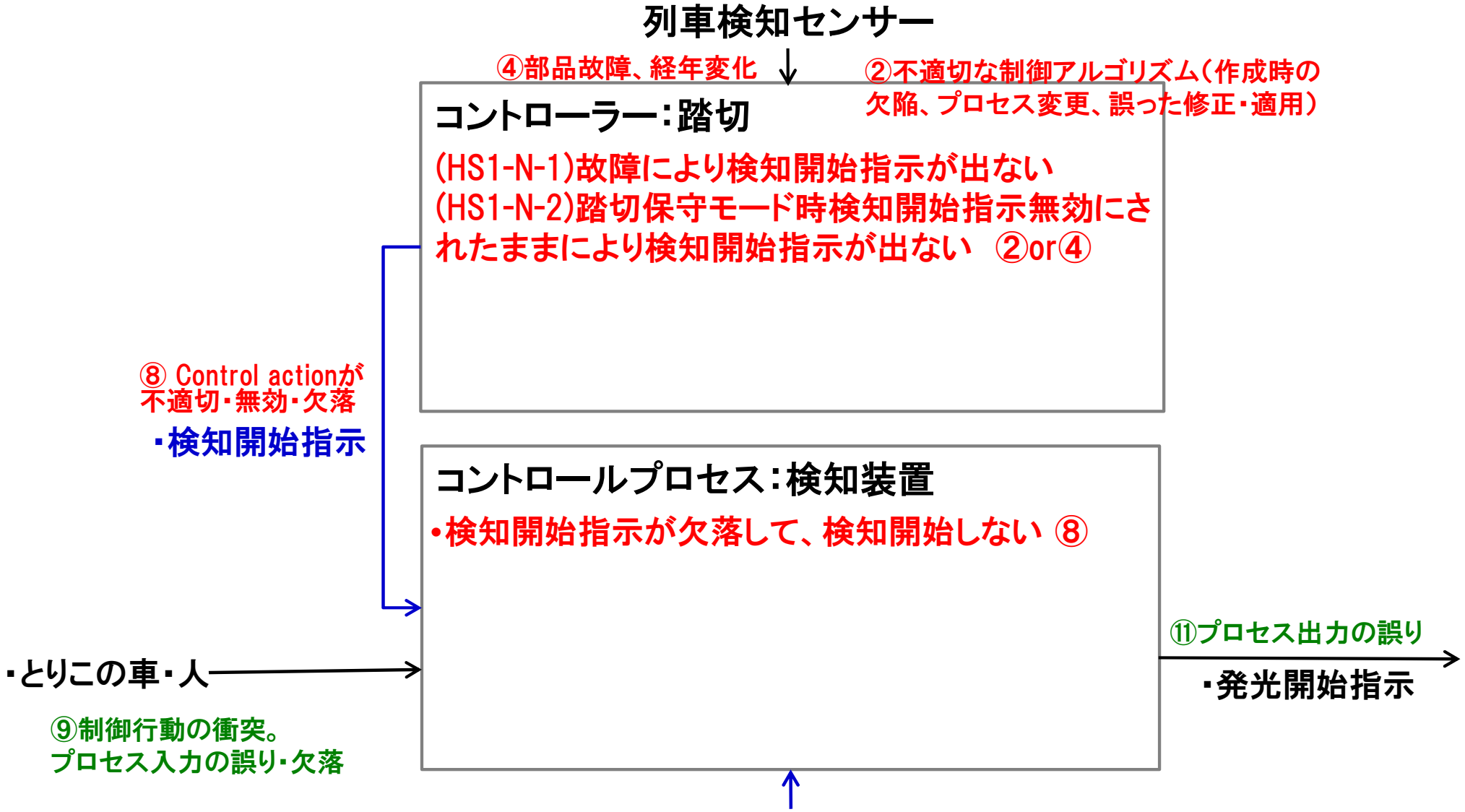
フィードバック(操作:SW、KB)

(F1)フィードバックが伝わらない(故障)
(F2)フィードバックの遅れ(故障・出し遅れ)
(F3)フィードバックでない
(F4)間違ったフィードバック

悪環境の例
発光を認識できない理由
・雪、雨、霧による視界不良
・逆光が強い
・線路が大きくカーブしている
・途中にトンネルがある
・途中に遮蔽物(木など)がある
・不適切な装備(サングラスなど)
・騒音で聞こえない

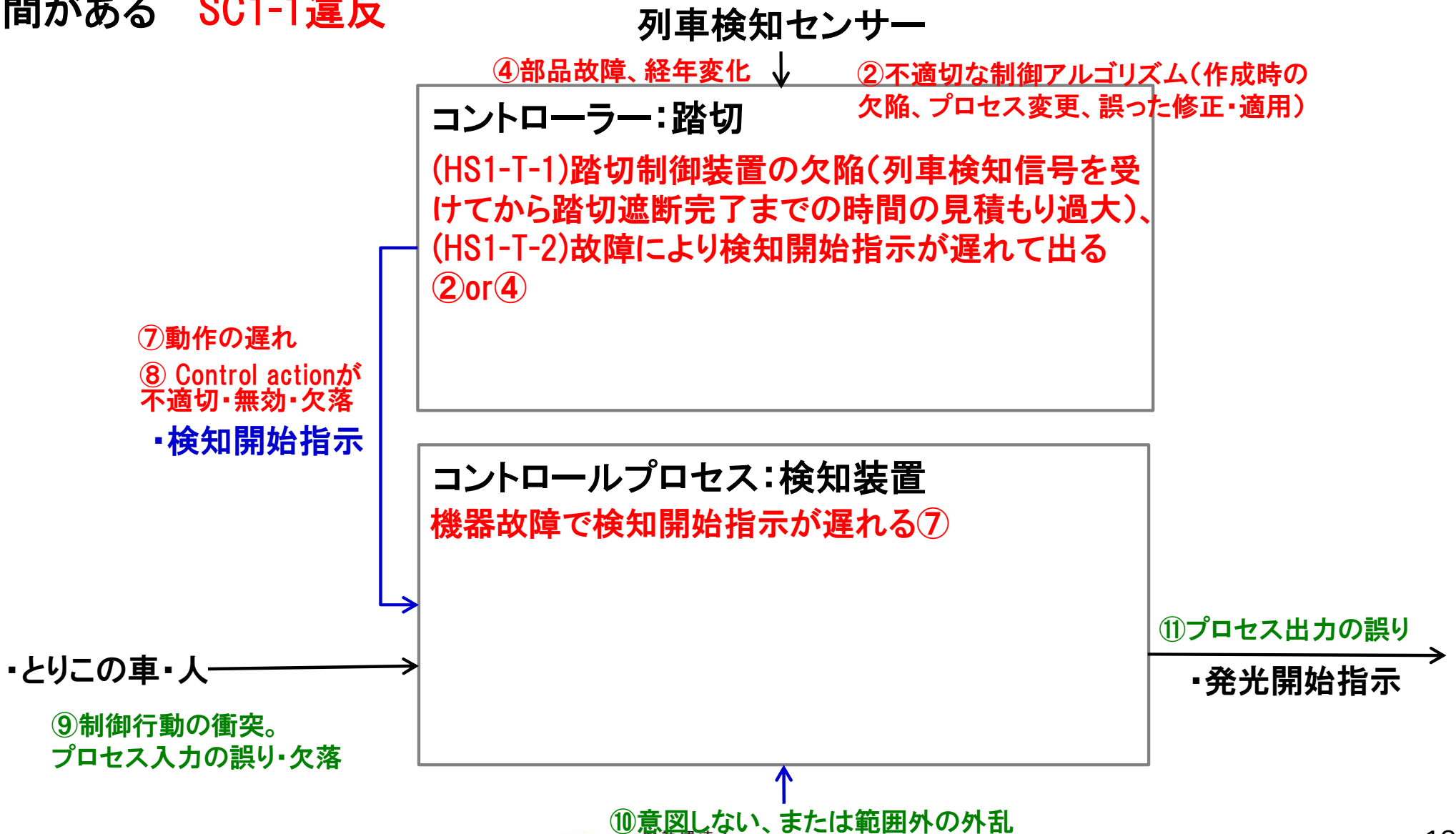
Step2　HCFの導出

(UCA1-N):検知開始指示が出ないので検知できない　SC1-1違反



Step2　HCFの導出

(UCA1-T): Too Lateで検知開始が遅れ、特殊信号の発光が遅れるので検知できない時間がある　SC1-1違反



Step2　HCFの導出

(UCA2-N):“とりこ”があっても発光せず列車を停止しない　SC1-2違反

・検知開始指示

④部品故障、経年変化

②不適切な制御アルゴリズム（作成時の欠陥、プロセス変更、誤った修正・適用）

コントローラー：検知装置

(HS2-N-1)検知装置の故障で“とりこ”発生しても検知できないので、発光開始指示を出さない　②
(HS2-N-2)認識アルゴリズム不良で“とりこ検知”できず発光開始指示出さない
(HS2-N-3)外部環境不良のため“とりこ検知”できず発光開始指示出さない
(HS2-N-4)カメラのレンズが汚れて検知できず

検査装置が正しく認識できない理由
・雪、雨による
・丸い形状（タンクローリー）
・小さ過ぎる（子供、倒れた人、）
・夜（カメラの場合）
・カメラ自体に障害物による遮蔽

⑦動作の遅れ
⑧ Control actionが不適切・無効・欠落
・発光開始指示

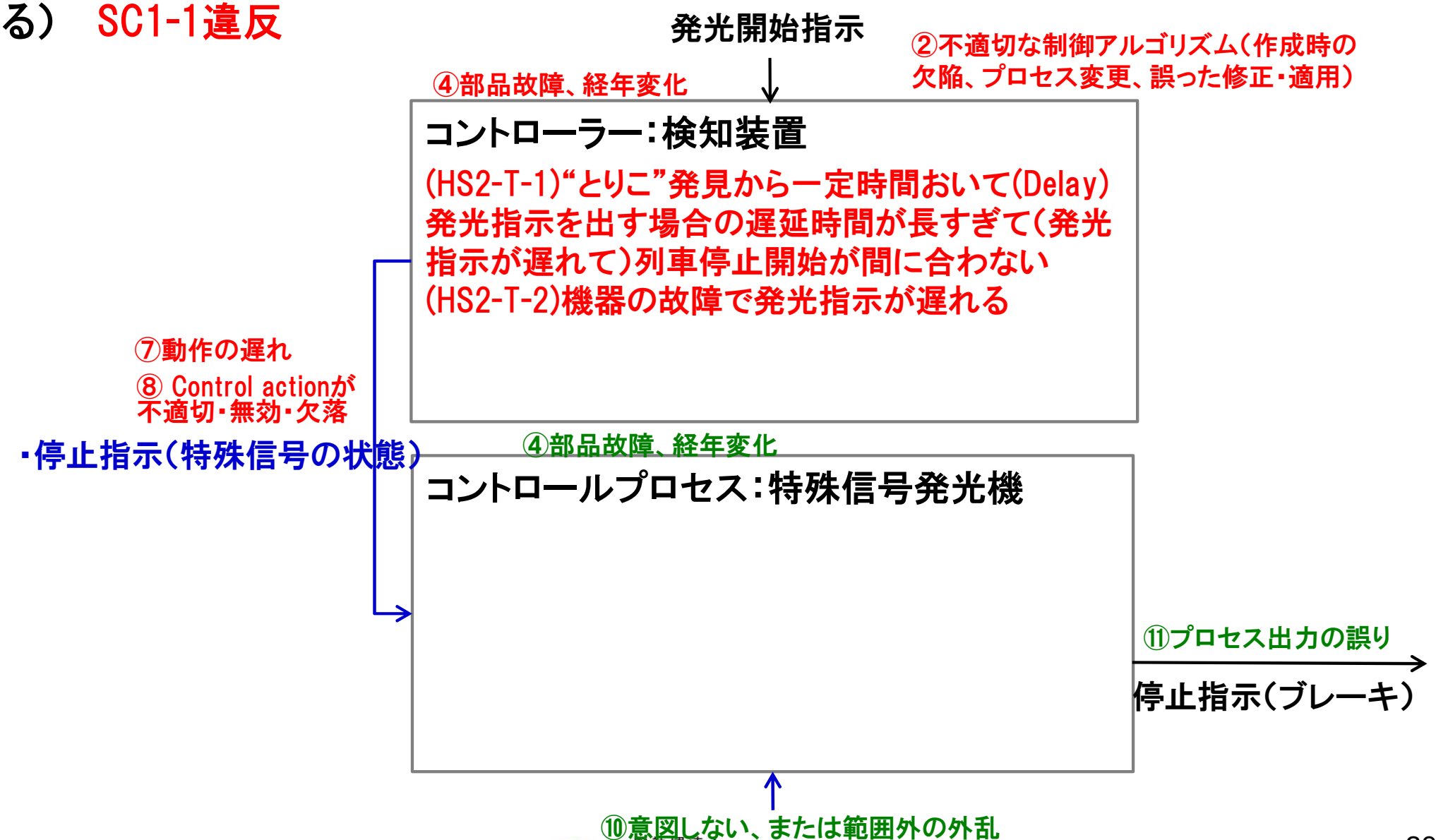
コントロールプロセス：特殊信号発光機

⑪プロセス出力の誤り
・停止指示（発光）

⑩意図しない、または範囲外の外乱

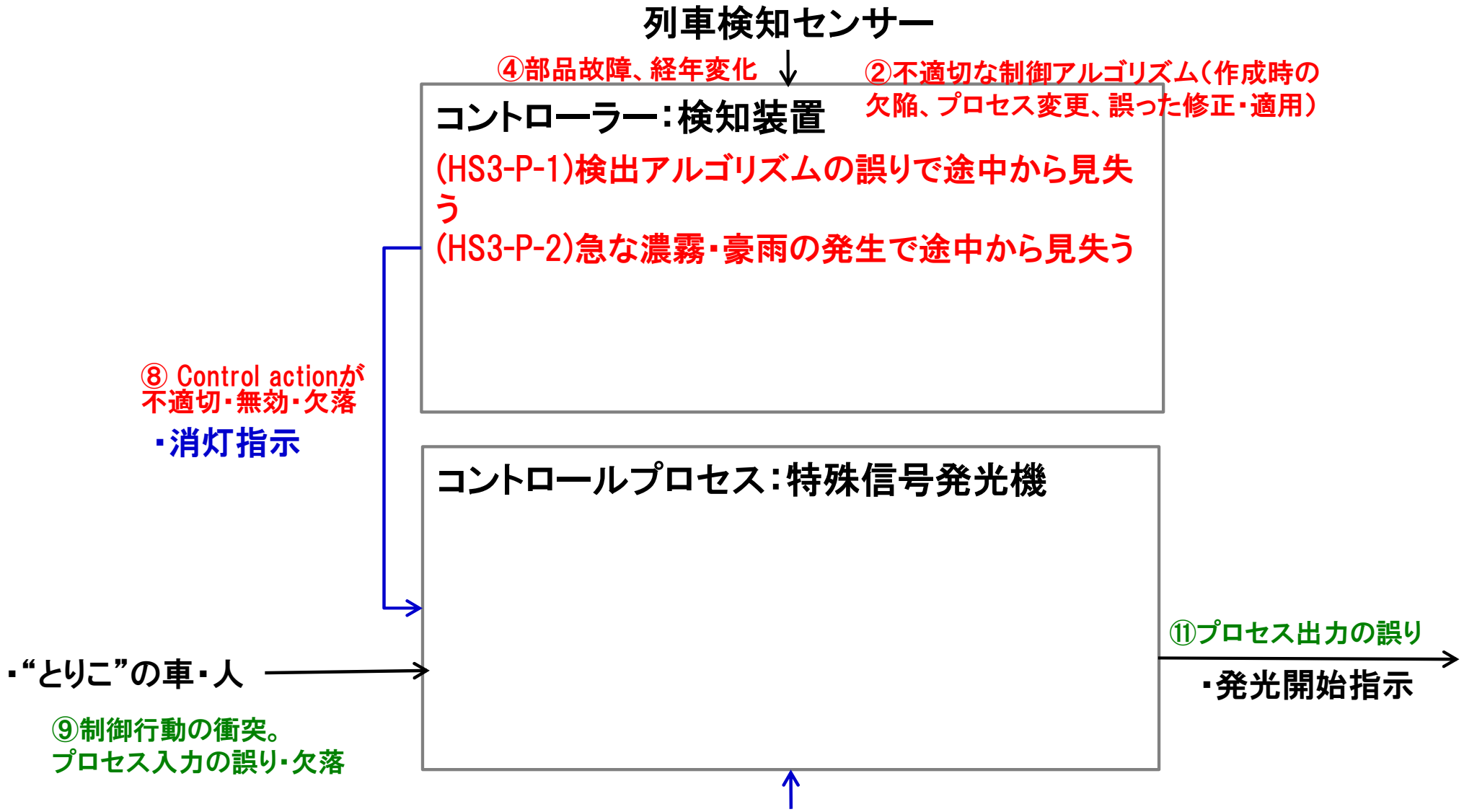
Step2　HCFの導出

(UCA2-T):Too lateで発光開始が遅れ、列車が停止できない(ブレーキをかけるのが遅れる)　SC1-1違反



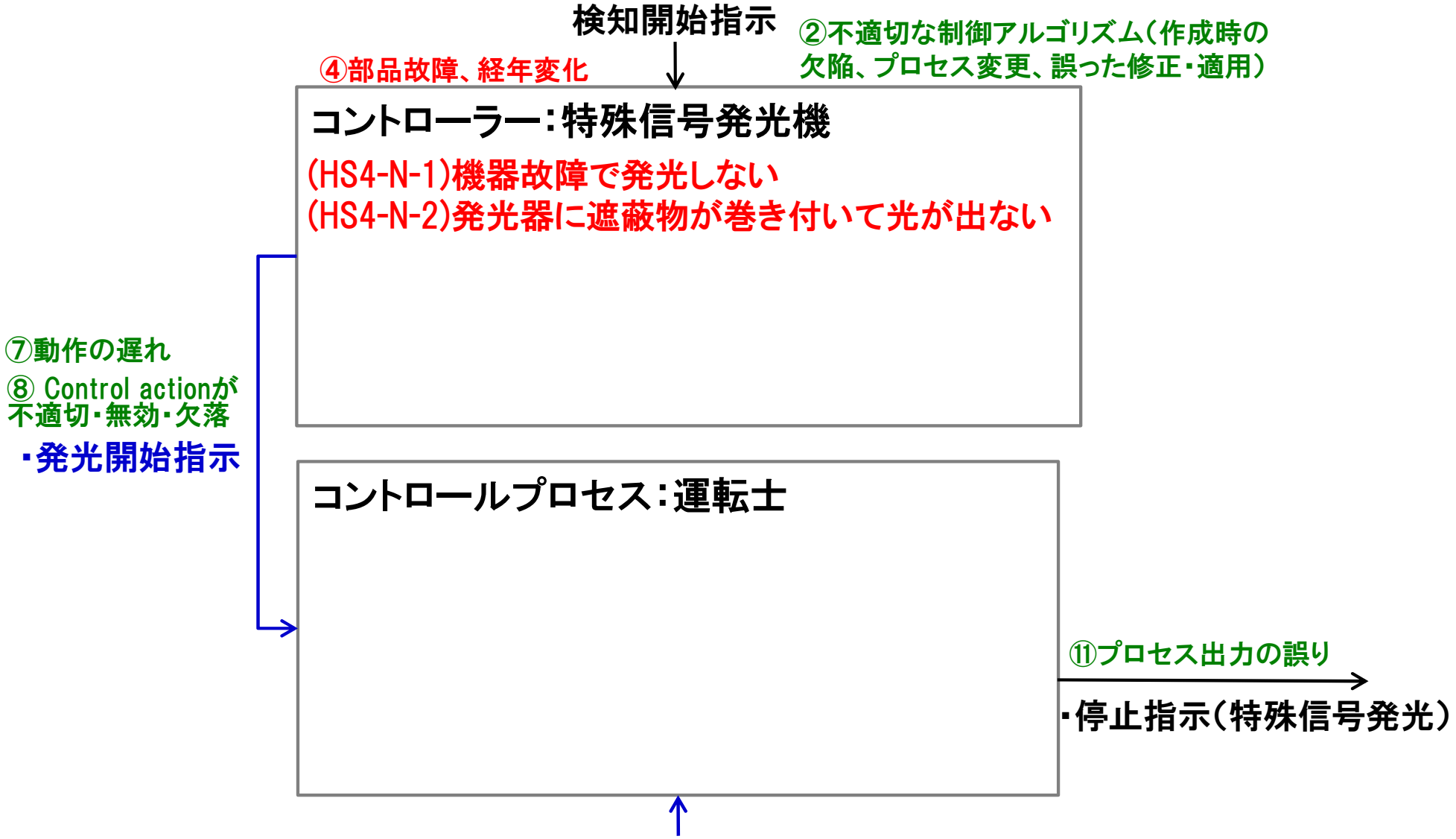
Step2　HCFの導出

(UCA3-P):とりこ中に特殊信号発光機消灯　SC1-2違反



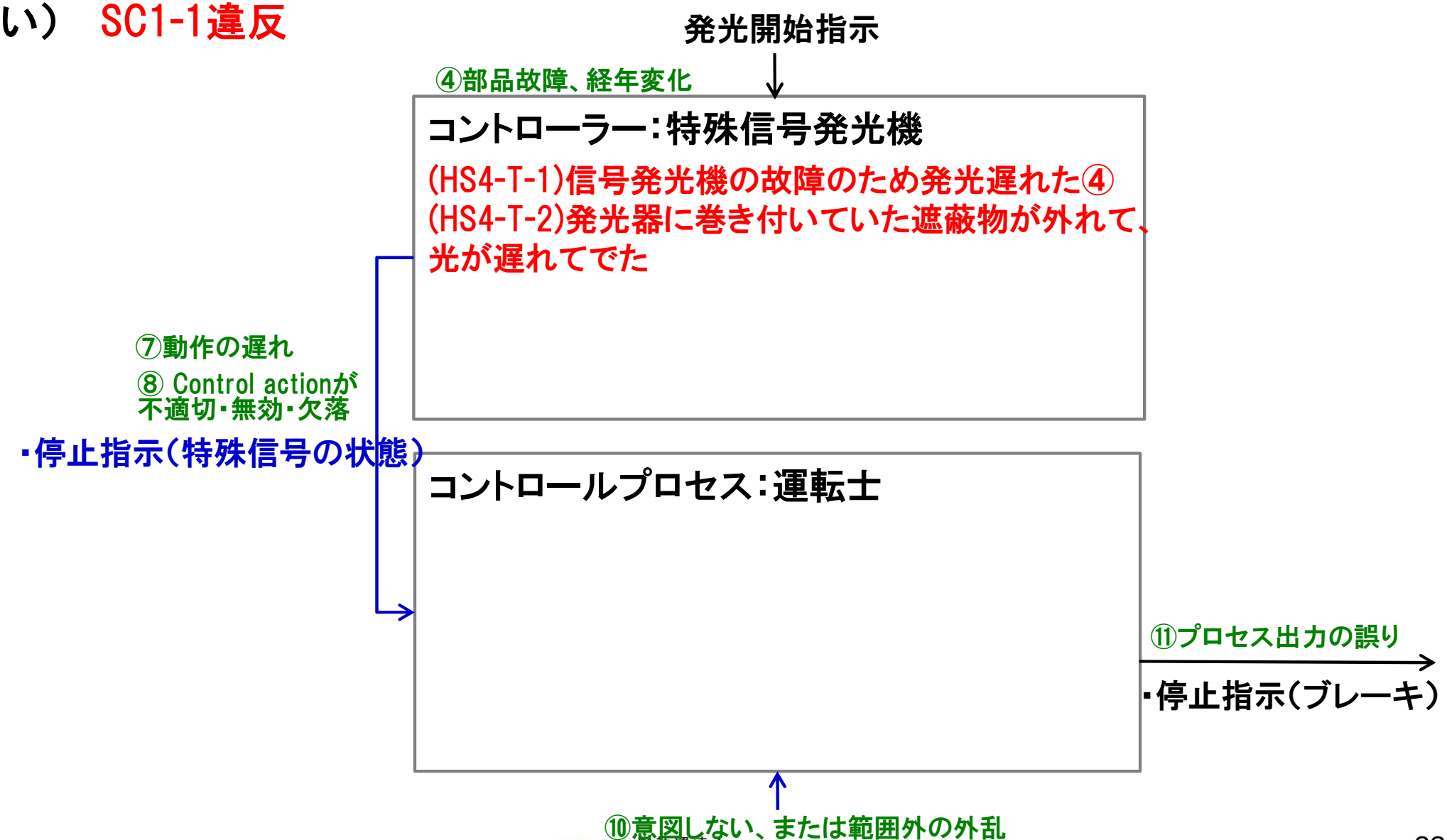
Step2　HCFの導出

(UCA4-N):とりこがあっても発光せず列車を停止しない　SC1-1違反



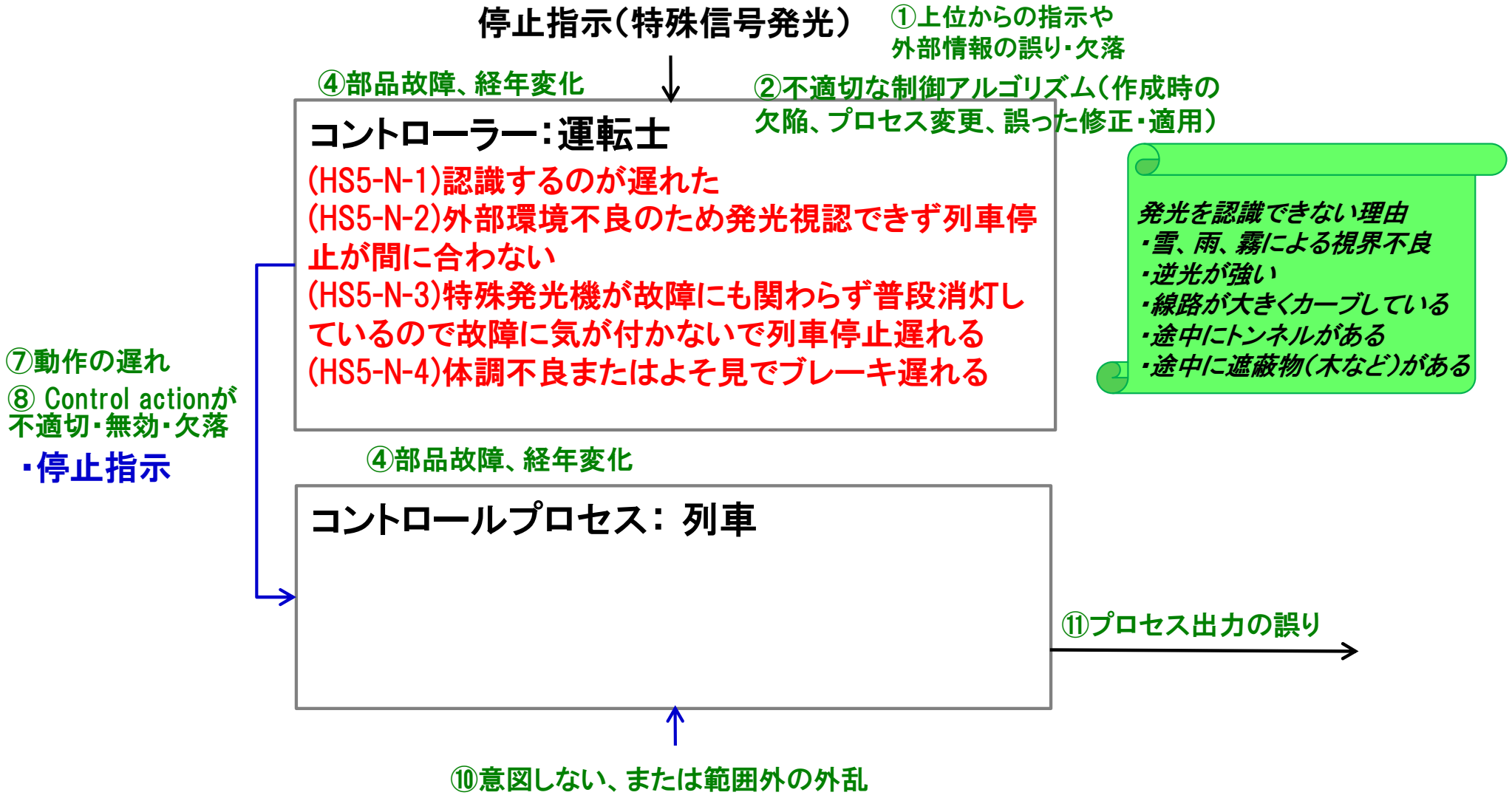
Step2　HCFの導出

(UCA4-T):Too lateで発光開始が遅れ、列車が停止できない(ブレーキをかけるのが遅い)　SC1-1違反



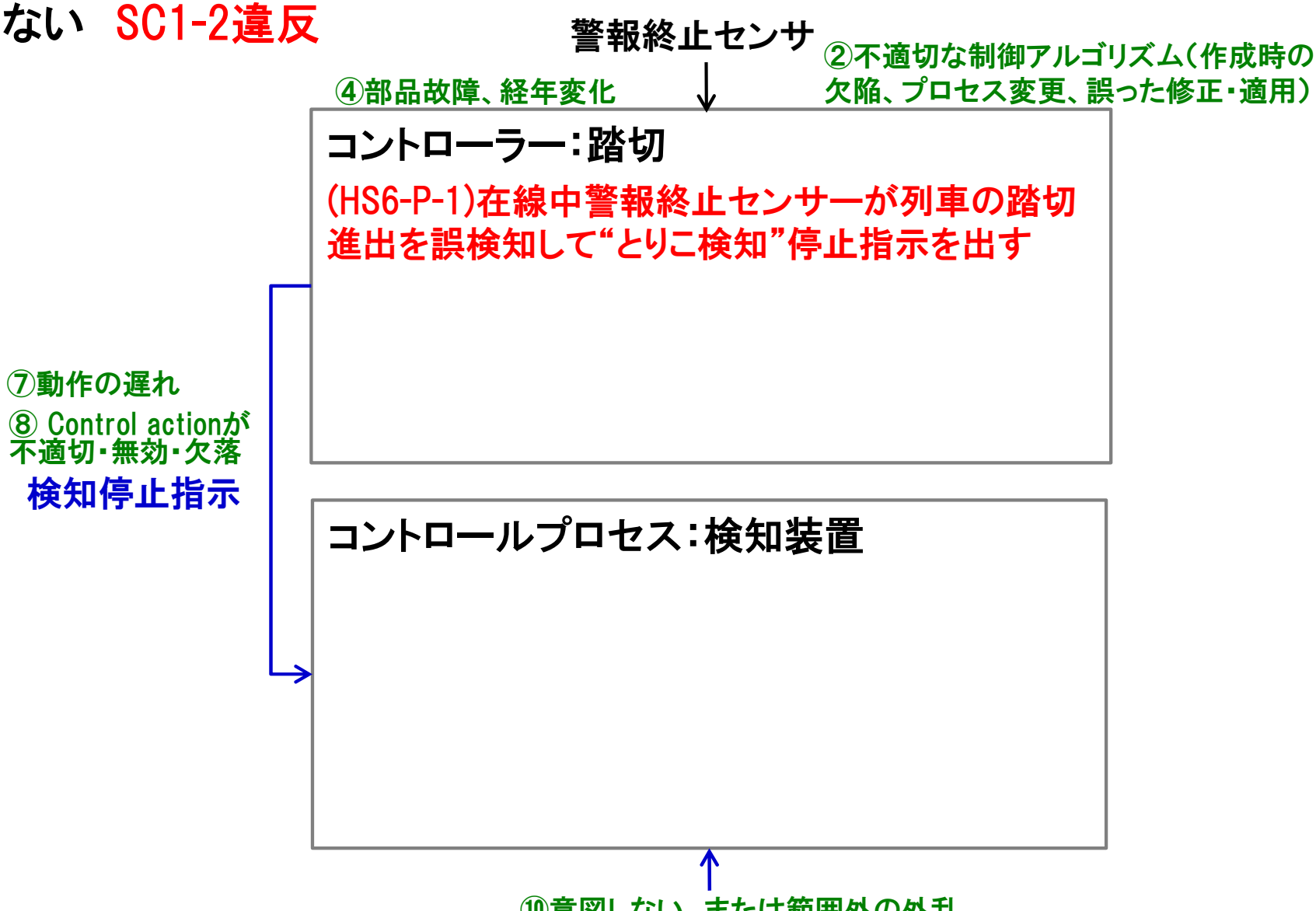
Step2　HCFの導出

(UCA5-N):運転士が特殊信号発光機の発光を認識できず列車を停止しない SC1-3違反



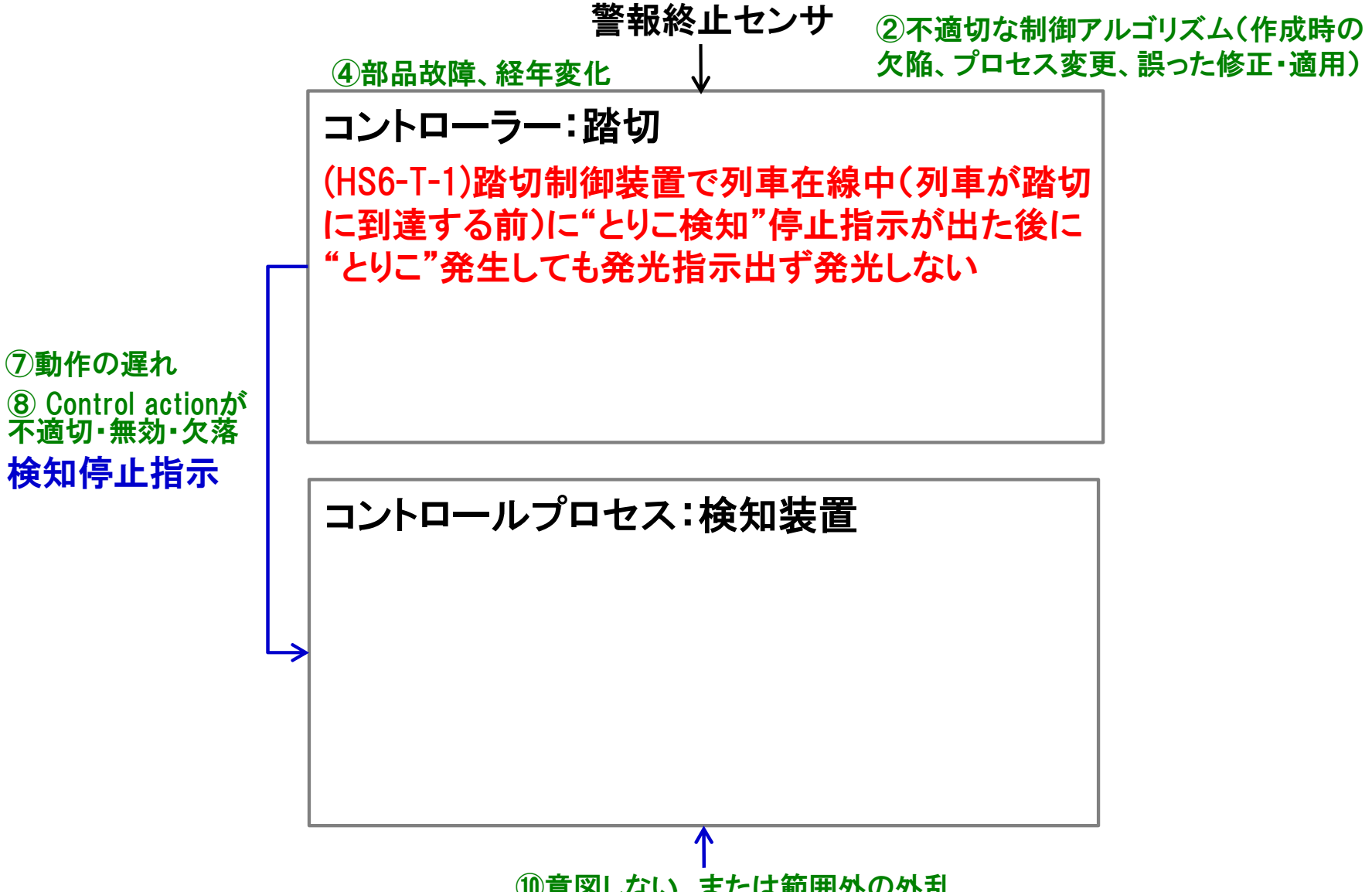
Step2　HCFの導出

(UCA6-P):列車が在線中に検知停止指示が出ると、“とりこ”があっても発光せず列車を停止させない　SC1-2違反



Step2　HCFの導出

(UCA6-T):Too earlyで“とりこ”があっても発光せず列車を停止させない　SC1-2違反



HCF一覧（1／3）

UCA/シナリオ		対策
UCA1-N(踏切→検知装置)	検知開始指示が出ないので検知できない　安全制約1-1違反	
シナリオ1-N-1	*踏切制御装置の故障により検知開始指示がでず、とりこ検知開始できない*	
シナリオ1-N-2	踏切制御装置保守のためとりこ検知機能無効状態のまま保守作業終了すると検知機能開始指示出ず、とりこ検知開始できない	①
UCA1-T(同上)	検知開始指示がToo Lateで検知開始が遅れ、特殊信号の発光が遅れるので検知できない時間がある 安全制約1-1違反	
シナリオ1-T-1	検知開始指示は踏切装置が遮断完了してから出すため、とりこ検知して特殊信号機発光しても列車停止が間に合わない可能性あり	②
シナリオ1-T-2	*踏切制御装置或いは伝送路の故障により検知開始指示が遅れとりこ検知が遅れ列車停止が間に合わない*	
UCA2-N(検知装置→特殊信号発光機)	とりこがあっても発光せず列車停止間に合わない安全制約1-1違反	
シナリオ2-N-1	*検知装置の故障でとりこ発生しても検知できないので、発光開始指示を出さない*	
シナリオ2-N-2	認識アルゴリズム不良でとりこ検知できず発光開始指示出さない	③
シナリオ2-N-3	外部環境不良のためとりこ検知できず発光開始指示出さない ・雪、雨、霧による　・丸い形状(タンクローリー)　・小さ過ぎる(子供、倒れた人、)　・反射光強すぎ ・夜(カメラの場合)　・カメラ自体に障害物による遮蔽	④
シナリオ2-N-4	カメラのレンズが汚れて検知できず	
UCA2-T(同上)	発光開始指示がToo lateで発光開始が遅れ、列車停止間に合わない　安全制約1-1違反	
シナリオ2-T-1	*機器の故障で発光指示が遅れる*	
シナリオ2-T-2	“とりこ”検発見から一定時間おいて(Delay)発光指示を出す場合の遅延時間が長すぎて(発光指示が遅れて)列車停止間に合わない	⑤

HCF一覧（2／3）

UCA/シナリオ		対策
UCA3-P(検知装置→特殊信号発光機)	とりこ中に特殊信号発光機消灯　安全制約1-1違反	
シナリオ3-P-1	検出アルゴリズムの誤りで途中から見失う	
シナリオ3-P-2	急な濃霧・豪雨の発生で途中から見失う	
UCA4-N(特殊信号発光機→運転士)	発光指示があっても発光せず列車停止間に合わない　安全制約1-1違反	
シナリオ4-N-1	*特殊信号機自身の故障で発光せず列車停止間に合わない*	
シナリオ4-N-2	発光器の発光部分に遮蔽物が巻き付いて光が出ず列車停止間に合わない	⑥
UCA4-T(同上)	発光開始が遅れ、列車が停止できない　安全制約1-1違反	
シナリオ4-T-1	*特殊信号機自身の故障で発光遅れ列車停止間に合わない*	
シナリオ4-T-2	発光器の発光部分に巻き付いた遮蔽物が外れて光が遅れて出たが列車停止間に合わない	⑦

HCF一覧（2／3）

UCA5-N(運転士→列車)	運転士が特殊信号の発光を認識できず列車を停止しない安全制約1-3違反	
シナリオ5-N-1	運転士が他に気を取られて認識するのが遅れ列車停止が間に合わない	⑧
シナリオ5-N-2	外部環境不良のため発光視認できず列車停止が間に合わない *・雪、雨、霧による視界不良　・逆光強すぎ　・カーブがきつくて見えない　・途中に遮蔽物(木など)で見えない* *・途中にトンネル*	⑨
シナリオ5-N-3	体調不良またはよそ見でブレーキ遅れる	
UCA6-P(踏切→検知装置)	列車が在線中に検知停止指示が出ると、とりこがあっても発光せず列車を停止させない安全制約1-2違反	
シナリオ6-P-1	*踏切制御装置故障で列車在線中にとりこ検知停止指示がでたあとにとりこ発生しても発光指示出ず発光しない*	
UCA6-T(同上)	列車が在線中に早く検知停止指示が出ると、とりこがあっても発光せず列車を停止させない安全制約1-2違反	
シナリオ6-T-1	*踏切制御装置故障で列車在線中(列車が踏切に到達する前)にとりこ検知停止指示がでたあとにとりこ発生しても発光指示出ず発光しない*	

対策(設計制約)の立案

1. アルゴリズム

a 制御機能に関するHCF

②検知開始指示は踏切装置が遮断完了してから出すと、とりこ検知して特殊信号機発光しても列車停止間に合わない

→ 遮断完了までにかかる時間をδ、更にとりこ確定待時間をα、列車検知センサから踏切までの距離をL、列車の最高許容速度をV_h、列車停止距離を∏(V)とすると、次の条件を満たさなければならない。

$$V_h \cdot (\delta + \alpha) + \Pi(V_h) < L$$

従って、踏切が遮断完了までにかかる時間、“とりこ”確定待ち時間、列車検知センサーから踏切までの距離、列車の最高許容速度の上限は上記制約式を満たすように決めなければならない。

b 認識機能に関するHCF

③認識アルゴリズム不良でとりこ検知できず発光開始指示出さない

→ 車を認識する場合、車の方向(前方/後方/斜め)、形状(乗用車、トラック、バス、コンテナ、自転車、バイク)、大きさを、車以外を認識する場合、種類(人、人以外の動物)、状態(起立、移動、転倒)、数などのバリエーションを考慮していなければならない。また、逆光、発光(とりこからの)など光に関する環境条件も考慮する必要がある。さらに、カメラの2台化(別角度からの像を合わせて検知)或いはカメラ以外の認識手段も考慮する必要がある。

c 検知機能に関するHCF

⑤とりこ状態確定判断するため一定時間待つ場合、発光開始指示が遅れ、列車停止間に合わない可能性あり

→ aに含まれる

＊機器・装置故障は除く

対策(設計制約)の立案(続き)

2. 性能に関わる対策

④外部環境不良のためとりこ検知できず発光開始指示出さない

・雪、雨、霧による　・反射光強すぎ　・夜(カメラの場合)

→ カメラを入力に使用する場合、入力光の量で制約がでるため感度、フィルタ、赤外線対応等も考慮する必要がある
評価用反射板を設置して環境不良をチェックすることも考慮する

⑥発光器の発光部分に遮蔽物が巻き付いて光が出ず列車停止間に合わない

→ 風で飛ばされてくる可能性のあるもの(凧、ビラ、旗など)とその材質(紙、ビニール、布など)が巻き付きにくいカメラの形状
巻き付いて視界が遮られたことを判別して通知する機能の付加も考慮する必要がある

3. 運用規約

①踏切制御装置保守のため検知機能無効状態のまま保守作業終了すると検知機能開始指示出ず、検知開始できない

→ 保守作業手順と規定、作業終了時点検方法の明確化
保守作業完了後の運用開始スウィッチを踏切制御装置と連動する形で検知装置に設けることも考慮する

4. その他

⑦発光器の発光部分に巻き付いた遮蔽物が外れて光が遅れて出たが列車停止間に合わない

→ 前記2. ⑥と合わせて検討する

⑧運転士の認知が遅れ列車停止が間に合わない

→ とりこに限らない

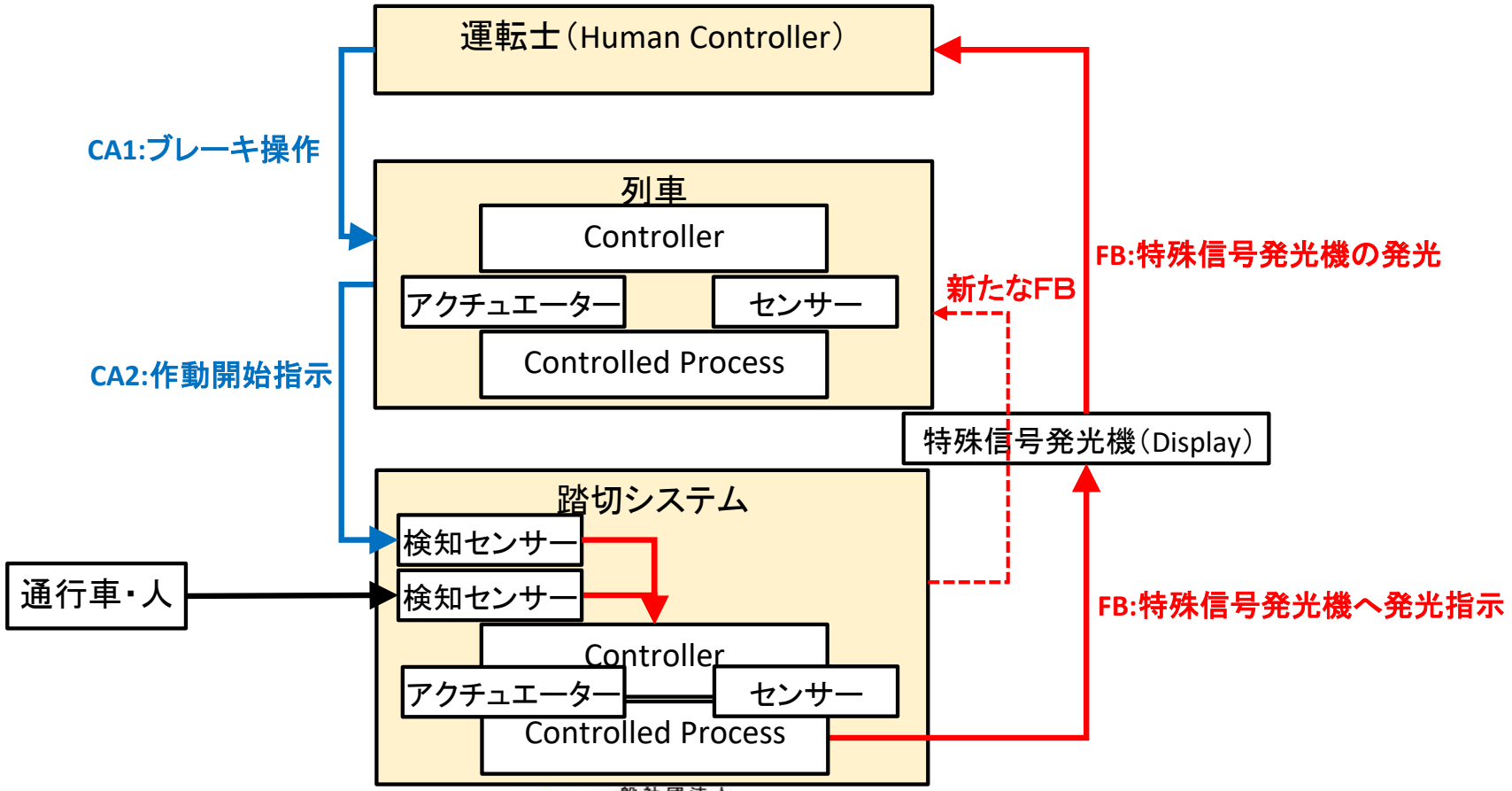
⑨外部環境不良のため発光視認できず列車停止が間に合わない

・雪、雨、霧による視界不良　・逆光強すぎ　・カーブがきつくて見えない　・途中に遮蔽物(木など)で見えない
・途中にトンネル

→ *対策1:*視界不良時のサービス中断、逆光を回避するためにサングラス、遮蔽物等に関しては定期的に保守(確認)が必要
それ以外は設置場所の選定と通常の点検に含める

対策(設計制約)の立案(続き)

対策2:運転士を中心にした3階層のコントロールストラクチャーから考えると、踏切からのフィードバックが列車を経由しないで運転士に直接入っている。踏切からのフィードバックを列車に入れるようにすることで自動的に列車を停止させることが可能になる。
ただし、具体的な実現手段に相当のコストが必要になることは考慮しなければならない(すでに一部区間では実装されている)。この対策は“とりこ検知”の流れに沿ったコントロールストラクチャーからは見つけるのが難しい。このことからモデルの抽象度によって考えられる対策の範囲に影響があることがわかる。



HCF特定に関わる考察

とりこ検知システムの検知/認知において、対象と特定されたHCFは、システムの如何に拘らず共通的と考えてもよいのではないだろうか。

機械による検知			
機能		HCFになりうる手段	
どうする	何を(目的)	HW	SW
モノの認識(識別)	モノの種別、位置	光、電波	アルゴリズム(形状、色、大きさ、環境)
内部状態検知	生死、圧力、温度、振動	計測器	アルゴリズム、対象モデル

人間による認知(監視)			
機能		HCFになりうる阻害要因	
どうする	何を(目的)	環境条件	人間(監視する)の状態
視認	光(信号)、モノの存在	障害物・(逆)光、気象	健康状態、生理現象
対象の状態認知	生死、正常・異常、運動	ｲﾝﾃﾞｨｹｰﾀ、事前状態	健康状態、生理現象

アルゴリズムに関するHCF候補例

機能		手段	HCF候補
どうする	何を(対象)		
(ものの)認識	種別(車、人、動物)、位置	カメラ(光)	形状、大きさ、環境(逆光、発光、夜間、雨、霧、雪)、動作、数
		カメラ(赤外線)	形状、大きさ、環境(逆光、発光、雨、霧、雪)、動作、数
		レーダー	形状(乱反射)、色(吸収)、電波吸収材、動作、数
計測	圧力	圧力センサー	ノイズ、バイアス、誤差
	水位	水位計	ノイズ、バイアス、誤差
	温度	温度計	ノイズ、バイアス、尺度(摂氏、華氏)、測定可能範囲、誤差
	流量	流量計	ノイズ、バイアス、振動
	速度	速度計	尺度(メートル、ヤード)、計測可能範囲、誤差
	距離		尺度(メートル、ヤード)、誤差
	重量	重量計	尺度(Kg,ポンド)、計測可能範囲(秤量)、誤差

とりこ検知事例のSTAMP・STPA分析のまとめ

- 従来の一方向の事故進展モデルに基づくハザード分析で難しい複雑システムのハザード分析が可能になる。特に、機械やコンピュータなどの技術要因に加えて、**人や組織などの非技術要因を含めた、包括的な事故防止アプローチ**を可能にする
- 安全制約と制御構造図により、**安全をどのような仕組み・体制で制御しようとしているかを可視化**できる。これにより、多様な視点からのレビューができる（次世代の安全制御のあり方など）