JR東日本におけるSTAMP活用の取り組み

IPA/SEC IoTシステム安全性向上技術WG委員／東日本旅客鉄道株式会社　北村 知

JR東日本では、信号保安システムのソフトウェア化が進み、従来の手法による安全性分析が難しくなっていることから、宇宙開発分野で実績のあるSTAMP活用の取り組みを始めている。
信号保安システムへのSTAMPの活用事例として、STAMP/STPAを用いたシステム設計段階での安全性分析と、STAMP/CASTを用いた過去の障害事例からの安全要求抽出に関する事例を紹介する。

1　信号保安システムの現状

鉄道では、連動装置※1や踏切保安装置※2といった各種信号保安システムにより安全が確保されている。これらの装置は、従来はリレーを用いたシーケンス回路の論理により安全性を確保してきたが、近年では情報通信技術の進展と共に、これらの装置についてもソフトウェアを用いた電子制御装置に置き換わっている。

このように、近年では信号保安システムにおけるソフトウェアの割合が拡大している。このため、システム設計段階での安全性分析として、これまでのFTAやFMEAといった手法の適用が難しくなっている。なぜなら、ソフトウェアはハードウェアのように故障するわけではなく、開発時の仕様や製作プロセスでの不備がシステム不具合につながるため、従来の安全性分析手法だけでは限界があるからである。

また、発生する不具合も、装置単体レベルでは説明ができないような複雑な事象が多くなっている。ソフトウェアで構成される装置特有の、新たな不具合の発生を考慮しなければならない。

この状況を踏まえ、JR東日本では、2013年度から、宇宙開発分野で先行実績のあるSTAMPの信号保安システムへの応用について検討を始めた。

2　信号保安システム開発とSTAMP/STPA

信号保安システムには、連動装置や踏切保安装置など様々な装置があるが、ここでは踏切保安装置を題材にして、STAMP/STPA手法の信号保安システムへの適用例について述べる。

2.1　踏切保安装置の構成

踏切保安装置は、現地の状況や導入する鉄道事業者によって異なるものの、当社においてはおおむね図2-1のような装置で構成されている。

踏切保安装置の動作ロジックは、おおむね次の通りである。

- 列車が「始動点制御子」と呼ばれるレールに設置したセンサに進入すると、踏切が列車の接近を検知する。
- 列車の接近を検知した踏切は、警報機を鳴らし、しゃ断機を閉める。
- 踏切を通過した列車が「終止点制御子」と呼ばれるセンサを通過し終わると、警報機が鳴動を停止し、しゃ断機を開放する。

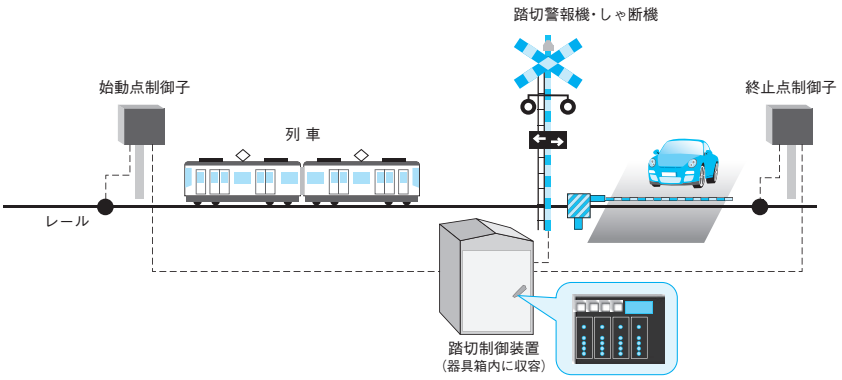

図2-1　踏切保安装置の概要

※1　駅構内の転てつ機などの設備と信号機を相互に関連付けて、列車運行の安全を担保する装置
※2　列車が踏切に接近したことを検知し、警報機やしゃ断機を作動させることで事故防止を図る装置

なお、駅構内※3の踏切の場合は、ポイントによる進路の分岐方向に応じて踏切制御の要否を識別しなければならないことから、「始動点制御子」ではなく、駅の一定区間ごとに設けた軌道回路※4と呼ばれるセンサと構成された進路の条件により、列車の接近を検知する場合が多い。

このように、駅間の踏切は比較的シンプルに構成されている一方で、駅構内の踏切については、走行する列車の進路が多岐にわたることから、その踏切内部の処理も複雑になる。

また、装置自体が故障した場合は、安全側すなわち踏切を警報するように動作しなければならない。万が一、列車が通過しても踏切が動作しない事象を「無しゃ断」と呼び、これは非常に危険な事象であるため発生させてはならない。

2.2 電子踏切保安装置の開発における STAMP/STPA分析の活用

踏切保安装置の電子化は1986年頃から行われているが、一部を除き、論理がシンプルな駅間の踏切に限られている。駅構内の条件を電子化した踏切（以下、構内電子踏切）は、多様な列車の動きに対応させるために制御論理が複雑となり、現状では本格的な導入には至っていない。

本節では、現在開発を進めている新たな構内電子踏切の制御機能にSTAMP/STPA手法を適用し、開発段階での制御論理における安全要件の抽出を行った事例を紹介する。

2.2.1 ハザード制御にかかわるControl Structureの作成（Step 0）

構内電子踏切へのSTAMP/STPA手法の適用にあたり、ハザードを以下の通りに定義した。

■安全上問題となるハザード

H1：列車が在線で踏切がしゃ断しない

H2：踏切がしゃ断後に列車が在線にもかかわらず開く

H3：警報時間の不足（法令への抵触）

■運用性の低下につながるハザード

H4：警報時間の過剰

H5：列車が非在線で踏切がしゃ断する

ただし、今回は「安全上問題となるハザード」を優先的に分析するために、ハザード定義を限定し、H1からH3のみを対象とすることとした

次に、検討中の仕様案に基づき、図2-2に示す構内踏切全体のControl Structure Diagramを作成した。

ここで、本分析の対象としている構内電子踏切は、踏切本体を制御する論理装置「構内LC」を中心に、列車位置を検知する軌道回路や、列車の進路を構成する信号機・転てつ機などの条件を入力していることに留意していただきたい。

図2-2のControl Structure上の、Control Actionの実行条件と実行内容の整理を行った。

構内LCから踏切本体への制御電文のうち、踏切警報開始／終止の命令を意味する「SR落下／扛上」※5を分析対象のControl Actionとして、次のStep 1の対象とすることとした。

2.2.2 非安全なControl Actionの識別による ハザードシナリオの分析（Step 1）

Control Actionごとに、4つのガイドワードを適用して、表2-1に示すようにハザードにつながる非安全なControl Actionを分析した。

非安全なControl Actionによるハザードシナリオを表2-2に示す通り整理した。H1からH3に関係するハザードシナリオに絞り込み、次のStep 2の対象とすることとした。

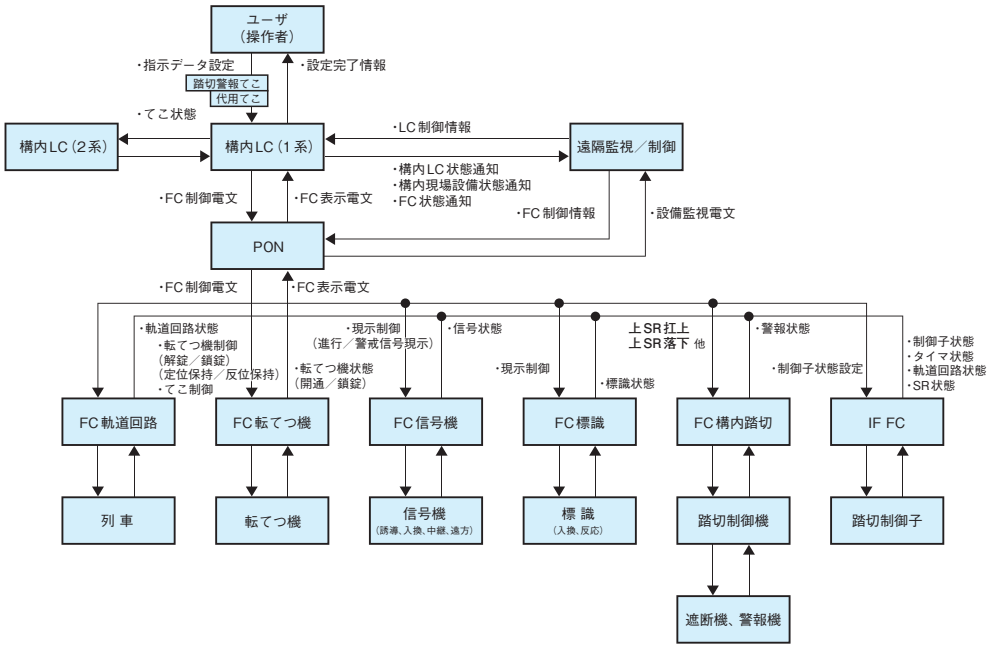

図2-2　構内踏切全体のControl Structure Diagram

※3　ここで言う「駅」とは、ポイント（分岐器）を持つ駅を指す。以下同様

※4　レールを介して電気回路を構成し、その電圧変化で列車の有無を検知する装置

※5　落下/扛上とは、従来から信号保安装置に用いられてきたリレーシーケンス回路において、リレーの電圧をしゃ断してOFF/電圧をかけてONにする制御ロジックに由来する。SRは当社内で一般的に踏切警報条件に用いるリレー名称であり、フェールセーフの観点から「SR落下」で踏切が鳴動するようになっている

表2-1　ハザードにつながる非安全なControl Action（抜粋）

制御アクション	内容	提供されない Not Providing	誤って提供される Providing causes hazard	早過ぎる／遅過ぎる／順序が違う Too early / Too late	途中で停止する／（過剰に長引く） Stop too soon / Applying too long
上SR落下	●警報区分進路の警報状態が「警報中」または「在線監視」のとき、SR落下。 (1)「警報中」となる条件（「警報準備」経由） (以下の条件のAND) ●「非警報（非在線）」→「警報準備」 〈詳細は省略〉 ●「警報準備」→「警報中」遷移 〈詳細は省略〉 (2)「警報中」となる条件（「非警報（在線）」経由） (以下の条件のAND) ●「非警報（非在線）」→「非警報（在線）」 〈詳細は省略〉 ●「非警報（在線）」→「警報中」 〈詳細は省略〉 (3)「在線監視」となる条件（以下の条件のOR） ●「警報準備」→「在線監視」 〈詳細は省略〉 ●「警報中」→「在線監視」 〈詳細は省略〉 ●「非警報（在線）」→「在線監視」 〈詳細は省略〉	列車が警報区分進路に実際に在線しており、左記条件（1）～（3）が合致する状況において、上SR落下が提供されないと、ハザードH1「列車が在線で踏切がしゃ断しない」に至る。【UCA 1-1-A】	列車が警報区分進路に実際に在線しておらず、左記条件（1）～（3）が合致しない状況において、上SR落下が提供されると、ハザードH5「列車が非在線で踏切がしゃ断する」に至る。【UCA 1-1-B】	列車が警報区分進路に実際に在線しているが、左記条件（1）～（3）が合致しない状況において、早まって上SR落下が提供されると、ハザードH4「警報時間の過剰」に至る。【UCA1-1-C】 列車が警報区分進路に実際に在線しており、左記条件（1）～（3）が合致する状況において、遅れて上SR落下が提供されると、ハザードH3「警報時間の不足（法令への抵触）」に至る。【UCA 1-1-D】	列車が警報区分進路に実際に在線しているときに、上SR落下の周期出力が途中で停止しても、直ちに上SR扛上にはならないので、ハザードH2「踏切がしゃ断後に列車が在線にもかかわらず開く」に至らない。 列車が警報区分進路に実際に在線しておらず、左記条件（1）～（3）が合致しない状況において、上SR落下が過剰に長引くと、ハザードH4「警報時間の過剰」に至る。【UCA 1-1-E】

表2-2　絞り込んだハザードシナリオ

No.	ハザードシナリオ
1	列車が警報区分進路に実際に在線しており、上SR落下が合致する状況において、上SR落下が提供されないと、ハザードH1「列車が在線で踏切がしゃ断しない」に至る。
2	列車が警報区分進路に実際に在線しており、上SR落下が合致する状況において、遅れて上SR落下が提供されると、ハザードH3「警報時間の不足（法令への抵触）」に至る。
3	列車が警報区分進路に実際に在線しており、上SR扛上のいずれも合致しない状況において、上SR扛上が提供されると、ハザードH2「踏切がしゃ断後に列車が在線にもかかわらず開く」に至る。
4	列車が警報区分進路に実際に在線しておらず、上SR扛上のいずれも合致しない状況において、早まって上SR扛上が提供されると、ハザードH3「警報時間の不足（法令への抵触）」に至る。

2.2.3　Control Loopの作成によるハザード要因の分析（Step 2）

Step 1で識別したハザードシナリオごとに、関係するControllerとControlled Processを識別してControl Loop Diagramを作成し、ガイドワードを適用して詳細なハザード要因を分析した。ハザードシナリオNo.1：(UCA1-1-A) のControl Loop Diagramを図2-3に示す。

図2-3中の外部状況の認識誤り要因の抜粋を以下に示す。

(a) 列車の在線状況を正しく判断しない

(b) 信号機（進路）の設定状態を正しく判断しない

(c) 転てつ機の開通方向を、正しく判断しない

ハザードシナリオNo.1：(UCA1-1-A) について、ハザード要因を整理したものを表2-3に示す。

なお、これまでのStepを通じて、検討中の仕様案にて定義されていた警報状態の遷移条件の抜け・誤りを5件識別した。そのうち2件は、H1のハザードに至る条件であった。

これらは安全上問題となるため、状態遷移図を再定義して、Step 0～2までを再度分析した。

図2-4に仕様案における変更前及び変更後の状態遷移図を示す。

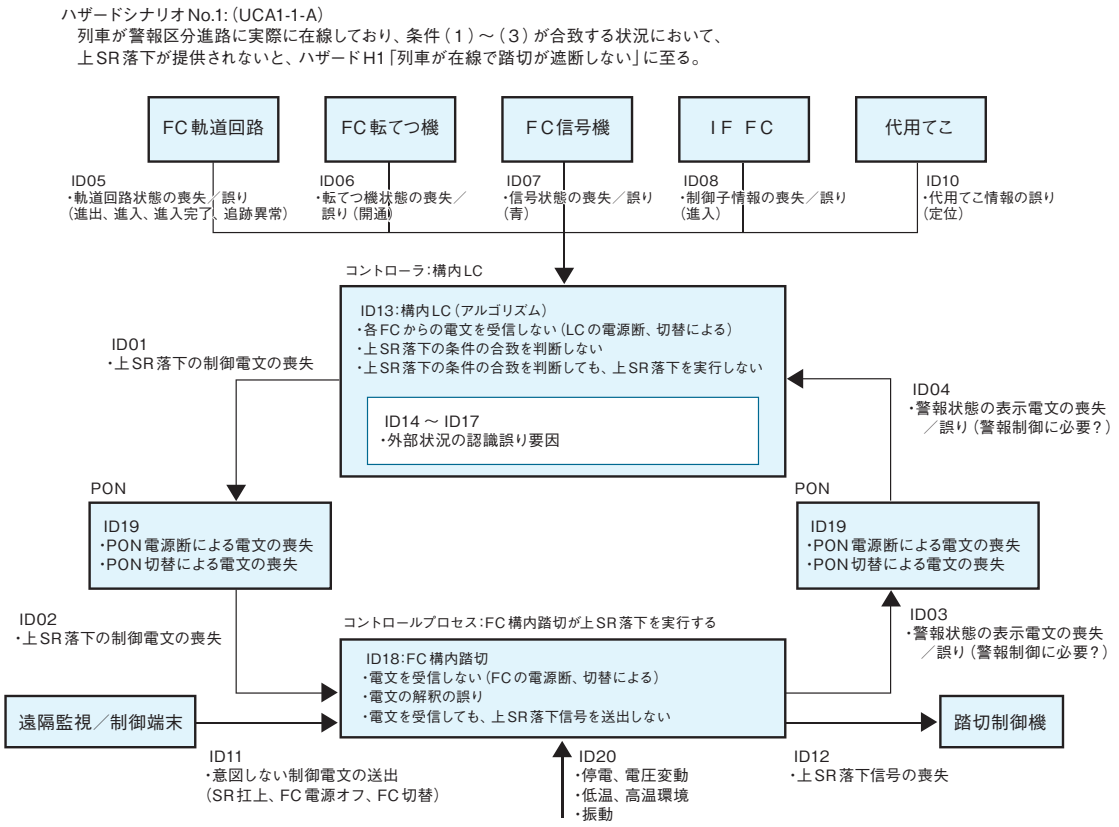

図2-3　Control Loop Diagram

表2-3　ハザード要因（抜粋）

分析対象			要因のカテゴリ				
カテゴリ	ID	対象	喪失、不実行	誤り、保持	遅延／早出	停止／継続	ハザード要因
データ伝送	ID01	構内LC → PON	×	−	−	−	・上SR落下の制御電文の喪失
	ID02	PON → FC構内論切	×	−	−	−	同上
	ID03	FC構内論切 → PON	−	−	−	−	・警報状態の表示電文の喪失／誤り（警報制御に必要？）
	ID04	PON → 構内LC	−	−	−	−	同上
	ID05～ID10	その他FC → 構内LC	×	×	−	−	・ID05:軌道回路状態の喪失／誤り ・ID06:転轍機状態の喪失／誤り ・ID07:信号状態の喪失／誤り ・ID08:制御子情報の喪失／誤り ・ID10:代用てこ情報の誤り
		遠隔監視／制御端末 → FC構内論切	−	×	−	−	・意図しない制御電文の送出（SR扛上、FC電源オフ、FC切替）
		FC構内論切 → 論切制御機	×	−	−	−	・上SR落下信号の喪失
内部（機器、人）	ID13	構内LC（アルゴリズム）	×	−	−	−	・各FCからの電文を受信しない（LCの電源断、切替による） ・上SR落下の条件の合致を判断しない ・上SR落下の条件の合致を判断しても、上SR落下を実行しない
	ID14	構内LC（外部状況「軌道回路状態」の認識）	×	−	−	−	(a) 軌道回路状態（警報区分進路）を、「進出」と判断しない ・「非警報（非在線）」に遷移する前（「在線監視」、「非警報（在線）」）に、既に「進出」と判断されていたので、あらためて判断しない ・FC軌道回路の出力が異常であると判断しているため (d) 軌道回路状態（警報区分進路）を、「進入」or「進入完了」と判断しない ・軌道回路状態と制御子情報が整合していないため（制御子がある軌道の場合） (i) 非在線中において、軌道回路状態（警報区分進路）が、「追跡異常」と判断しない ・「警報準備」に遷移する前（「非警報（非在線）」）に、既に異常と判断されていたので、あらためて判断しない (k) 在線中において、軌道回路状態（警報区分進路）が、「追跡異常」、かつ、進路予約状態が、「なし」と判断しない ・「非警報（在線）」に遷移する前（「非警報（非在線）」）に、既に異常と判断されていたので、あらためて判断しない

FTAで分析が可能

STAMP/STPAが得意とするカテゴリ

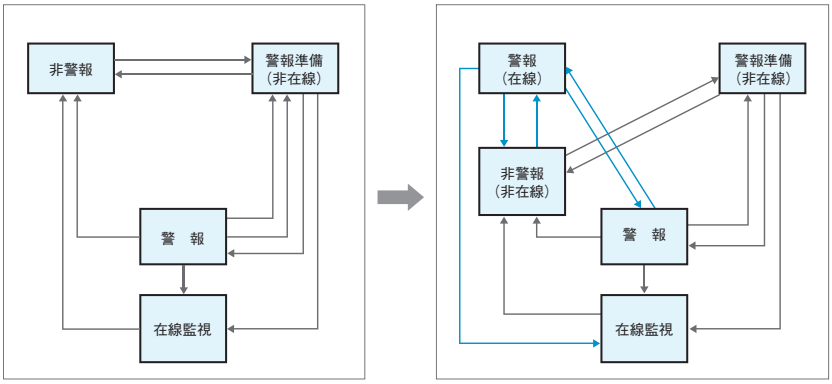

図2-4　警報状態遷移図（変更前及び変更後）※遷移条件の記載は省略

2.2.4　安全制約の識別（Step 3）

Step 2で識別したハザード要因ごとに、ハザード要因を制御／除去するための安全制約を識別した。ハザードシナリオ1～4の合計で、111件の安全制約（安全要求）を識別できた。ハザードシナリオ1におけるハザード要因／安全制約（安全要求）の抜粋を表2-4に示す。

2.2.5　設計時の安全性検証におけるSTAMP/STPAの位置付け

これまでのStepにて、STAMP/STPA分析で安全要件を抽出したが、安全性分析はここで終わるわけではない。実際には、その結果により絞られた検査対象に対し、モデル検査などのツールを用いた安全性の検証が必要となる。逆に、検査対象を絞り込

表2-4　ハザードシナリオ1のハザード要因／安全制約（安全要求）抜粋

ID	ハザード要因	安全制約（要求）
ID01	●上SR落下の制御電文の喪失	●制御電文を喪失しない。あるいは、喪失を検知する。
ID02	同上	同上
ID03	●警報状態の表示電文の喪失／誤り	同上
ID04	同上	同上
ID05～ID10	●ID05：軌道回路状態の喪失／誤り ●ID06：転てつ機状態の喪失／誤り ●ID07：信号状態の喪失／誤り ●ID08：制御子情報の喪失／誤り ●ID09：ユーザ（操作者）の誤り ●ID10：代用てこ情報の誤り	●各FCからの電文を喪失しない。あるいは喪失を検知する。 ●各FCからの電文を誤らない。あるいは誤りを訂正する。
ID11	●意図しない制御電文の送出（SR扛上、FC電源オフ、FC切替）	●構内LC運用中において、遠隔監視／制御端末の利用制限を設ける。

まずにモデル検査を行おうとすると、容易に状態爆発を引き起こしてしまい、実用的な時間内での検査は不可能となる。

すなわち、STAMP/STPA手法は、設計時の安全性検証における「検査対象を安全上重要な個所に絞り込む」役割を担っていると言える。

また、今回紹介した分析事例から、とくに、イベントの前後関係が動作上クリティカルになることの多い信号保安システムにおいては、状態遷移図の抜け・漏れの分析としてSTAMP/STPA手法の適用が有効であることも分かった。

3 STAMP/CASTと用いた事故事例の分析と安全要件の抽出

前節では、STAMP/STPA手法を用いた信号保安システムの設計段階での安全要件抽出の事例を示した。一方、STAMP/CAST（Causal Analysis using System Theory）手法は、過去に発生した障害事例から安全要求を抽出するのに有効な手法である。

本手法においても、コントロールループを用いて、安全制約を実現する制御機能のコントロールストラクチャ（Safety Control Structure）を作成する。しかし、解析事象の網羅性を重視するSTAMP/STPAとは異なり、実際のシナリオと各機能の流れを一覧表にて整理することで、関連した要因を結び付けながら背後にある要因の分析を容易にする点が特徴である。

3.1 分析対象

分析対象として、踏切制御における過去の不具合事例をもとに、12件のケースを想定した。想定にあたっては、STAMPモデルの特性から、以下の2点を満たすものとした。

①2つ以上のコンポーネントが関係する不具合事象であること

②事象によって引き起こされたハザードが万遍なく（2-2-1節のH1～H5）選択されること

ここではその一つの例として以下の題材を取り上げる。

「▲▲本線○○駅の■■踏切にてしゃ断不良※6が発生した」というケースを考える。図3-1に示すように、下り列車1レによって警報開始した踏切制御に対し、同じ構内にて上り方向〈3LT〉へ出発する列車2レによって誤って終止条件が成立した事象を想定する。

3.2 STAMP/CAST分析

3.2.1 Step 1：不具合シナリオの分析

このStepでは、不具合に至るシナリオを時系列（event chain）で分析する（表3-1）。すなわち、本事象にて登場する列車や制御機能と発生した事象を列挙する。

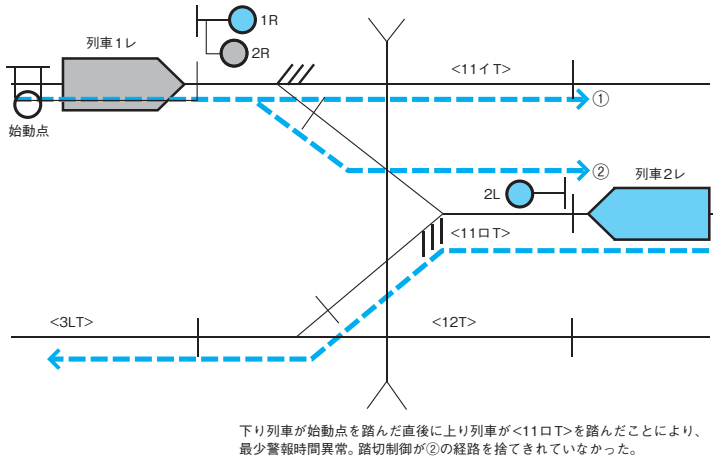

図3-1　想定事象のイメージ

表3-1　本事象のevent chain
Step.1 不具合シナリオの分析

ID	列車1レ	列車2レ	連動制御	踏切制御
①-1			転てつ機11イ定位（信号機1Rが青、信号機2Rが赤）てつ器11ロ定位（信号機2Lが青）	
①-2	下り始動点に進入			
①-3				踏切鳴動開始し、警報時間の計測開始
②-1		11ロTに進入		
②-2				列車1レが11ロTへ進入したと誤判断し、警報時間の計測開始から15秒以内であったため、最少警報時間異常を検知し、警報持続

※6　ここでは、警報中の踏切が、不正なタイミングで警報を停止し、しゃ断機を上げてしまう事象

3.2.2 Step 2：不具合事象と安全要求の定義

このStepでは、不具合事象とその発生を防ぐための安全要求を定義する。本Stepにおける安全要求は、不具合事象の裏返しである抽象度の低い安全要求と、ハザードの裏返しである抽象度の高い安全要求とのバランスを考慮して識別する。その理由は以下の通りである。

- 抽象度が低い安全要求は、具体的なシステムの用語を用いて定義されるので、不具合に気づきやすい。
- 抽象度が高い安全要求は、ほかの類似した不具合事例の分析時に、再利用しやすい。

本事象において識別した安全要求を表3-2に示す。なお、本事象においては、これは不具合事象の裏返しと同等であった。

3.2.3 Step 3：Safety Control Structure作成

安全要求の実行にかかわるSafety Control Structureを作成する（図3-2）。

Safety Control Structureは、安全要求に関係するコントロールアクションとフィードバックデータの流れとして作成する。各コンポーネントの安全要求を満たす役割として、安全制約を定義し、各コンポーネントの内部に記載する。

3.2.4 Step 4：Physical system levelの要因分析

ガイドワードを使用して、末端の制御対象である物理的要素（＝Physical system level）で不具合要因を分析する（表3-3）。ここでガイドワードとは、図3-3を基本として定めた、不具合の発生要因を導き出すための考え方である。

なお、本事象では関係する装置がすべて正しく動作しているので、物理的要素の不具合はない。

3.2.5 Step 5：Controller levelの要因分析

ガイドワードを使用して、制御を実行するController levelで不具合要因を分析する（表3-4）。すなわち、制御論理要素の不具合を列挙する。この中で、「踏切制御」のControllerが果たす安全制約を実行するための役割の一つである「警報の開始／停止指示を行う」点において不具合が発生している。

3.2.6 安全要求の導出

以上のようなSTAMP/CAST分析を、12件のケースすべてで実施した。その結果を整理し、踏切制御機能における一般的なSafety Control Structure及びその安全要求を作成した。

本研究で作成したSafety Control Structureを図3-4に、踏切制御機能に関する安全要求を表3-5に示す。

表3-2　抽象度を考慮した安全要求の識別

不具合事象の裏返し（抽象度：低）	識別した安全要求	ハザードの裏返し（抽象度：高）
連動制御による進路の独占権を踏切制御に反映し、警報開始させた列車が警報終止条件を成立できるようにする。	連動制御による進路の独占権を踏切制御に反映し、警報開始させた列車が警報終止条件を成立できるようにする。	警報時間を過剰に取らない。

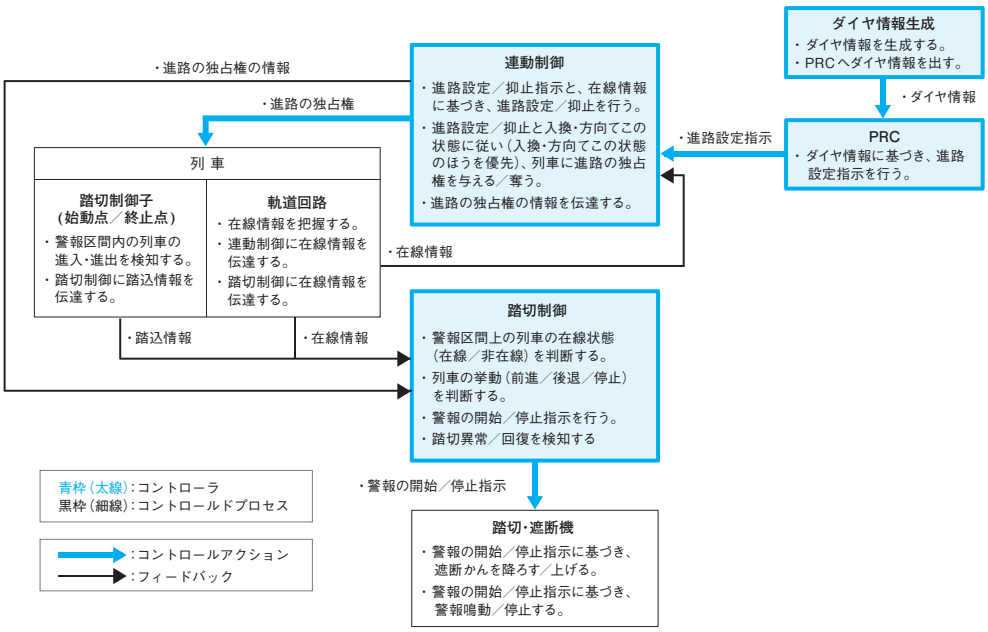

図3-2　本事象のSafety Control Structure

表3-3　Physical system levelの要因分析

No.	Physical system	(a) Safety Responsibilities アクターが果たす安全制約を実行するための役割／責任	(b) Safety Equipment (controls) 安全制約の実行に係るアクター内の機器とその動作	(c) Failures and Inadequate Control Actions (a) (b) を果たせない機器の故障、及び、不適切なコントロールアクション	(d) Physical Contextual Factors (c) のアクションがなぜ起こったか
1	軌道回路	在線情報を把握する	レールと車輪で電気回路を形成する	正しく動作したためN/A	正しく動作したためN/A
2		連動制御に在線情報を伝達する	通信手段を用いて在線情報を伝達する	正しく動作したためN/A	正しく動作したためN/A
3		踏切制御に在線情報を伝達する	通信手段を用いて在線情報を伝達する	正しく動作したためN/A	正しく動作したためN/A
4	踏切制御子 (始動点／終止点)	警報区間内の列車の進入・進出を検知する	始動点／終止点において、レールと車輪により電気回路を形成し、踏込を検出する	正しく動作したためN/A	正しく動作したためN/A
5		踏切制御に踏込情報を伝達する	通信手段を用いて踏込情報を伝達する	正しく動作したためN/A	正しく動作したためN/A
6	踏切・しゃ断機	警報の開始／停止指示に基づき、しゃ断かんを降ろす／上げる	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A
7		警報の開始／停止指示に基づき、警報鳴動／停止する	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A

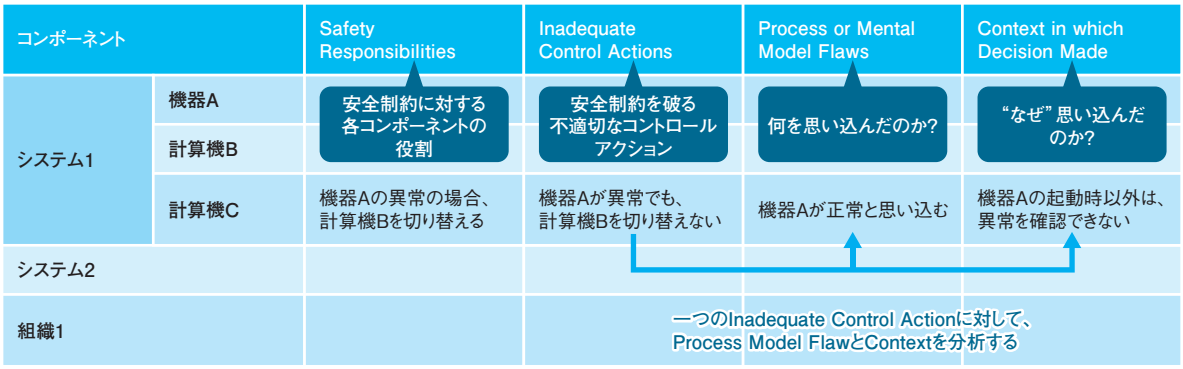

図3-3　Step 4,5で行う要因分析（ガイドワード）

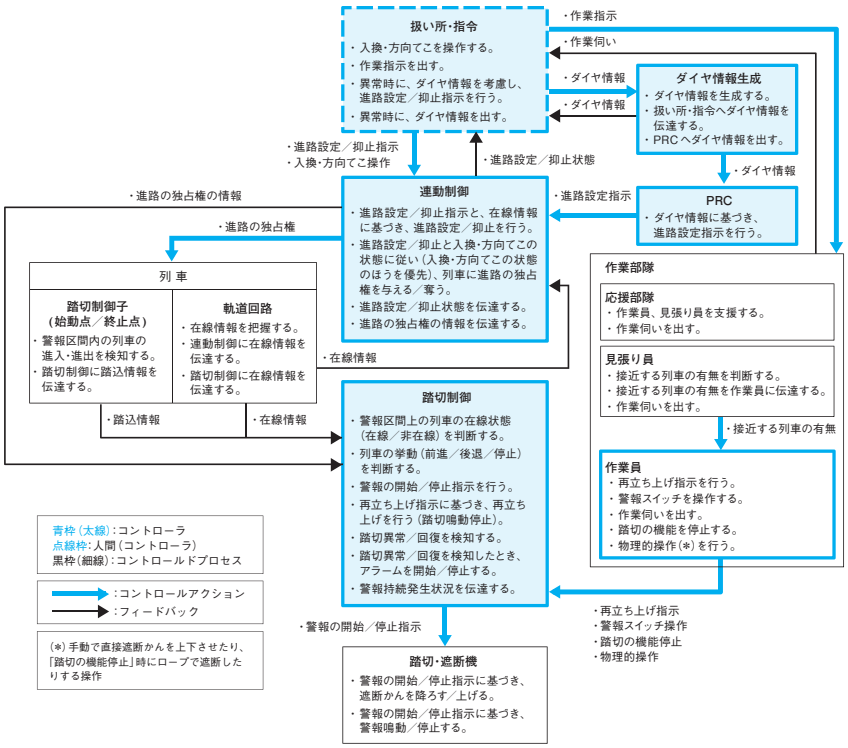

図3-4　今回のSTAMP/CAST分析において作成された踏切制御に関するSafety Control Structure

表3-4　Controller levelの要因分析

No.	Controller	(a) Safety Responsibilities アクターが果たす安全制約を実行するための役割／責任	(b) Inadequate Control Actions (a) を果たせない不適切なコントロールアクション	(c) Process or Mental Model Flaws (b) の振る舞いとなる動作条件について、アクターが信じている事実	(d) Context in which Decision Made (c) の動作条件や思い込みがなぜ生じたのか
6	踏切制御	警報区間上の列車の在線状態（在線／非在線）を判断する	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A
7		列車の挙動（前進／後退／停止）を判断する	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A
8		警報の開始／停止指示を行う	【要因】 ● 警報始動条件を成立させた列車（進路の独占権を持つ列車）以外の列車により、警報終止条件が成立してしまい、異常検知してしまった。その結果、非在線となっても踏切鳴動が継続してしまった	【要因】 ● 連動制御が独占権を与えていない進路（警報経路②）も警報経路としてしまった	【要因】 ● 独占権を与えている進路の情報（進路設定）を連動制御からもらっていなかった ● 警報進路を推定して作っていた 【提言】 ● 独占権を与えている進路の情報（進路設定）を連動制御からもらうようにする
9		踏切異常／回復を検知する	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A	【要因】 正しく動作したためN/A

表3-5　踏切制御機能に関する安全要求

Control Action	踏切制御に関する安全要求
警報開始	以下の①～④のORで警報を開始する。 ① 少なくとも1つの、独占権が確保され挙動が前進である列車の進路に警報区間が含まれるとき ② 先行列車の通過後、進出確定までの設定時素以内に、続行列車が警報区間に進入したとき ③ 警報スイッチが落下状態のとき ④ 踏切異常状態のとき
警報停止	以下の⑤～⑧のANDで警報を停止する。 ⑤ すべての、独占権が確保され挙動が前進である列車の進路に警報区間が含まれていないとき ⑥ 先行列車と続行列車の間隔が、進出確定までの設定時素より大きいとき ⑦ 警報スイッチが扛上状態のとき ⑧ 踏切正常状態のとき
進路設定／抑止指示 入換・方向てこ操作 作業指示 （扱い所・指令）	常に、踏切異常／回復を誤検知しない。 常に、踏切異常／回復を検知したとき、アラームを開始／停止する。 常に、警報持続発生状況を伝達する。

4　信号保安システムの開発プロセスとSTAMPの役割

これまで述べてきたように、STAMP/STPA手法は信号保安システムの開発段階における安全性分析への活用が期待できる。また、STAMP/CAST手法により従来システムの不具合の分析から抽出された安全要求は、システムの更新・展開及び新たな信号保安システム（例えば、次世代の踏切システム）の開発において活用できる。

これを一般的な信号保安システムの開発プロセス（Vモデル）に表すと図4-1の通りとなる。

当社においては、STAMPの導入はまだ試行段階であるが、今後は更に導入実績を積み、手順のブラッシュアップを図ることで、信号保安システムのソフトウェア開発プロセスの一部としてSTAMPの活用を図っていきたい。

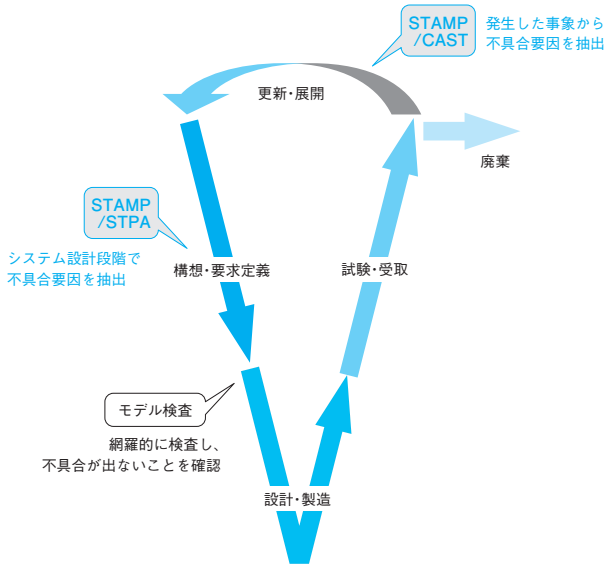

図4-1　信号保安システムの開発プロセス

【参照文献】
[1] Nancy G. Leveson, Engineering a Safer World -Systems Thinking Applied to Safety, MIT Press, 2011
[2] エリック・ホルナゲル著 小松原明哲監訳, 社会技術システムの安全分析～FRAMガイドブック～, 海文堂出版, 2013
[3] 重田ほか, 駅構内論理装置の開発, JR EAST Technical Review No.36, pp.19-26, 2011
[4] 信号システムの進歩と発展 ＝近年20年の展開と将来展望＝, 日本鉄道電気技術協会, 2009
[5] はじめてのSTAMP/STPA～システム思考に基づく新しい安全性解析手法～, 情報処理推進機構, 2016