STAMP解析での定量的評価と STAMP解析の開発プロセスにおける適用段階

株式会社京三製作所　開発センター
高田哲也（Tetsuya TAKATA）

目次

製品サービス群

鉄道信号システム　適用分野

これら適用分野における列車を制御する装置を提供

新幹線

都市鉄道

LRT

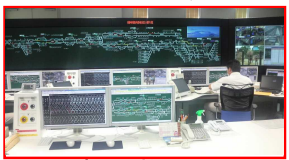
モノレール

リニアモーターカー

APM

鉄道信号システム　その2　製品群

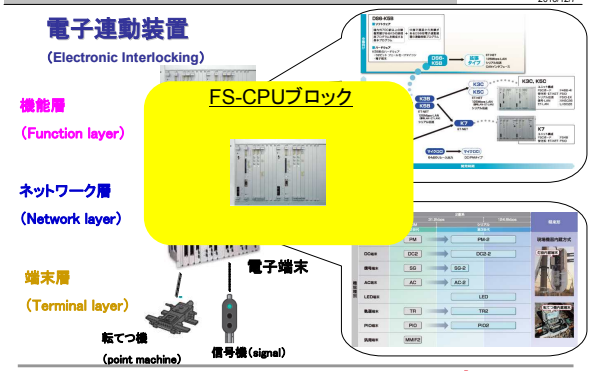
列車運行管理装置

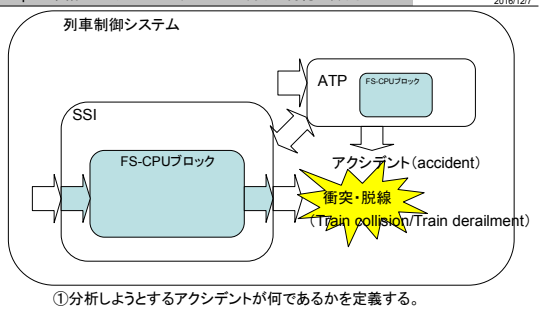


可動ホーム柵

踏切しゃ断機

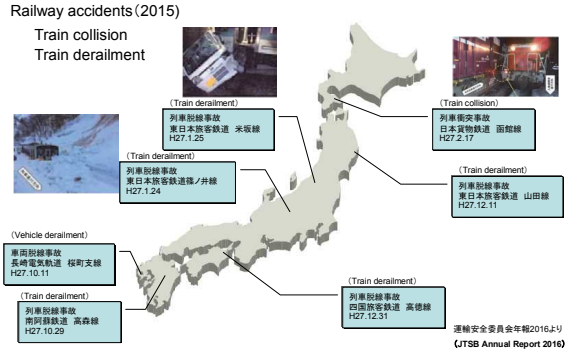
転てつ機





①分析しようとするアクシデントが何であるかを定義する。
②アクシデントとなりうるハザードには何があるかを考える。
③ハザードの裏返しとなる安全制約を導き出す。

Railway accidents(2015)
Train collision
Train derailment



運輸安全委員会年報2016より
(JTSB Annual Report 2016)

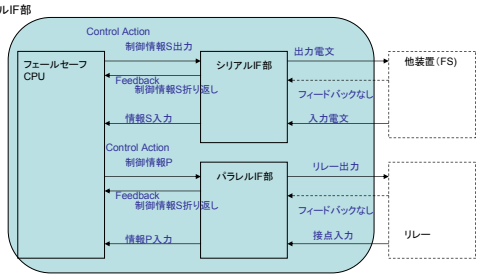
表1. Step0 アクシデント、ハザード、安全制約の識別

アクシデント(Loss)	ハザード(Hazard)	安全制約(Safety Constraints)
(A1)危険側事象 列車衝突など	(H1)出力0時に制御リレーが扛上する。	(SC1)各部の診断機能と、誤り検出時の安全側制御機構を備える。
(A1)危険側事象 列車衝突など	(H2)意図しないデータが伝わり不正な制御される。	(SC1)各部の診断機能と、誤り検出時の安全側制御機構を備える。

2-2. Step0　準備2　コントロールストラクチャーの構築

登場人物（Controller、Controlled Process）の整理

・フェールセーフCPU部
・シリアルIF部
・パラレルIF部



2-3. Step1　UCA（Unsafe Control Action）の抽出

STPA Step1：安全でないコントロールアクション（Unsafe control action）の識別

UCAの識別は、ハザードにつながる恐れのあるコントロールアクションの不具合を明確にすることを目的としており、大きく分けて以下に分類される。

1.Not Provided：安全のためのコントロールアクションが設置されていない。
2.Incorrectly Provided：
ハザードにつながるおそれのある、安全ではないコントロールアクションが設置されている。
3. Provided Too Early, Too Late, or Out of Sequence：
コントロールアクションのタイミングが遅すぎる、早すぎる、または定められた順序に設置さていない。
4.Stopped Too Soon：コントロールアクションがすぐに止まる、もしくは適用が長すぎる。

⇩

ハザードにつながる恐れのあるコントロールアクションの分類

以前のSTPA 解説書に記載されていた「Incorrectly Provided」は、「誤った制御情報が提供される」ではなく、「誤った条件で正しい制御情報が提供される」の意味なので、今は「Providing causes hazard」と記載するように改善されている。

2-4. Step2　HCF（Hazard Causal Factor）の特定

STPA Step2：**Causal factor**（誘発要因）の特定
STPAの最後の段階として、STPA Step 1で識別したUCAの原因となる**Causal factor** と、予想される事故シナリオの特定を行う。（要求されたコントロールアクションが設置されているが、それに従っていない）

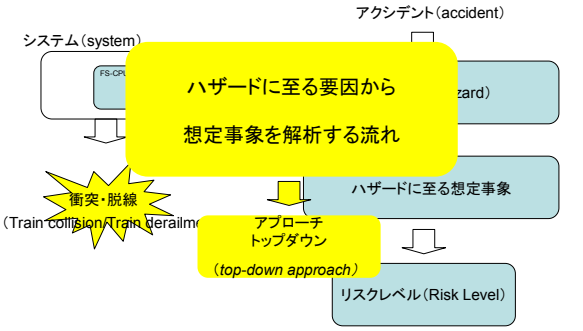
(1) コントロール入力や外部情報の誤りや喪失
(2) 不適切なコントロールアルゴリズム（作成時の欠陥、プロセスの変更、誤った修正や適用）
(3) 不整合、不完全、または不正確なプロセスモデル。不適切な操作。
(4) コンポーネントの不具合。経年による変化。
(5) 不適切なフィードバック、あるいはフィードバックの喪失。フィードバックの遅れ。
(6) 不正確な情報の供給、または情報の欠如。測定の不正確性。フィードバックの遅れ。
(7) 操作の遅れ
(8) 不適切または無効なコントロールアクション、コントロールアクションの喪失。
(9) コントロールアクションの衝突。プロセス入力の喪失または誤り。
(10) 未確認、または範囲外の障害
(11) システムにハザードを引き起こすプロセス出力

⇩

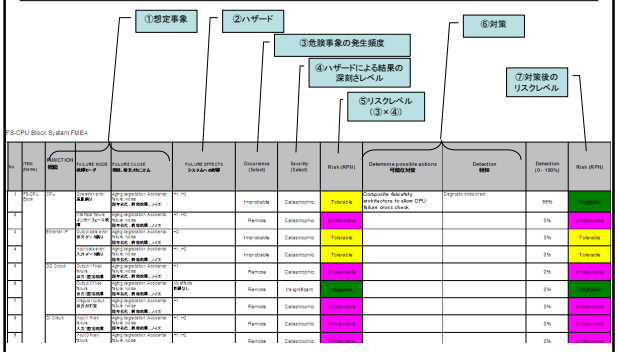
コントロールループの流れにおいて予想される不備を示したもの

※「STAMP手法に関する調査報告書」 IPA 2015年8月

2-5. STAMPの解析

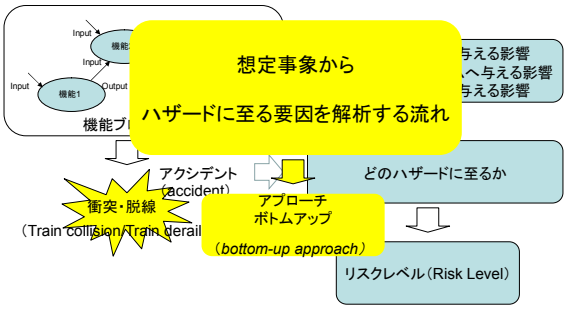


3. 既存のPHAの事例



3. 既存のPHAの事例

システム



4. STAMPでの定量的評価について

これまでの信号システム

「フェールセーフ技術」を その安全性の基本

システムの一部に故障が生じたときには必ず赤信号となって、列車を停止するようにシステムが動作

安全性だけでなく信頼性、稼動性、保全性をバランスよく考えてシステムを構築

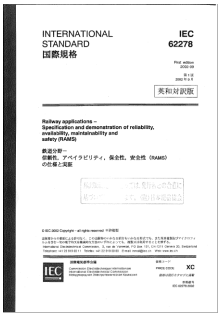
保守の介在による危険、故障時の危険、使用停止時の危険を考え、正常時、故障に至った瞬間だけの安全性では不十分

＋ できるだけ定量的に評価

RAMSの考え方

4. STAMPでの定量的評価について

IEC62278(EN50126) RAMS規格



Railway applications-

Specification and demonstration of reliability,availability,maintainability and safety(RAMS)

鉄道分野-

信頼性,アベイラビリティ,保全性,安全性(RAMS)の使用と実証

4. STAMPでの定量的評価について

IEC62278(EN50126) RAMS規格

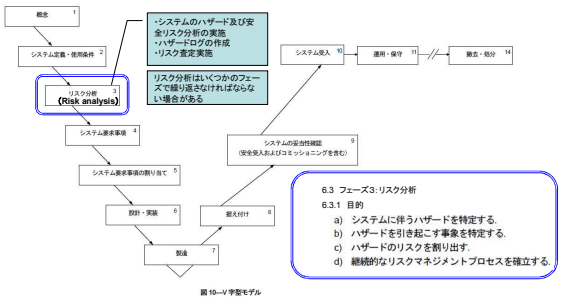


図 10—V 字型モデル

4. STAMPでの定量的評価について

第3段階

②ハザード ハザードを特定

Step0 準備1 アクシデント、ハザード、安全制約の識別 にて抽出

④ハザードによる結果の深刻さレベル

IEC62278 RAMS規格

4.6.2.3 表3

などにより設定

表3—ハザードによる結果の深刻さレベル

結果の深刻さレベル	人間あるいは環境に対する結果	サービスに対する結果
Catastrophic (破滅的)	死亡者複数、および/あるいは重傷者多数、および/あるいは環境への損害続めて大	
Critical (危機的状況)	死亡者1名、および/あるいは重傷者1名、および/あるいは環境への損害大	主要システムの損失
Marginal (わずかな影響)	負傷者発生、および/あるいは環境に対する危険性あり	重大なシステム損害
Insignificant (問題なし)	負傷者発生の可能性あり	軽度のシステム損害

①想定事象 ハザードを引き起こす事象を特定

Step1 にて UCA

(Unsafe Control Action)の抽出

③危険事象の発生頻度

IEC62278 RAMS規格

4.6.2.2 表2

などにより設定

表2—危険事象の発生頻度

カテゴリー	内容
Frequent (頻繁に発生)	頻繁に発生し得る、おそらく、常にハザードが存在することになる
Probable (十分起こり得る)	おそらく何回か発生する、ハザードがたびたび発生すると予測される
Occasional (時々発生)	何回か発生し得る、ハザードが何回か発生すると予測される
Remote (まれに発生)	システムライフサイクルのどこかで発生し得る、ハザードが妥当な程度で発生すると予測される
Improbable (極めて少ない)	発生し得ないが、可能性はある、ハザードが例外的に発生し得ると想定される
Incredible (起こり得ない)	発生の可能性は極めて低い、ハザードが発生し得ないと想定される

⑤リスクレベル　リスクを割り出す
IEC62278 RAMS規格
4.6.2.4 表6
などにより設定

想定シナリオ
Step2　にてHCF
第4段階　（Hazard Causal Factor）の特定

⑥要求仕様
第6段階　想定シナリオに至らないための制約事項を設定

⑦設計
制約事項をもとに対策の検討

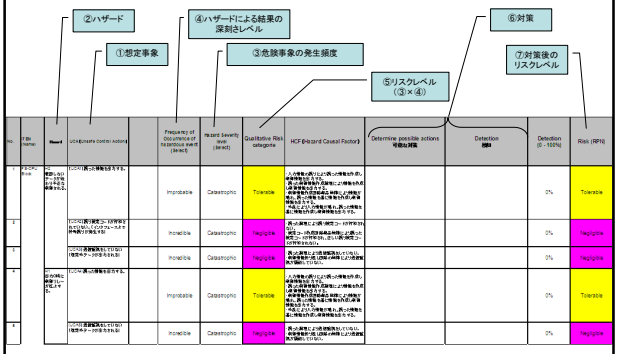
⑧FMEA等で結果を解析
対策の効果を確認（設計の妥当性確認⇒部品レベルでのFMEA

表6―リスク評価およびリスク受入の代表例

危険事象の発生頻度	リスクレベル			
Frequent（頻繁に発生）	望ましくない	受入不可	受入不可	受入不可
Probable（十分起こり得る）	許容可	望ましくない	受入不可	受入不可
Occasional（時々発生）	許容可	望ましくない	望ましくない	受入不可
Remote（まれに発生）	無視できる	許容可	望ましくない	望ましくない
Improbable（極めて少ない）	無視できる	無視できる	許容可	許容可
Incredible（起こり得ない）	無視できる	無視できる	無視できる	無視できる
	問題なし	わずかな影響	危険的状況	壊滅的
	ハザードがもたらす結果の深刻さ			

*危険事象の発生頻度の基準は、鉄道対象の用途によって異なる（4.6.2.2）

リスク評価	リスク軽減／コントロール
Unacceptable（受入不可）	排除すること
Undesirable（望ましくない）	リスク軽減が実行不可能であり、かつ最適事業者の合意を得られた場合のみ受入可能
Tolerable（許容可）	適切にコントロールでき、また最適事業者の合意が得られた場合に受入可能
Negligible（無視できる）	いかなる合意がなくとも受入可能



STAMP解析

開発初期段階（**Preliminary design phase**）に行い、
安全が確保できることを確認し、
その後、設計を進める中で、STAMPを遵守しているか、逸脱する場合は、どのように修正するかを考え、トップダウン（top-down）で進めていく。

連携

FMEA解析

設計完了段階（**Final design phase**）に、
部品（ハードウェア）、モジュール（ソフトウェア）レベルに基づく詳細のFMEAを実施し、ボトムアップ（bottom-up）で対策の妥当性確認する。

これからの信号システムの目指す安全

列車制御システム（Train Control system）

機能安全（functional safety）　→　**本質安全**（intrinsic safety）

ご清聴ありがとうございました

Thank you for your attention.