

1st STAMP Workshop in Japan
2016/12/7

Control, Computer, Communication

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)

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

1

1st STAMP Workshop in Japan
2016/12/7

目次

- はじめに
- STAMP解析 (FS-CPUブロックの事例)
 - Step0 準備1 アクシデント、ハザード、安全制約の識別
 - Step0 準備2 コントロールストラクチャーの構築
 - Step1 UCA (Unsafe Control Action) の抽出
 - Step2 HCF (Hazard Causal Factor) の特定
- 既存のPHAの事例 (FS-CPUブロックの事例)
- STAMPでの定量的評価 (Quantitative analysis) について
- おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

2

1st STAMP Workshop in Japan
2016/12/7

- はじめに
- STAMP解析 (FS-CPUブロックの事例)
 - Step0 準備1 アクシデント、ハザード、安全制約の識別
 - Step0 準備2 コントロールストラクチャーの構築
 - Step1 UCA (Unsafe Control Action) の抽出
 - Step2 HCF (Hazard Causal Factor) の特定
- 既存のPHAの事例 (FS-CPUブロックの事例)
- STAMPでの定量的評価 (Quantitative analysis) について
- おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

3

1st STAMP Workshop in Japan
2016/12/7

- はじめに

製品サービス群

- 鉄道信号システム
- 交通管理システム
- 電力変換システム
- 海外事業

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

4

1st STAMP Workshop in Japan
2016/12/7

- はじめに

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

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

5

1st STAMP Workshop in Japan
2016/12/7

- はじめに

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
- 踏切しや断機
- 転てつ機

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved.

京三製作所

6

1. はじめに 1st STAMP Workshop in Japan 2016/12/7

電子連動装置 (Electronic Interlocking)

機能層 (Function layer)
ネットワーク層 (Network layer)
端末層 (Terminal layer)

FS-CPUブロック

電子端末 (point machine) 信号機 (signal)

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 7

1st STAMP Workshop in Japan 2016/12/7

1. はじめに

2. STAMP解析 (FS-CPUブロックの事例)

2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別

2-2. Step0 準備2 コントロールストラクチャーの構築

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

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

3. 既存のPHAの事例 (FS-CPUブロックの事例)

4. STAMPでの定量的評価 (quantitative analysis) について

5. おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 8

2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別 1st STAMP Workshop in Japan 2016/12/7

列車制御システム

SSI ATP FS-CPUブロック

アクシデント (accident)
衝突・脱線 (Train collision/Train derailment)

- 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。

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 9

2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別 1st STAMP Workshop in Japan 2016/12/7

事故等発生件数の推移

2005年4月25日(日)福知山線脱線
2015年5月12日(木)アトムトラック脱線
2015年11月14日(土)山手線脱線
2016年11月9日(土)高崎電車脱線

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 10

2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別 1st STAMP Workshop in Japan 2016/12/7

Railway accidents (2015)

Train collision
Train derailment

列車脱線事故 米坂線 H27.1.25
列車脱線事故 東日本旅客鉄道 井線 H27.1.24
列車脱線事故 西武旅客鉄道 高徳線 H27.10.29
列車脱線事故 京浜東北線 山田線 H27.12.11
列車脱線事故 西武旅客鉄道 高徳線 H27.12.31
列車脱線事故 長崎電気軌道 桜町支線 H27.10.11

列車衝突事故 日本貨物鉄道 函館線 H27.2.17

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

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 11

2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別 1st STAMP Workshop in Japan 2016/12/7

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時に制御リレーが扱上する。	(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。

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 京三製作所 12

2-2. Step0 準備2 コントロールストラクチャーの構築

1st STAMP Workshop in Japan
2016/12/7

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

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 13

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

1st STAMP Workshop in Japan
2016/12/7

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れていない。
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。

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 14

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

1st STAMP Workshop in Japan
2016/12/7

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6月

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 15

2-5. STAMPの解析

1st STAMP Workshop in Japan
2016/12/7

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 16

1. はじめに
2. STAMP解析 (FS-CPUブロックの事例)
 - 2-1. Step0 準備1 アクシデント、ハザード、安全制約の識別
 - 2-2. Step0 準備2 コントロールストラクチャーの構築
 - 2-3. Step1 UCA (Unsafe Control Action) の抽出
 - 2-4. Step2 HCF (Hazard Causal Factor) の特定
3. 既存のPHAの事例 (FS-CPUブロックの事例)
4. STAMPでの定量的評価 (Quantitative analysis) について
5. おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 17

3. 既存のPHAの事例

1st STAMP Workshop in Japan
2016/12/7

Item No.	Hazard	Cause	Severity	Risk	Detection	Detection (0-100%)	Risk (RPN)
1	FS-CPUの制御情報S出力が正常に出力されない	FS-CPUの制御情報S出力回路の故障	Improbable	Catastrophic	Yes	99%	High
2	FS-CPUの制御情報S折り返し情報が正常に折り返しされない	FS-CPUの制御情報S折り返し回路の故障	Remote	Catastrophic	Yes	99%	High
3	FS-CPUの制御情報P出力が正常に出力されない	FS-CPUの制御情報P出力回路の故障	Improbable	Catastrophic	Yes	99%	High
4	FS-CPUの制御情報P折り返し情報が正常に折り返しされない	FS-CPUの制御情報P折り返し回路の故障	Remote	Catastrophic	Yes	99%	High
5	FS-CPUの制御情報S出力が正常に出力されない	FS-CPUの制御情報S出力回路の故障	Improbable	Catastrophic	Yes	99%	High
6	FS-CPUの制御情報S折り返し情報が正常に折り返しされない	FS-CPUの制御情報S折り返し回路の故障	Remote	Catastrophic	Yes	99%	High
7	FS-CPUの制御情報P出力が正常に出力されない	FS-CPUの制御情報P出力回路の故障	Improbable	Catastrophic	Yes	99%	High
8	FS-CPUの制御情報P折り返し情報が正常に折り返しされない	FS-CPUの制御情報P折り返し回路の故障	Remote	Catastrophic	Yes	99%	High

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 18

3. 既存のPHAの事例 1st STAMP Workshop in Japan 2016/12/7

システム

想定事象から
ハザードに至る要因を解析する流れ

Input 機能1 Output
機能2

与える影響
与える影響
与える影響

どのハザードに至るか

衝突・脱線
(Train Collision/Train Derail)

アプローチ
ボトムアップ
(bottom-up approach)

リスクレベル(Risk Level)

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 19

1st STAMP Workshop in Japan 2016/12/7

- はじめに
- STAMP解析 (FS-CPUブロックの事例)
 - Step0 準備1 アクシデント、ハザード、安全制約の識別
 - Step0 準備2 コントロールストラクチャーの構築
 - Step1 UCA(Unsafe Control Action)の抽出
 - Step2 HCF(Hazard Causal Factor)の特定
- 既存のPHAの事例 (FS-CPUブロックの事例)
- STAMPでの定量的評価 (Quantitative analysis) について
- おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 20

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

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、稼働性、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

サービス品質 (Quality of service)
信頼性 (Reliability)
可用性 (Availability)
保守性 (Maintainability)

故障率 (Failure rate)
稼働率 (Operational rate)
修理時間 (Repair time)

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 21

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

IEC62278 (EN50126) RAMS規格

INTERNATIONAL STANDARD IEC 62278
国際規格

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

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 22

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

IEC62278 (EN50126) RAMS規格

図 10-10 V 学際モデル

6.3 フェーズB: リスク分析
6.3.1 目的

- システムに伴うハザードを特定する。
- ハザードを引き起こす事象を特定する。
- ハザードのリスクを割り出す。
- 継続的なリスクマネジメントプロセスを確立する。

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 23

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

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

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

故障の深刻さレベル	発生する危険に起因する結果	サービスに対する結果
Critical (危険/故障)	死に至る危険、存続しない危険、重大な損害、あるいは人命の危険、人身の傷害、財産の損失	主要システムの損失
Marginal (中程度の事象)	人身の傷害、財産の損失、あるいは人身の健康に対する危険	重大なシステム損傷
Insignificant (軽微)	人身の健康の危険性あり	軽微なシステム損傷

故障の発生頻度	発生する危険に起因する結果
Frequent (頻発)	頻りに発生し得る。おそれなく、適切な対応を必要とする可能性がある
Occasional (偶発)	頻りに発生し得る。ハザードが頻りに発生すると予測される
Rare (まれ)	システムライフサイクルのどこかで発生し得る。ハザードが頻りに発生すると予測される
Very rare (極めてまれ)	発生し得ない。可能性はある。ハザードが頻りに発生すると予測される
Unlikely (まれ)	発生する可能性は極めて低い。ハザードが発生し得ないと思定される

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 24

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

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 (Hazard Causal Factor) の特定

⑥要求仕様 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)

危険事象の発生頻度	重大でない	重大	重大	重大
頻度(発生)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可
頻度(修理)	許容可	許容可	許容可	許容可

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 25

4. STAMPでの定量的評価について 1st STAMP Workshop in Japan 2016/12/7

②ハザード ①想定事象 ③危険事象の発生頻度 ⑤リスクレベル(③×④) ⑦対策後のリスクレベル

Item	Result	Understand cause category	Frequency of occurrence of hazardous event (times)	Hazard severity and level	Qualitative risk category	HCF (Hazard Causal Factor)	Determine possible failure mode (発生モード)	Directive (指)	Detection (検) (%)	Risk (RPN)
1	危険	ハードウェア	頻度	Critical	High	想定事象	発生モード		2%	Critical
2	危険	ソフトウェア	頻度	Critical	High	想定事象	発生モード		2%	Critical
3	危険	ソフトウェア	頻度	Critical	High	想定事象	発生モード		2%	Critical
4	危険	ソフトウェア	頻度	Critical	High	想定事象	発生モード		2%	Critical
5	危険	ソフトウェア	頻度	Critical	High	想定事象	発生モード		2%	Critical

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 26

1st STAMP Workshop in Japan 2016/12/7

- はじめに
- STAMP解析 (FS-CPUブロックの事例)
 - Step0 準備1 アクシデント、ハザード、安全制約の識別
 - Step0 準備2 コントロールストラクチャーの構築
 - Step1 UCA (Unsafe Control Action) の抽出
 - Step2 HCF (Hazard Causal Factor) の特定
- 既存のPHAの事例 (FS-CPUブロックの事例)
- STAMPでの定量的評価 (Quantitative analysis) について
- おわりに

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 27

5. おわりに 1st STAMP Workshop in Japan 2016/12/7

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。

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。

連携

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 28

5. おわりに 1st STAMP Workshop in Japan 2016/12/7

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)

既存システム → Unified Train System

Safety 0.0 ■人の注意力に頼る時代

Safety 1.0 ■安全を組み込んだものを提供する時代

Safety 2.0 ■それぞれが必要な情報を交換することにより安全を確保する時代

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 29

1st STAMP Workshop in Japan 2016/12/7

謝辞

ご清聴ありがとうございました

Thank you for your attention.

Copyright 2016 kyosan Electric Mfg. Co., Ltd. All Rights Reserved. 30