STAMP Workbenchではじめる安全分析

株式会社　チェンジビジョン

ChangeVision

STAMP支援ツール

STAMP Workbench

IPA

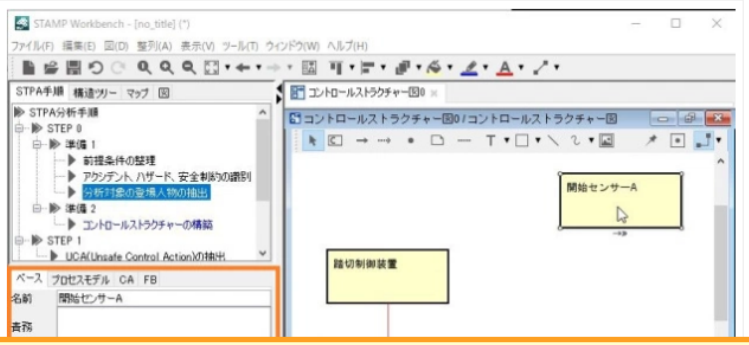
2018/03月～ IPAより無償提供中

STAMP/STPA向けモデリングツール「STAMP Workbench」リリース

by Satomi Joba　April 4, 2018　announcement

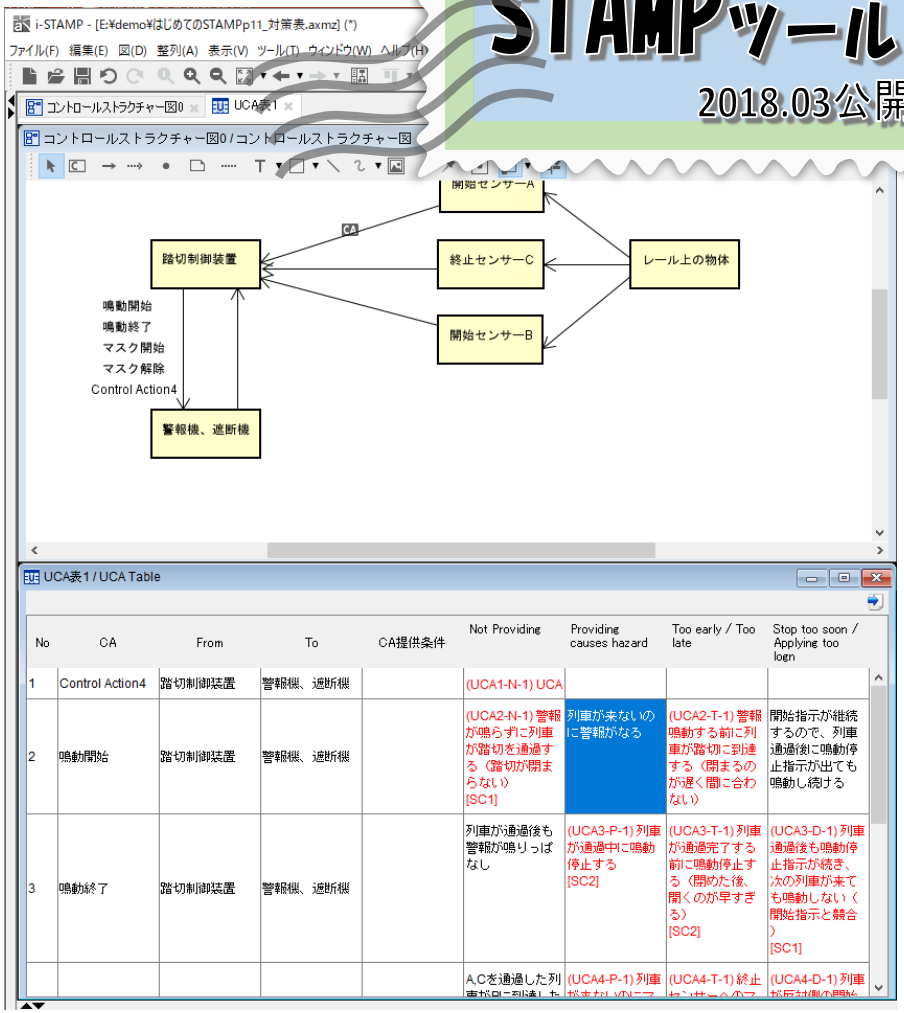
STAMP Workbench

3月30日、IPA(独立行政法人情報処理推進機構)は、大規模・複雑化するシステムに適した安全解析手法STAMPの導入を容易にするモデリングツール「**STAMP Workbench**」を無償公開しました。このSTAMP Workbenchのモデリングツールのベースには、astah*を採用頂きました。



https://ja.astahblog.com/2018/04/04/stamp-workbench-by-ipa/
「STAMP Workbench」で検索

NIPPON発
STAMPツール
2018.03公開



No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too logn
1	Control Action4	踏切制御装置	警報機、遮断機		(UCA1-N-1) UCA			
2	鳴動開始	踏切制御装置	警報機、遮断機		(UCA2-N-1) 警報が鳴らずに列車が踏切を通過する（踏切が閉まらない）[SC1]	列車が来ないのに警報がなる	(UCA2-T-1) 警報鳴動する前に列車が踏切に到達する（閉まるのが遅く間に合わない）	開始指示が継続するので、列車通過後に鳴動(停止指示が出ても鳴動し続ける
3	鳴動終了	踏切制御装置	警報機、遮断機		列車が通過後も警報が鳴りっぱなし	(UCA3-P-1) 列車が通過中に鳴動停止する [SC2]	(UCA3-T-1) 列車が通過完了する前に鳴動停止する（閉めた後、開くのが早すぎる）[SC2]	(UCA3-D-1) 列車通過後も鳴動(停止指示が続き、次の列車が来ても鳴動しない（開始指示と競合）[SC1]
					ACを通過した列	(UCA4-P-1) 列車	(UCA4-T-1) 終止	(UCA4-D-1) 列車

会社概要

- **商号**
  - 株式会社チェンジビジョン （英語名 Change Vision, Inc）
- **設立**
  - 2006年 2月 22日
- **代表者**
  - 代表取締役社長　熊谷恒治
  - 代表取締役　平鍋健児
- **所在地**
  - 本社　東京都千代田区神田須田町 2-3-1　NBF神田須田町ビル7F
  - 福井開発部　福井県福井市問屋町3-111
  - 米国マーケティングパートナー　Prosynesis （オハイオ州）
- **事業内容**
  - ソフトウェア開発環境を支援するツールの製造・販売
  - ソフトウェア工学適用のコンサルティング
  - 主力製品　astah* （旧製品名 JUDE）

astah 製品ラインナップ

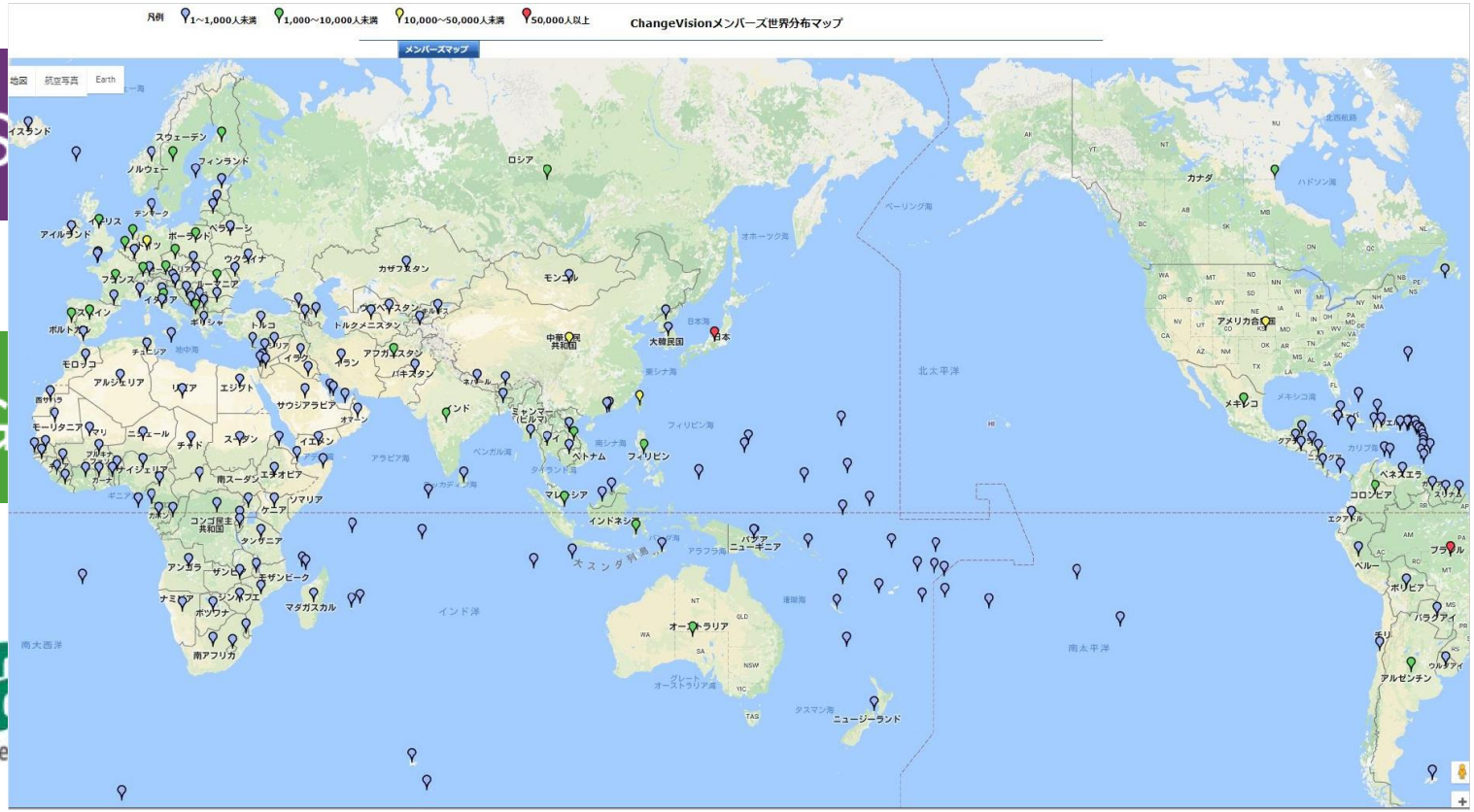
astah pro

astah S

astah G

Sa Safety Conce

全世界 50万越のユーザーに支えられるモデリングツール



STAMP / STPA

STAMP/STPAとは

STAMP

（Systems Theoretic Accident Model and Process）

現代のシステムのアクシデントの多くは、システム構成要素の故障によって起きるのではなく、システムの中で安全のための制御を行う要素（コントローラー：Controller）と制御される要素（被コントロールプロセス：Controlled Process）の相互作用が働かないことによって起きるというアクシデントモデル

STPA

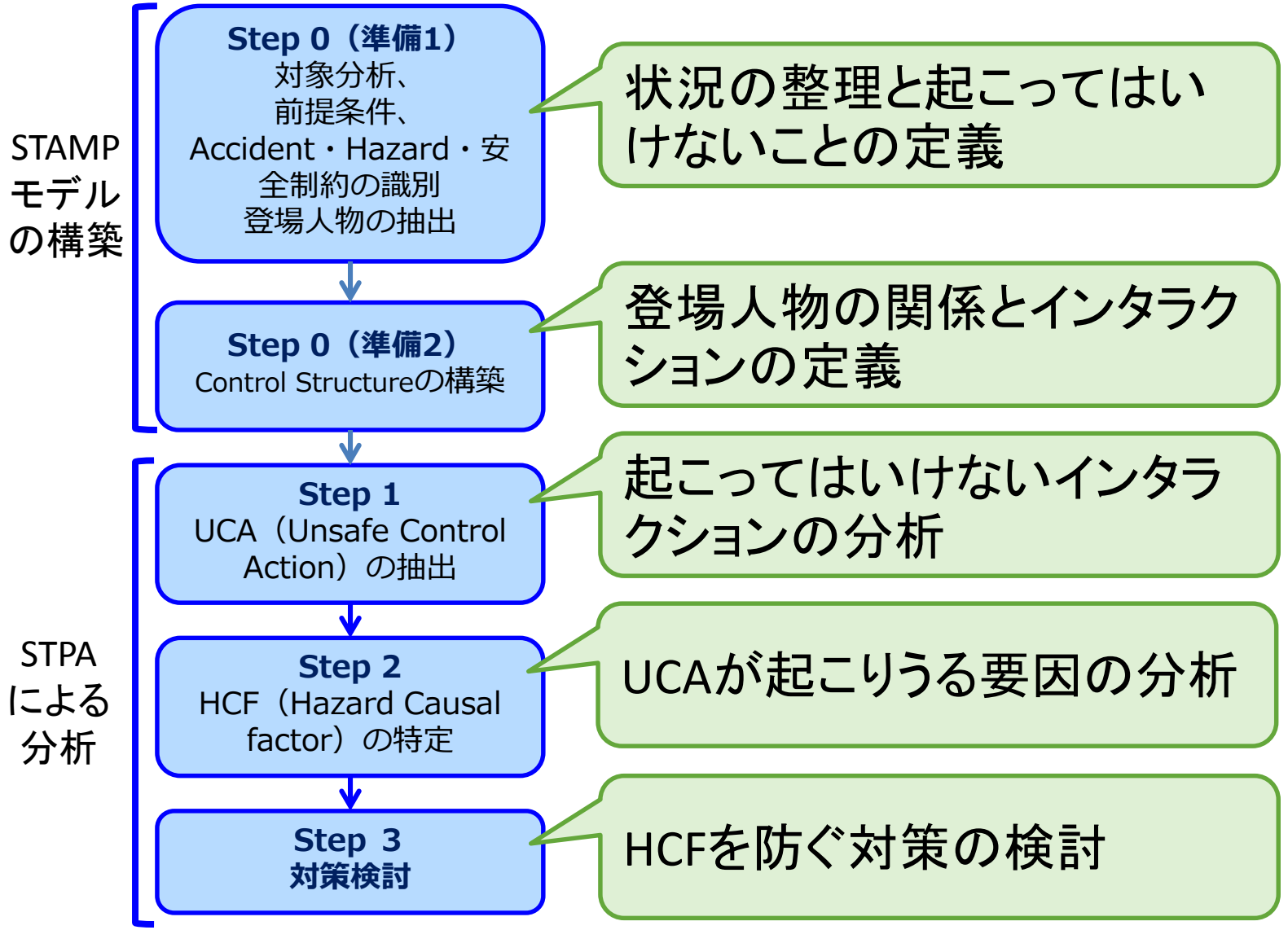
（STAMP based Process Analysis）

STAMP アクシデントモデルを前提として、システムのハザード要因を分析する新しい安全解析手法

はじめてのSTAMP/STPA

https://www.ipa.go.jp/sec/reports/20160428.html「IPA　STAMP」で検索

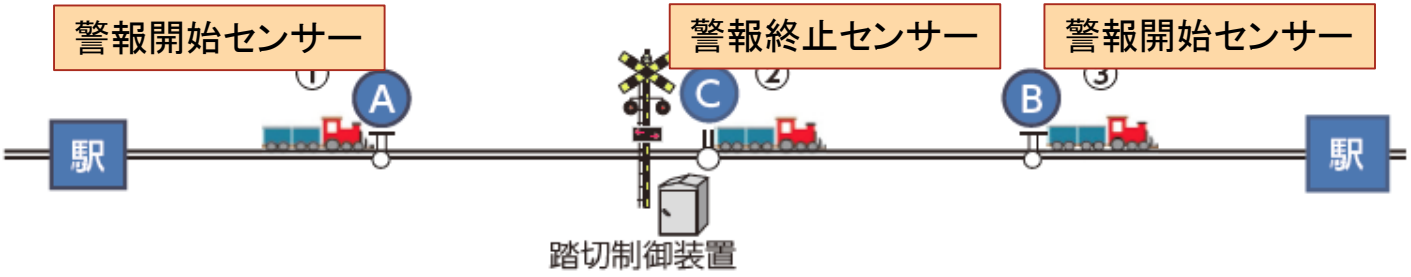
STPA手順



DEMO：プロジェクト作成

前提条件

単線の駅中間踏切制御装置



出典:IPA, はじめてのSTAMP/STPA p11～, Ver1.0, 2016/3

- 前提条件
  - 車両を検知するセンサ（A,B,C）と踏切制御装置からなるシステム
  - 警報開始センサ（A,B）が車両を検知すると、踏切鳴動を開始する
  - 警報終止センサー（C）が車両を検知し一定時間後に警報鳴動を停止する
  - センサAを検知した時は、センサBをマスクする。同様にBを検知した時はAをマスクする

DEMO：前提条件

Step0準備1:
アクシデント・ハザード・安全制約

Accident
望ましくない事象

Hazard
Accidentが起こりうる状態

Safety Constraint
Hazardを防ぐ安全制約

［Accident］
列車と人・車が踏切内で衝突する

［Hazard］
列車接近中に踏切が閉まらない

［Hazard］
列車通過中に踏切が開く

［Safety Constraint］
列車が在線中は踏切が閉まらなければならない

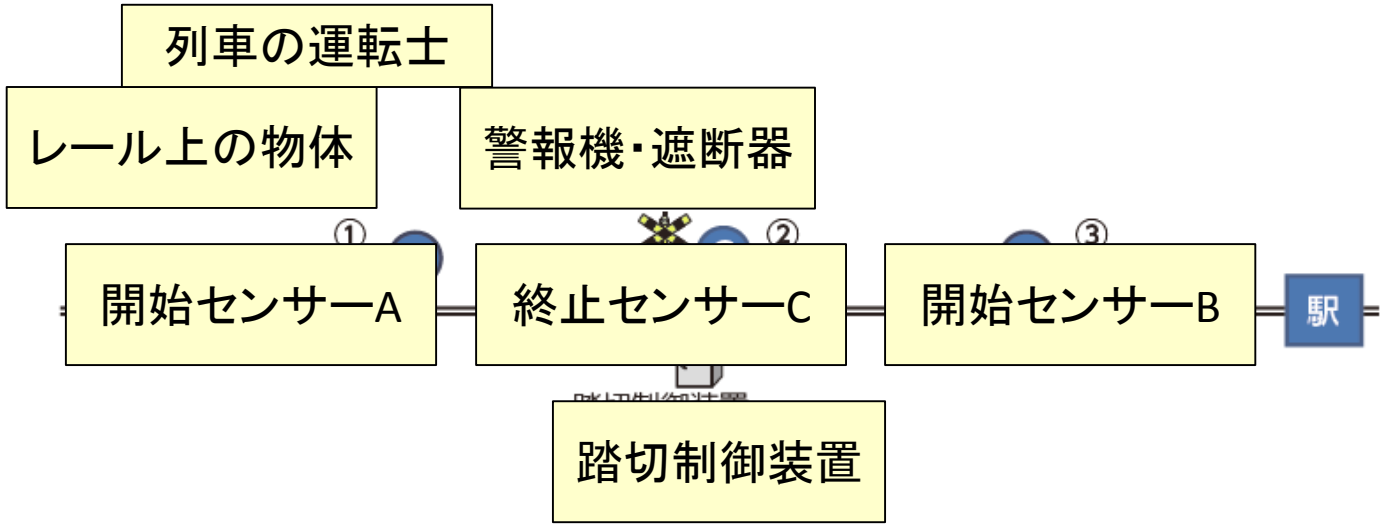
［Safety Constraint］
列車が在線中は踏切が開いてはならない

アクシデントハザード安全制約表0 / Accident Hazard Safety Constraint Table

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	列車と人・車が踏切内で衝突する	H1	列車が在線中に踏切が開まらない（警報が鳴らない）	SC1	列車が在線中は踏切が開まらなければならない
A1	列車と人・車が踏切内で衝突する	H2	踏切遮断後、列車が在線中に踏切が開く（警報が鳴りやむ）	SC2	列車が在線中は踏切が開いてはならない
A2	列車が開かず、交通が渋滞する	H3	列車が不在なのに踏切が開まる（警報が鳴りだす）	SC3	列車が不在ならば踏切を開じない
A2	列車が開かず、交通が渋滞する	H4	列車が通過したのに踏切が開かない（警報が鳴りやまない）	SC4	列車が通過したら踏切を開ける

DEMO : AHS

Step0準備1:
分析対象の登場人物の抽出



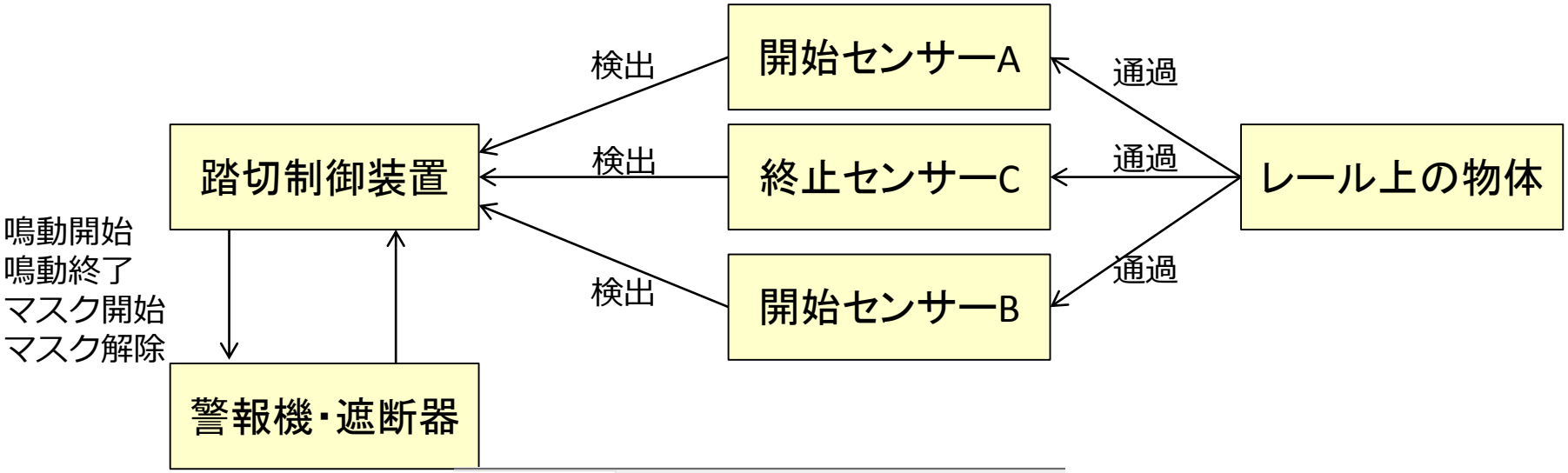
コンポーネント抽出表0 / Component Extracting Table

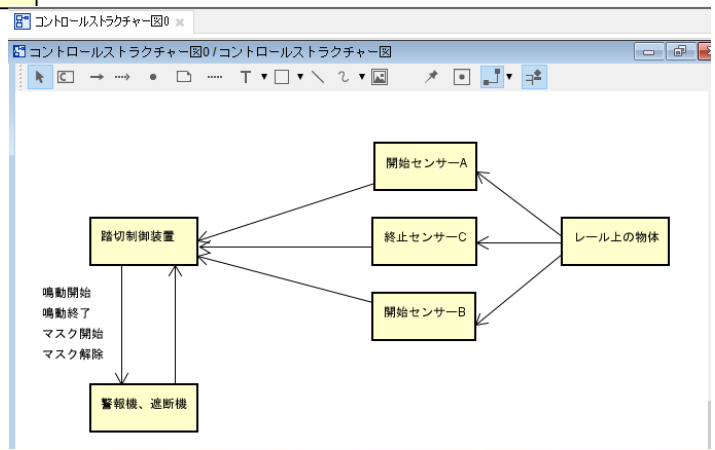
対象	登場人物	責務	コントロールアクション	フィードバック	備考
☑	踏切制御装置		鳴動開始 (To: 警報機、遮断機) 鳴動終了 (To: 警報機、遮断機) マスク開始 (To: 警報機、遮断機) マスク解除 (To: 警報機、遮断機)		
☑	警報機、遮断機				
☑	レール上の物体				
☑	開始センサーA				
☑	終止センサーC				
☑	開始センサーB				
☐	列車の運転士				分析対象外

DEMO : 抽出表

Step0準備2：コントロールストラクチャの作成

コンポーネント抽出表で整理した登場人物から、分析対象のコンポーネントを選定し、安全制約の実現に関係するコンポーネント（サブシステム、機器、組織等）、及び**コンポーネント間の相互作用**（コントローラによる指示、フィードバックデータ）を抽出し、それらの関係を表す**Control Structure** を構築する。





DEMO : CS

Step1 : Unsafe Control Actionの抽出

Control Structureから安全制約の実行に必要なコントローラによる指示(Control Action)を識別し、**ガイドワード**を適用して、ハザードにつながる**非安全なControl Action（UCA）**を抽出する。

UCA表1 / UCA Table

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too logn
1	鳴動開始	踏切制御装置	警報機、遮断機		(UCA1-N-1) 警報が鳴らずに列車が踏切を通過する(踏切が開まらない) [SC1]	列車が来ないのに警報がなる	(UCA1-T-1) 警報鳴動する前に列車が踏切に到達する(閉まるのが遅く間に合わない)	開始指示が継続するので、列車通過後に鳴動停止指示が出ても鳴動し続ける
2	鳴動終了	踏切制御装置	警報機、遮断機		列車が通過後も警報が鳴りっぱなし	(UCA2-P-1) 列車が通過中に鳴動停止する [SC2]	(UCA2-T-1) 列車が通過完了する前に鳴動停止する(閉めた後、開くのが早すぎる) [SC2]	(UCA2-D-1) 列車通過後も鳴動停止指示が続き、次の列車が来ても鳴動しない(開始指示と競合) [SC1]
3	マスク開始	踏切制御装置	警報機、遮断機		ACを通過した列車がBに到達した時に再鳴動する	(UCA3-P-1) 列車が来ないのにマスク指示し、警報鳴動しない [SC1] (UCA3-P-2) 反対側の開始センサーにマスク指示し、警報鳴動しない [SC1]	(UCA3-T-1) 終止センサーへのマスク指示が遅れ、列車の当該センサー通過に間に合わないと、マスク指示が残り、対向列車が二本続いたときに警報鳴動しない [SC1]	(UCA3-D-1) 列車が反対側の開始センサー通過後までマスク指示し続けると、対向列車が来ても鳴動しない [SC1]
4	マスク解除	踏切制御装置	警報機、遮断機		(UCA4-N-1) 反対側の開始センサーにマスク解除指示が出ず、対向列車が来ても鳴動しない(マスク指示後に列車が引き返す場合を含む) [SC1]	警報が再鳴動する	列車がBを通過完了前に出ると再鳴動する	解除を後続列車によるマスク開始指示と競合するとマスクされずに再鳴動する可能性がある

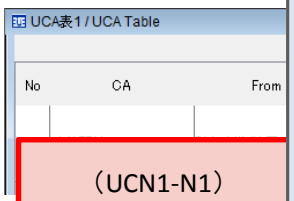
Not Provide	Providing causes-hazard	Too early / Too late	Stop too soon / Applying too long
来なかったら？	(意図せず)来たら？	早かったら？ 遅れたら？	短かったら？ 長かったら？

DEMO : UCA

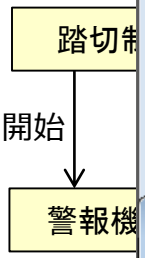
Step1：Hazard Causal Factorの特定

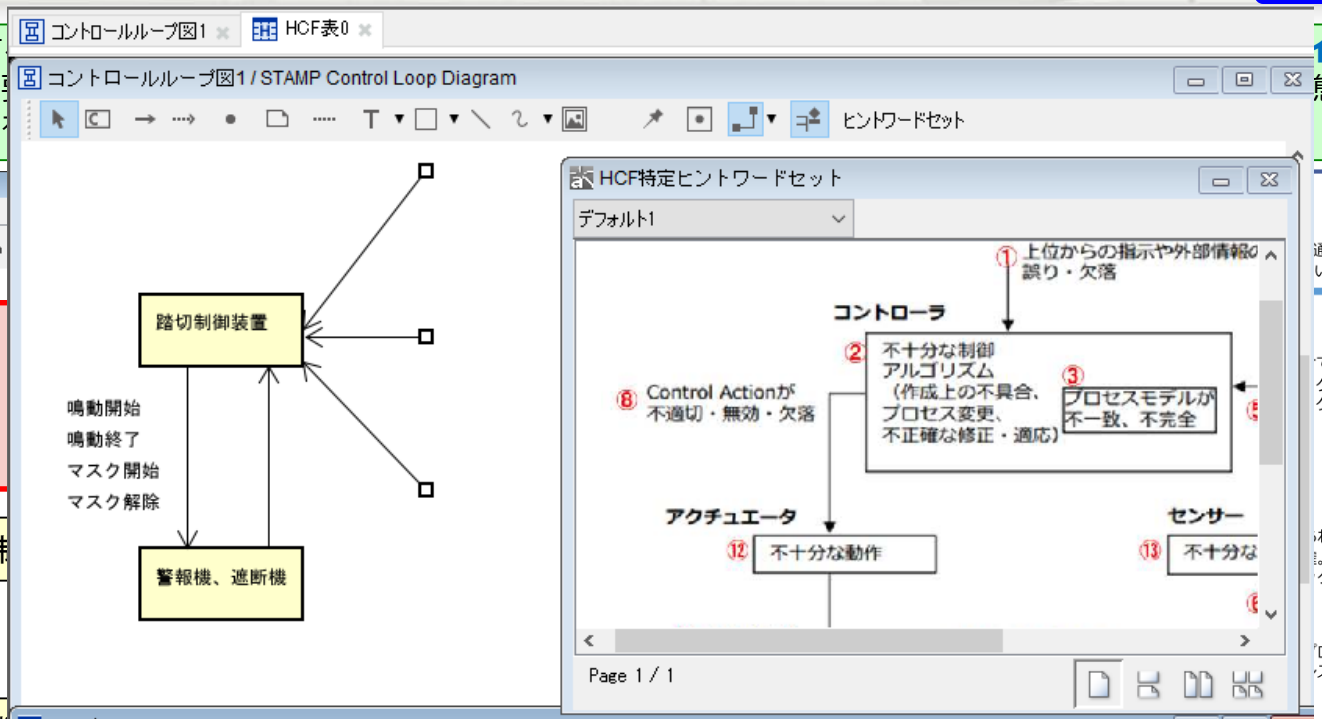
- Step 0 -1: 登場人物
- Step 0-2：CSの構築
- Step 1：UCAの抽出
- Step 2：HCFの特定
- Step 3：対策検討

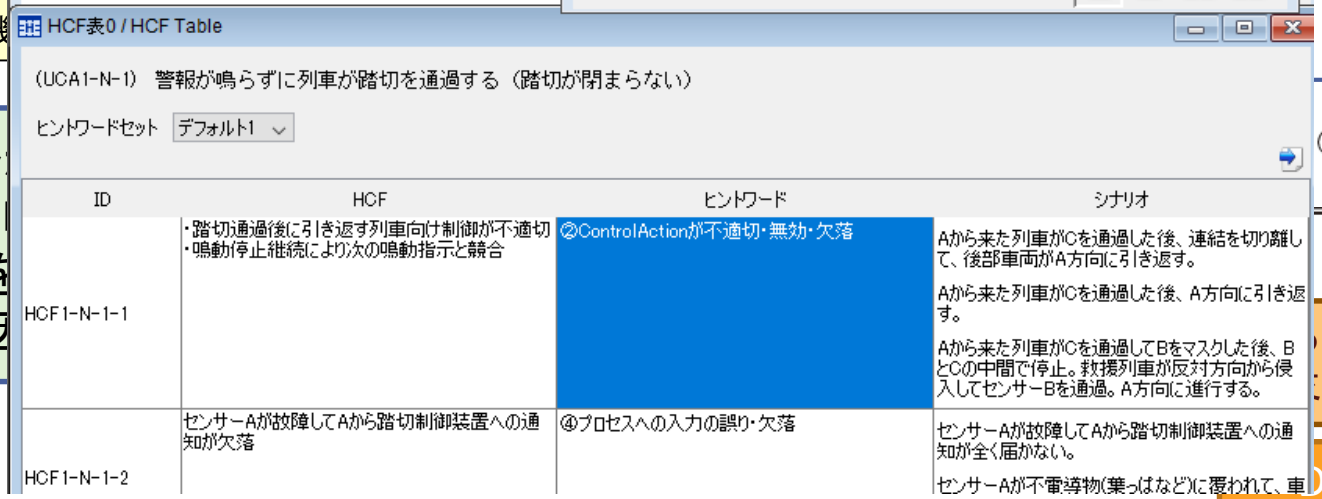
UCA毎に，関係す… 適用してハザード… ことで起きる要因… …イドワードを …態と矛盾する



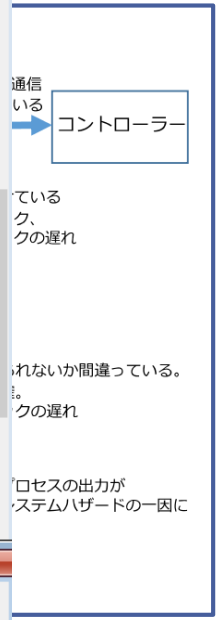
（UCN1-N1）
警報が鳴らず列車が踏切を通過する（踏切が閉まらない）







関係するコン… 抽出し（コント… ヒントワードを… こりうる要因…



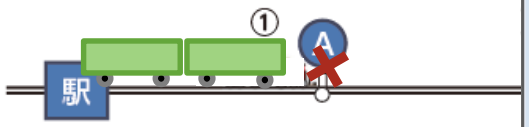
DEMO：HCF

Step3：対策検討

分析から得たハザードシナリオへの対策を検討する。

- Step 0 -1: 登場人物
- Step 0-2：CSの構築
- Step 1：UCAの抽出
- Step 2：HCFの特定
- Step 3：対策検討

HCF:センサAが故障して、踏切制御装置への通知が

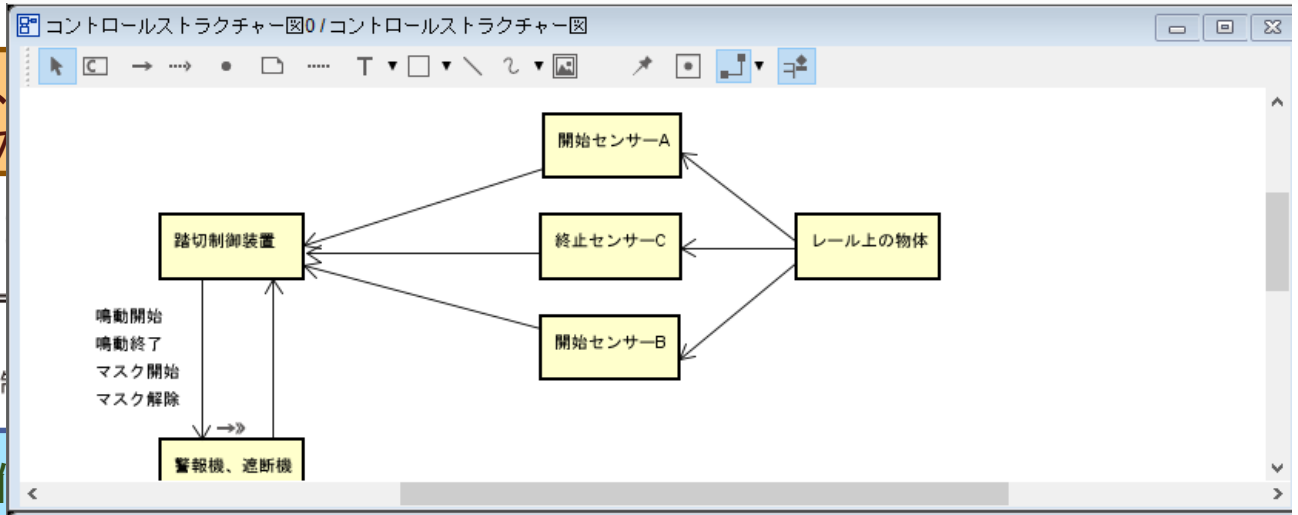


踏切制

【対策1】センサを多重化

【対策2】Heartbeat信号センサ異常を常に監視

【対策3】車両GPSと併用



UCA表1 / UCA Table

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too logn
1	鳴動開始	踏切制御装置	警報機、遮断機		(UCA1-N-1) 警報が鳴らずに列車が踏切を通過する(踏切が閉まらない) [SC1]	列車が来ないのに警報がなる	(UCA1-T-1) 警報鳴動する前に列車が踏切に到達する(閉まるのが遅く間に合わない)	開始指示が継続するので、列車通過後に鳴動停止指示が出ても鳴動し続ける

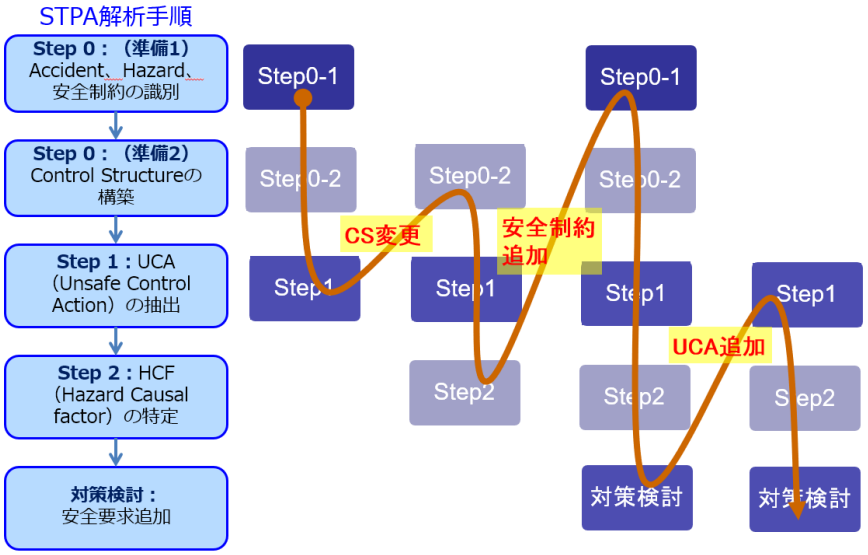
対策表0 / Countermeasure Table

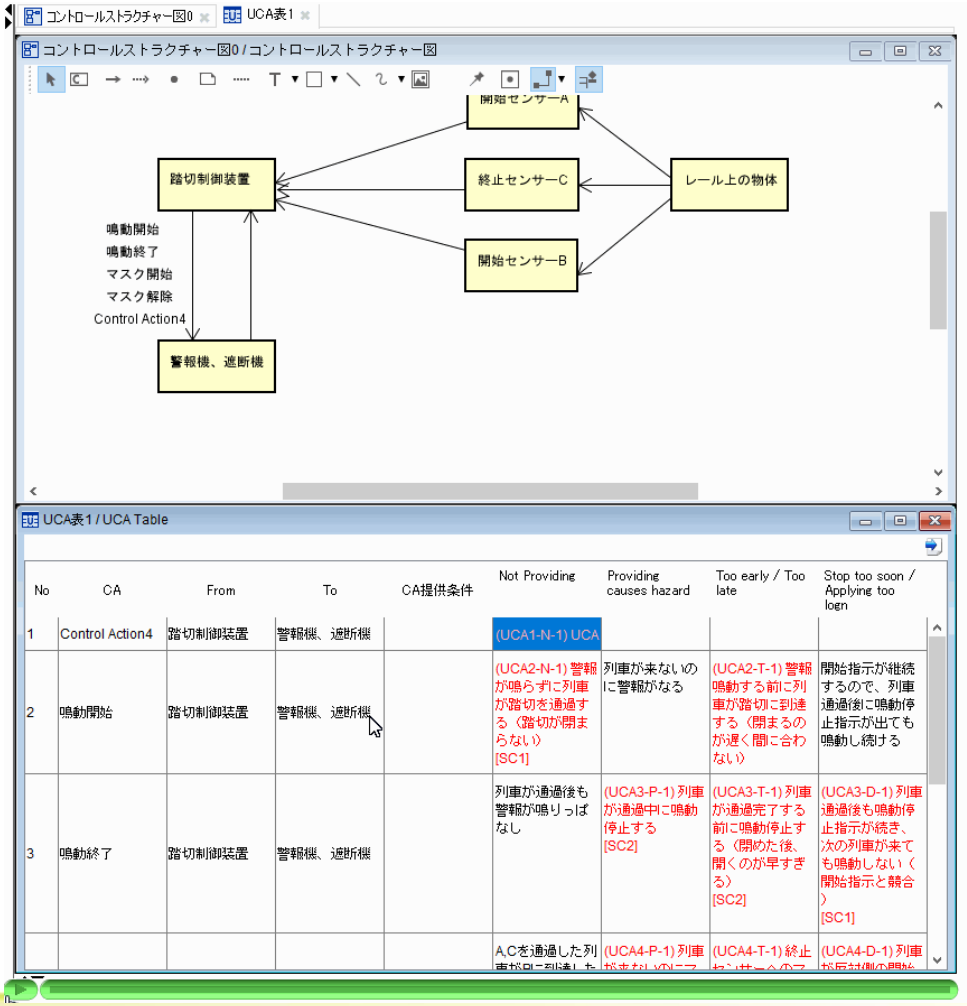
HCFID	HCF	対策ID	対策	UCA	対策対象コンポーネント	備考
HCF1-N-1-1	・踏切通過後に引き返す列車向け制御が不適切 ・鳴動停止継続により次の鳴動指示と競合	M1	センサー検出順番の不正を検出したら警報鳴動し続ける	UCA1-N-1	踏切制御装置	順番の正誤判断基準要
HCF1-N-1-2	センサーAが故障してAから踏切制御装置への通知が欠落	M2	開始センサーからの信号が途絶えたら警報を鳴らす	UCA1-N-1	踏切制御装置 開始センサーA 開始センサーB	Heartbeat, Healthy信号等による監視機能が必要

DEMO：対策

イテレーティブな分析サポート

解析の過程で不足や誤りに気付いたら、分析手順を立ち戻って解析しなおせる





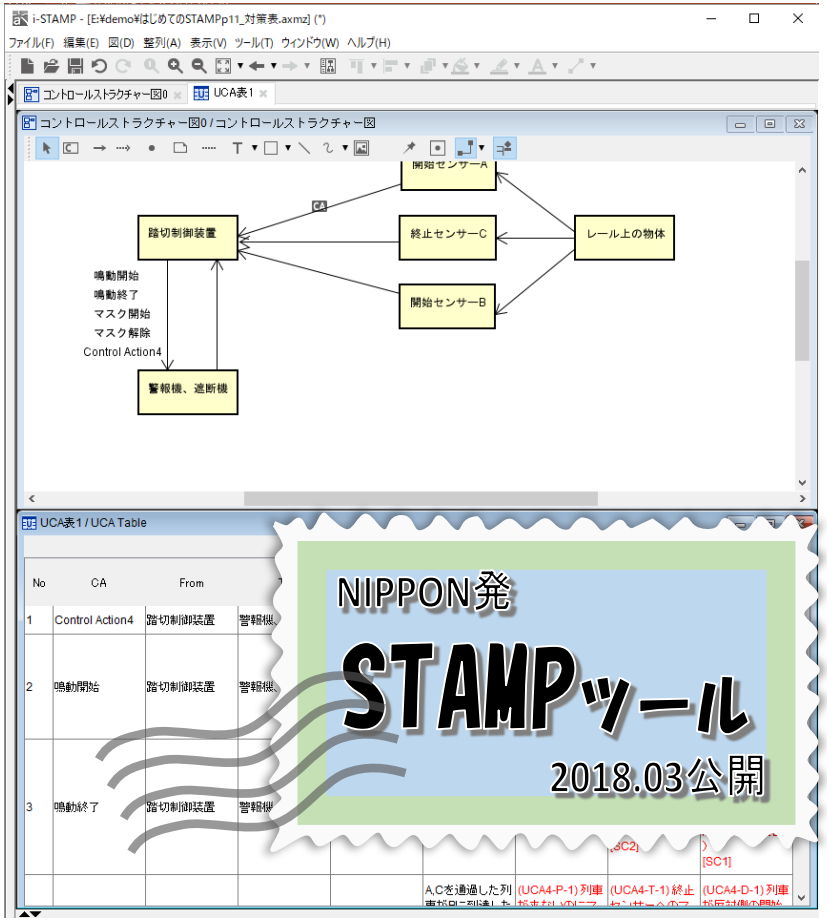
ツール拡張


利用者が自社向けにツール強化、またはツールベンダーが強化して提供
STAMP図テンプレート追加
STAMP表拡張
自社ツール形式データ出力
自社ツール連携
STPA手順カスタマイズ
トレーサビリティ機能追加等、・・・
他手法手順の追加(CAST,STPA-Sec等)
ツール利用者が開発して社内利用
ツールベンダーが機能強化して提供
STAMPカスタムのご要望お待ちしております
STAMP支援ツール
（基本的には(1)+(2)の組合せで使い続けることが可能）
（1）本ツール開発範囲 （ソースコードおよびバイナリー公開）
STAMP図生成
STAMP表生成
汎用形式データ出力
外部ツール連携I/F
STPA基本手順支援
IPAが提供
（2）既存モデルベース開発支援ツールのプラットフォーム
（バイナリー公開）
ファイル管理機能
モデル描画基本機能
モデル編集基本機能
GUI基本機能
API基本機能
ツール開発受注者が提供

まとめ

- IPA STAMP/STPAツールの特徴
  - 分析者の思考を妨げないUIの提供
  - 商用ツールの使い勝手、機能を踏襲
  - STAMP導入の難しさを低減するIPA推奨手順のガイドの組み込み

https://ja.astahblog.com/2018/04/04/stamp-workbench-by-ipa/




IPA
Better Life
with IT