STAMPベース ハザード分析ツールの紹介

A Brief Survey of STAMP-based Hazard Analysis Tools

2nd STAMP Workshop Japan

National Institute of Technology, Sendai College

Keishi Okamoto

目次

- はじめに
- STAMP/STPA概説
- STAMP/STPA支援ツール
  - 専用支援ツール以外のツールの活用
  - XSTAMPP
  - SafetyHAT
- まとめ

STAMP/STPA導入の課題

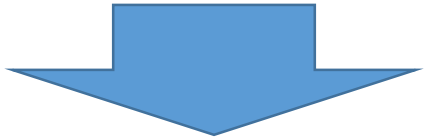
- STAMP/STPA導入における課題
  - STAMP/STPAプロセスのガイド
    ⇒「An STPA Primer (MIT)」,
    ⇒「はじめてのSTAMP/STPA入門編 (IPA)」他
  - 分析成果物の記述・修正に手間がかかる（後述）
    - 本来の分析に対する思考集中が妨げられる

    ⇒ STAMP/STPA支援ツールの活用
- ツール活用における課題
  - 既存STAMPツールは大学等が開発
  - 連携・流用可能なMBD支援ツールは一般に高価

MBD：Model Base Development モデルベース開発

STAMP/STPA概説

- STAMP/STPA手順
  - 「はじめてのSTAMP/STPA入門編」を基に概説
- STAMP/STPAの各Step出力のデータ形式
  - A STPA Primer [Leveson, Thomas 2013]
  - はじめてのSTAMP/STPA入門編 [IPA 2016]
- STPAの各Stepで気付いた点・課題等
  - 標準的なデータ形式の課題
  - 描画ツール・表作成ツールによる記述の課題



STAMP/STPA支援ツールに期待するモノ

Step0-1 アクシデント，ハザード，安全制約の識別

作業名称	アクシデント、ハザード、安全制約の識別
目　　的	アクシデントを定義する 安全制約を導き出す
入　　力	①要求仕様書 ②［ドメイン専門家］
処　　理	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アクシデントと成り得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程度の粒度で安全制約を導き出す
出　　力	①アクシデント、ハザード、安全制約の一覧表
備　　考	・アクシデント：喪失（Loss）を伴うシステムの事故 ・ハザード：アクシデントにつながるシステムの状態 ・安全制約：システムが安全に保たれるために必要なルール 例えば、踏切制御システムにおいて。 踏切がいつまでも開かないのは、サービス利用者･提供者に経済的損失を与えたり、精神的苦痛を与えることになることもあるが、人の生命に関わる事柄に焦点を絞ったときには『アクシデントではない』と定義できる。

表 4.2-1 手順：Step0 準備1アクシデント、ハザード、安全制約の識別 [IPA2016]

例：Step0-1 A/H/SCの一覧表の出力

アクシデント（Loss）	ハザード（Hazard）	安全制約（Safety Constraints）
(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閉まらない（警報が鳴らない）	(SC1) 列車が在線中は踏切が閉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（警報が鳴り止む）	(SC2) 列車が在線中は踏切が開いてはならない
ず、交通が渋滞する	列車が不在なのに踏切が閉まる（警報が鳴りだす）	列車が不在ならば踏切を閉じない
ず、交通が渋滞する	列車が通過したのに踏切が開かない（警報が鳴り止まない）	列車が通過したら踏切を開ける

番号付けは
参照時に便利

表 4.2-2 実施例：Step0 アクシデント、ハザード、安全制約の識別 [IPA2016]

Hazard	Related Accident
H-1: Release of radioactive materials	A-1, A-2
H-2: Reactor temperature too high	A-1, A-2, A-3, A-4
H-3: Equipment operated beyond limits	A-3, A-4
H-4: Reactor shut down	A-4

pp.47 [LevesonThomas2013]

関係は一般に多対多
項目に重複が発生
(修正漏れの可能性)

Step0-2
コントロールストラクチャーの構築

作業名称	コントロールストラクチャーの構築
目　　的	登場人物間の依存関係を制御構造図で表す。 制御主体と制御対象の間で行われる制御（サブシステム間の相互作用）には何があるかを明確化する。 その後の分析作業において理解し易いイメージを共有する。
入　　力	①要求仕様書
処　　理	①要求仕様書から登場人物（ブロック）を抽出する ②要求仕様書から各ブロックの役割を抽出する。 ③役割を果たすために必要な制御、役割を果たした結果のフィードバックを抽出する。 ④制御、入出力情報（情報を与えるのみで制御を行うわけではない）の違いを分別する ⑤ブロック間を矢印線で結び、制御・入出力を・・(?) センサー出力のようなフィードバックを制御と考える ??
出　　力	①制御構造（コントロールストラクチャー）図
備　　考	ブロックの数は 4 つ程度が良いと言われている。 それ以上多くなる（抽象度を下げる）と、以降の分析すべき組み合わせが多くなり、集中しにくくなる、検討漏れを起こしかねないので、工夫が必要になる。

表形式もある(SafetyHAT)

出典：[I]pp.17,表 4.3 1 手順：Step0 準備2 コントロールストラクチャーの構築

例：Step0-2出力 PM付CSD

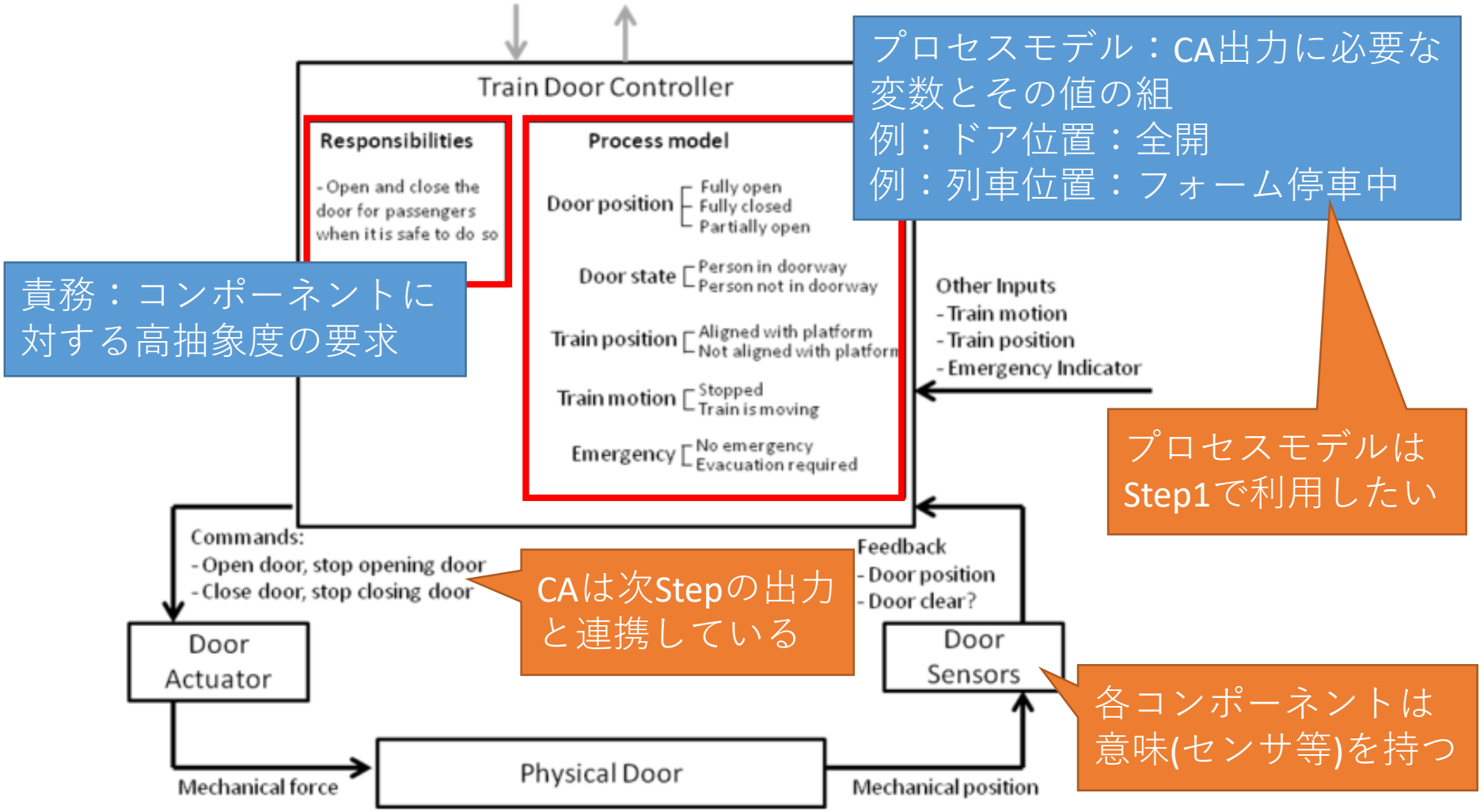


Figure 2.13. Simple Safety Control Loop for a Train Door Controller [LevesonThomas2013]

例：Step0-2出力 CSD(詳細化)

コントロールストラクチャーは大変複雑なので，抽象化したり，一部を詳細化することは，コントロールを理解するのに役立つ

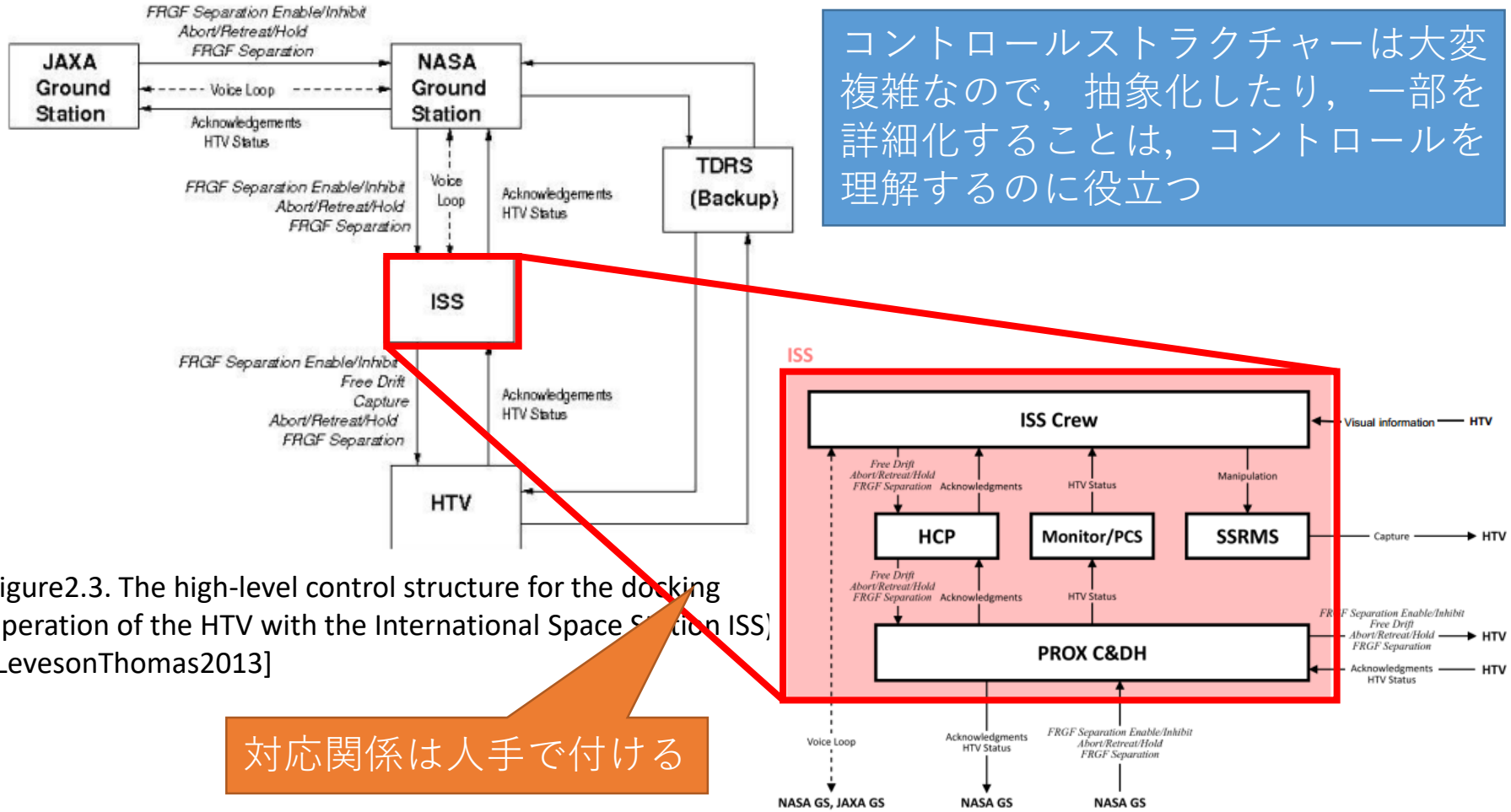


Figure2.3. The high-level control structure for the docking operation of the HTV with the International Space Station ISS) [LevesonThomas2013]

対応関係は人手で付ける

Figure 2.5. A more detailed view of the ISS control structure for HTV docking.

Figure 2.5. A more detailed view of the ISS control structure for HTV docking. [LevesonThomas2013]

Step1 非安全制御動作の抽出

作業名称	UCA（Unsafe Control Action：非安全制御動作）の抽出
目　的	ハザードにつながり得る制御動作の不具合を識別する（発想する）
入　力	①UCA を導き出すための 4 つのガイドワード（4 分類） ②アクシデント、ハザード、安全制約の一覧表 ③制御構造図
処　理	①UCA 識別の表を準備する ②最上列に 4 つのガイドワードを記す ③最左行に制御構造図中にある制御をすべて記す ④各マスごとに、当該（最左行の）制御動作が当該（最上列）状況になった場合、いずれかの安全制約違反に成り得るかを考える。 ⑤安全制約違反に成り得るならば、UCA であると判断する
出　力	①縦軸：制御行動、横軸：ガイドワードとした UCA 一覧表。
備　考	想定外を排除することを忘れないように。

表 4.4 1 手順：Step1 UCAの抽出 [IPA2016]

例：Step1出力 UCA一覧表

Step0-1 CS図内のCAを列挙

縦：制御行動　　横：ガイドワード(タイプ)

STPAで定義済

番号を付与

#	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	鳴動開始指示	(UCA1) 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) 違反	列車が来ないのに警報が鳴る	(UCA2) 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) (SC1) 違反	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	鳴動停止指示	列車が通過後も警報が鳴りっぱなし	(UCA3) 列車が通過中に鳴動停止する (SC2) 違反	(UCA3) 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) 違反	(UCA1) 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) 違反
3	マスク開始指示	A、Cを通過した列車がBに到達した時に再鳴動する	(UCA4) 列車が来ないのにマスク指示し、警報鳴動しない (UCA4) 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) 違反	(UCA5) 終始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2本続いたときに警報鳴動しない (SC1) 違反	(UCA6) 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) 違反
4	マ	開始 除指 が来 車が 引き返す場合を含む) (SC1) 違反	警報が再鳴動する		によるマ 続合うと 再鳴動す

UCAに番号を付与すると参照が容易

ハザードへ至る条件(+ハザード, 安全制約)

表 4.4-2 実施例：Step1 UCAの抽出 [IPA2016]

Step2 誘発要因の特定

作業名称	HCF（Hazard Causal factor：誘発要因）の特定
目　　的	どのようなHCFがあったらUCAに成り得るのかを考え、ハザードシナリオを作る
入　　力	①HCF特定のための11個のガイドワード ②制御構造図 ③UCA一覧表
処　　理	①制御構造図からコントロールループを抜き出して、その中の各制御に該当するガイドワードを割り当てる ②［制御構造図中の各制御に該当するガイドワードを割り当てる］ ③Step1で識別したUCA毎に、ガイドワードをひとつづつ当てはめてみて、ハザードと成り得るかを考える ④ハザードと成り得るならば、どういう条件下で当該ガイドワードの事象が発生して、その後、どういうシステム挙動になったらハザードとなって、アクシデントにつながるかのシナリオを作る
出　　力	①縦軸：UCA, 横軸：ガイドワードとした、ハザード要因の一覧表 ②ハザードシナリオ
備　　考	すべてのUCAに夫々ガイドワ[illegible]すべてを当てはめて考える

4.5. Step2 HCF (Hazard Causal Factor)の特定
[IPA2016]

①にはリストを，②にはアノテーション付きCLDを使うこともある

例：Step2出力CF一覧表とシナリオ

表 4.5-2 実施例：Step2 HCF の特定 [IPA2016]

	①上位からの指示や外部情報の誤り・欠落	②Ｃｏｎｔｒｏｌ action が不適切・無効・欠落	③動作の遅れ	④プロセスへの入力の誤り・欠落	⑤意図しない、または範囲外の外乱	⑥不十分な制御・アルゴリズム
(UCA1) 警報が鳴らずに列車が踏切を通過 (踏切が閉まらず)		・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		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		
(UCA2) 鳴動前に列車が踏切に到達 (閉まるのが遅い)			・警報機の動れ			
(UCA3) 列車が踏切を通過する前に鳴動停止 (開くのが早い)						
(UCA4) 不正なマて、警						
(UCA5) マスク解除指示漏れで、列車がきても鳴動せず			・超高速応できクク解除の指れ			
(UCA6) マスク開始指示漏れ	・誤った外部入力（外乱）でマスク解除漏れ	・制御装置の処理遅れでマスク解除漏れ	・状態制御誤マスク解除			

横：ガイドワード

縦：UCA

ハザード要因

対応関係は人手で付ける

Step1 UCA表のUCAを列挙

シナリオ

■（UCA1）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）安全制約 1 に違反

シナリオ 1-1「④プロセスへの入力の誤り・欠落」センサー A が故障して A から踏切制御装置への通知が全く届かない
- 対策：開始センサーからの信号が途絶えたら警報を鳴らす

シナリオ 1-2「④プロセスへの入力の誤り・欠落」センサー A が不電導物（葉っぱなど）に覆われて、車輪経由の検知電流が流れず、列車到達を検知できない
- 対策：一瞬でも短絡したら、短絡時間異常と判断し警報鳴動し続ける
- 対策：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

シナリオ 1-3「② control action が不十分」A から来た列車が C を通過した後、連結を切り離して、後部車両が A 方向に引き返す。
- 対策：通常運行において列車は退行してはならない

シナリオ 1-4「② control action が不十分」A から来た列車が C を通過した後、A 方向に引き返す。
- 対策：通常運行において列車は退行してはならない

シナリオ 1-5「② control action が不十分」A から来た列車が C を通過して B をマスクした後、B と C の中間で停止。救援列車が反対方向から侵入してセンサー B を通過。A 方向に進行する。

4.5.1.【実施例】UCA1 に至るハザードシナリオ [IPA2016]

例：Step2出力 注釈付きCLD

コントローラーが人間の場合等に，
「原因の例」を切り替えられると便利．
(SafetyHATは対応している)

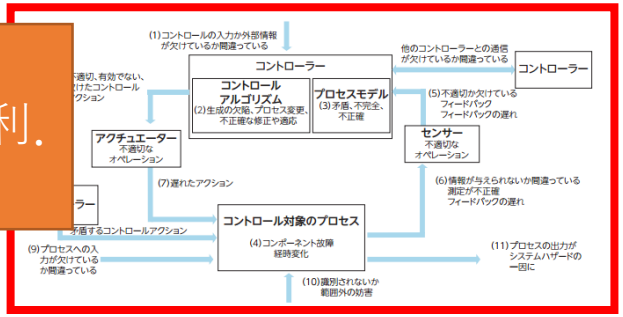
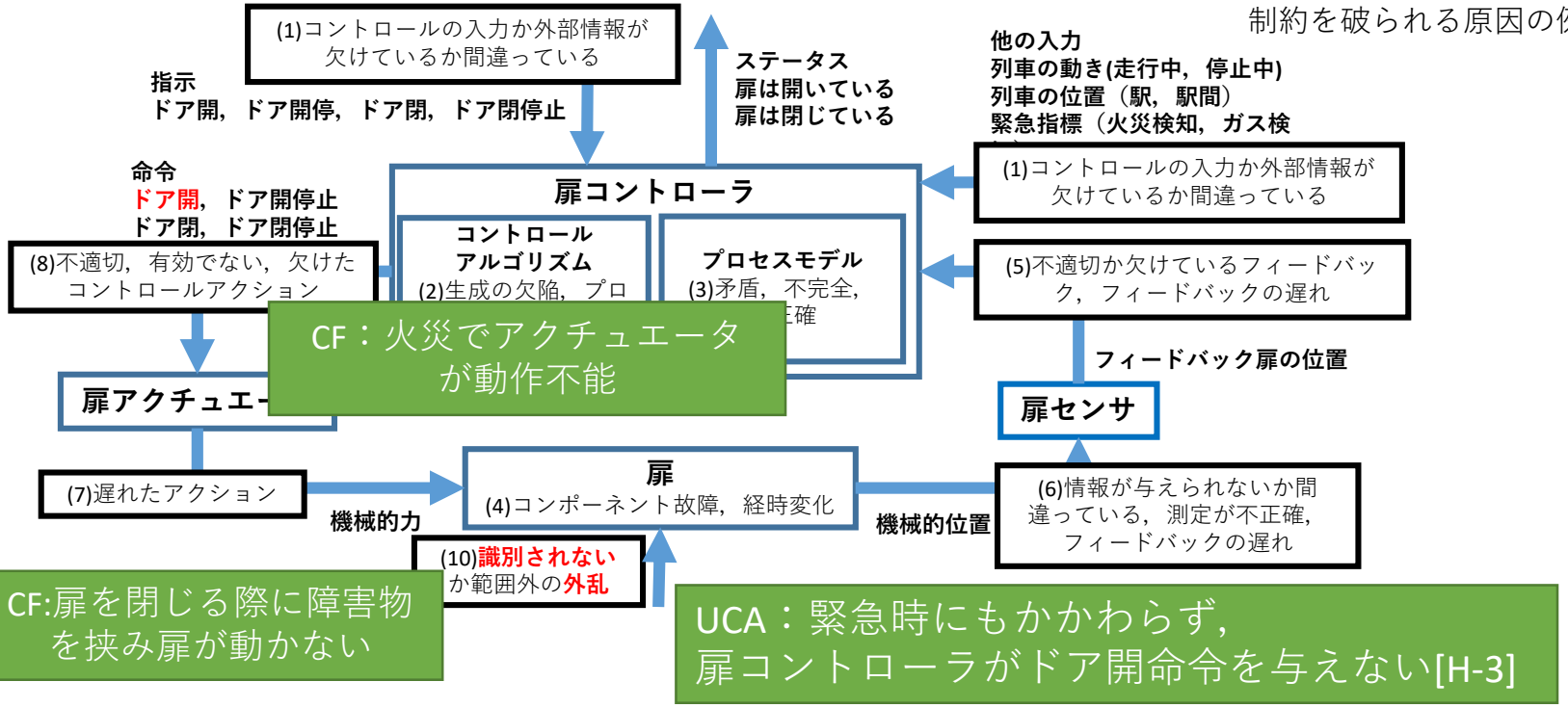


図 2.5-1 コントロールループで安全制約を破られる原因の例 [IPA2016]

シナリオ：扉コントローラはドア開命令を出したが，ドアが開かない．



3.4.1 Identifying how safe control actions may not be followed or executed [Thomas2013]に追記

既存のSTAMP/STPA支援ツール

- XSTAMPP：多彩な拡張機能(モデル検査連携等)
  - http://www.xstampp.de/
- SafetyHAT：DB連携，ガイドワード編集
  - https://www.volpe.dot.gov/infrastructure-systems-and-technology/advanced-vehicle-technology/safetyhat-transportation-system
- an STPA tool：拡張STPAをサポート
  - 文献：Tool assisted Hazard Analysis and Requirement Generation based on STPA
  - 文献：An STPA Tool
- SAHRA： Enterprise Architect拡張
  - http://sahra.ch/
  - 後継ツール：ANSHIN

[Krauss2015] Tool qualification considerations for tools supporting STPA
[MIT] MIT Partnership for a Systems Approach to Safety (PSAS) web pages

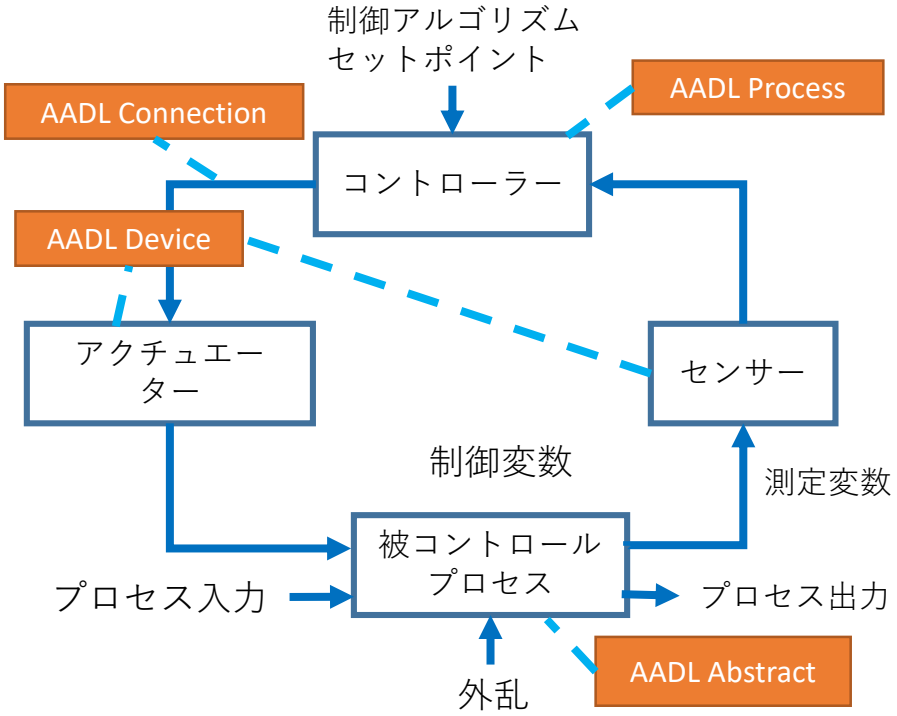
専用ツール以外のツールの活用

- 専用ツール以外のツール(言語・記述法)の検討
- 汎用ツールの利用
  - ドローイング・ツール：
    コントロールストラクチャー図の記述
  - 表計算ツール：ハザード一覧表，UCA表他
- 設計ツール(言語，記法)の流用
  - 設計ツールとの連携は有効
  - 本来の使い方とは異なる使い方こともも
    - 詳細設計のみ⇒機能CSDを記述できない
  - [Procter2014] An Architecturally-Integrated, Systems-Based Hazard Analysis for Medical Applications
    - STPAの結果付きAADLモデルから分析報告書を自動作成

AADLの流用：AADLとは？

- Architecture Analysis and Design Language (AADL)
  - アーキテクチャ分析設計用言語(テキスト形式，図式)
  - コンポーネントベース
  - 主たる記述対象：組込みシステム(HW/SW)
  - コンポーネント：Abstract
    - 3.5 Developing a Conceptual Model [Feiler2012]
- Error Model Annex (EMV2)
  - AADLモデルにエラー情報を付加するための拡張
  - Error type：類型化されたエラーの階層構造
  - Error flows：コンポーネント間(内)のエラー伝搬
  - Error behavior：エラー状態の遷移
  - Properties：ハザードの情報等

AADLによるSTAMP/STPA要素の記述



STAMP/STPA (Step2-1タイプ)	Error Model Annex (エラータイプ)	分析対象固有エラー・タイプ (拡張として定義)
与えられないとハザード	ServiceOmission, …	ServiceOmission等の拡張エラー・タイプとして定義
与えられるとハザード	ServiceComission, …	ServiceComission等の拡張エラー・タイプとして定義
早すぎ、遅すぎ、誤順序でハザード	EarlyDelivery, …	EarlyDelivery等の拡張エラー・タイプとして定義
早すぎる停止、長すぎる適用でハザード	EarlyServiceTermination, …	EarlyServiceTermination等の拡張エラー・タイプとして定義

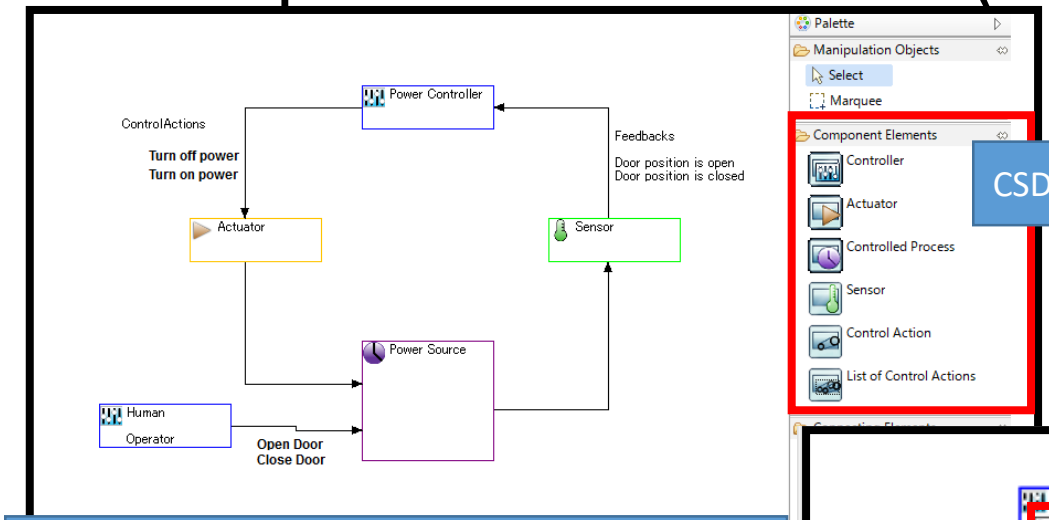
Procter, S. and Hatcliff, J. An Architecturally-Integrated, Systems-Based Hazard Analysis for Medical Applications, Formal Methods and Models for Codesign (MEMOCODE), 2014

XSTAMPP

- eXtensible STAMP Platform
- 以下のプラグインを含む
  - A-STPA：A-STPAのスタンドアロン版の後継
  - A-CAST：CAST用
  - XSTPA：トーマス博士の拡張STPA用
  - STPASec：STPA for Security用
  - STPAPriv：STPA for Privacy用
  - STPA Verifier：モデル検査とSTPAの連携
  - STPA Safety-based Test Cases Generator

- [Abdulkhaleq] XSTAMPP 2.0: New Improvements to XSTAMPP Including CAST Accident Analysis and an Extended Approach to STPA
- http://www.xstampp.de/
- [Abdulkhaleq2015] A comprehensive safety engineering approach for software intensive systems based on STPA

Step0-2出力 CSD (XSTAMPP)

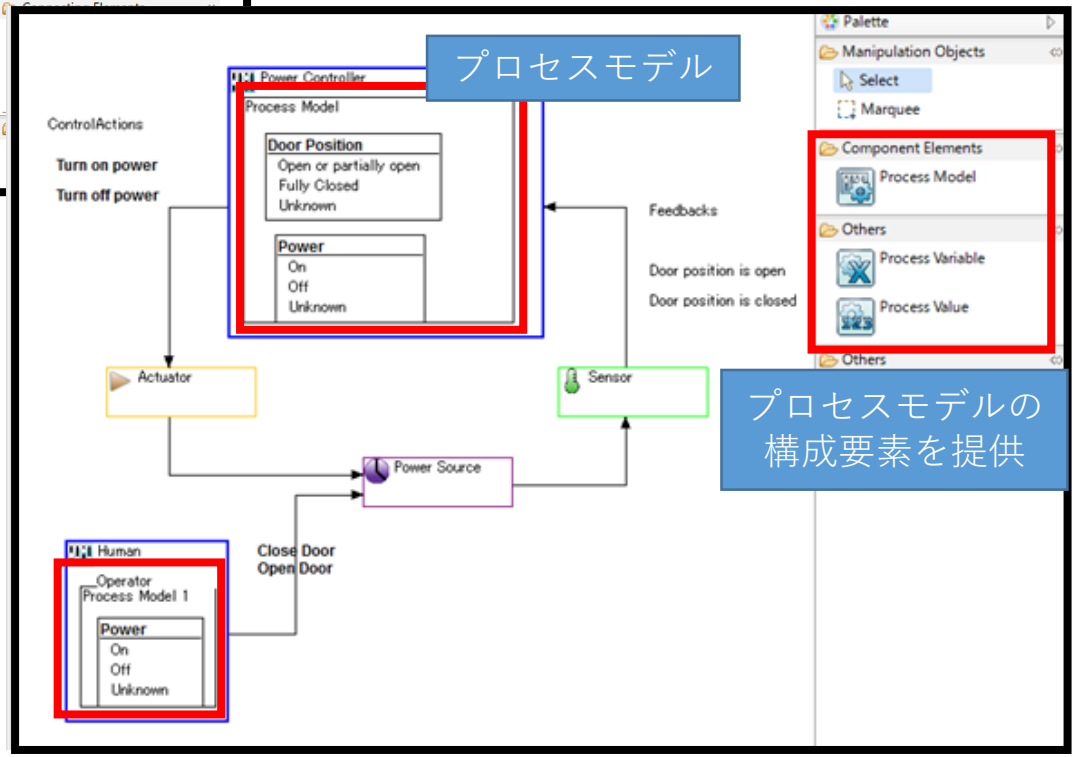


CSDの構成要素を提供

Step0-2のCSD作成でCAを記述すると，
step1のControl Actionsに自動的に追記される

サブコンポーネントのようなものは
記述できない

プロセスモデル

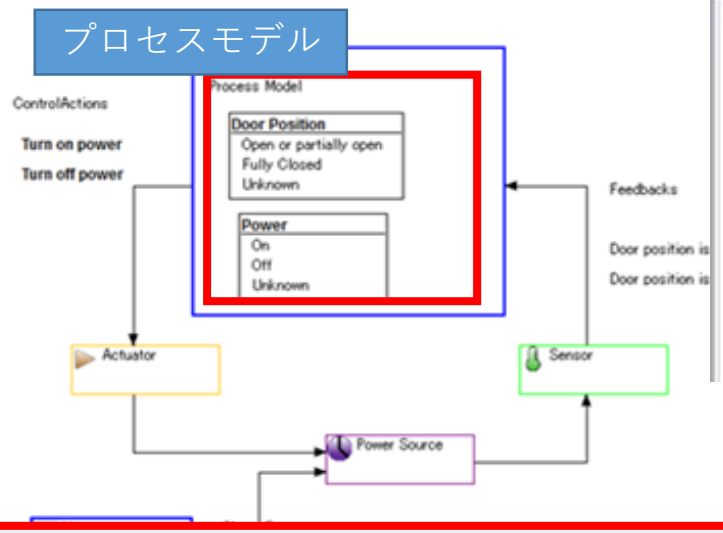


プロセスモデルの
構成要素を提供

拡張Step1 (XSTAMPP)

Context Table

プロセスモデル



Control Action Provided | Control Action Not Provided

Show All

ID	Power	Door Position	Hazardous if provided: Anytime	to Early	to late
1	Off	Open or partially open	☐	☑	☐
2	On	Open or partially open	☑	☐	☐
3	Off	Open or partially open	☑	☐	☐

左の条件下で，ハザードへ至るか？

Filter Categories: control action

Control Action	Not providing causes hazard	Providing incorrect causes hazard	Wrong timing or order causes hazard	Stopped too soon or Applied too long
Turn on power				
		RUCA1.20 The Turn on power command is provided anytime when Power is On and Door Position is Open or partially open [H-1]	RUCA1.19 The Turn on power command is provided too early when Power is Off and Door Position is Open or partially open [H-1]	
		RUCA1.21 The Turn on power command is provided anytime when Power is Off and Door Position is Open or partially open [H-1]		
Turn off power				
	RUCA1.16 The Turn off power command is not provided when Power is On and Door Position is Open or partially open [H-1]		RUCA1.17 The Turn off power command is provided too late when Power is On and Door Position is Open or partially open [H-1]	

条件＝(プロセス変数,プロセス値)の組

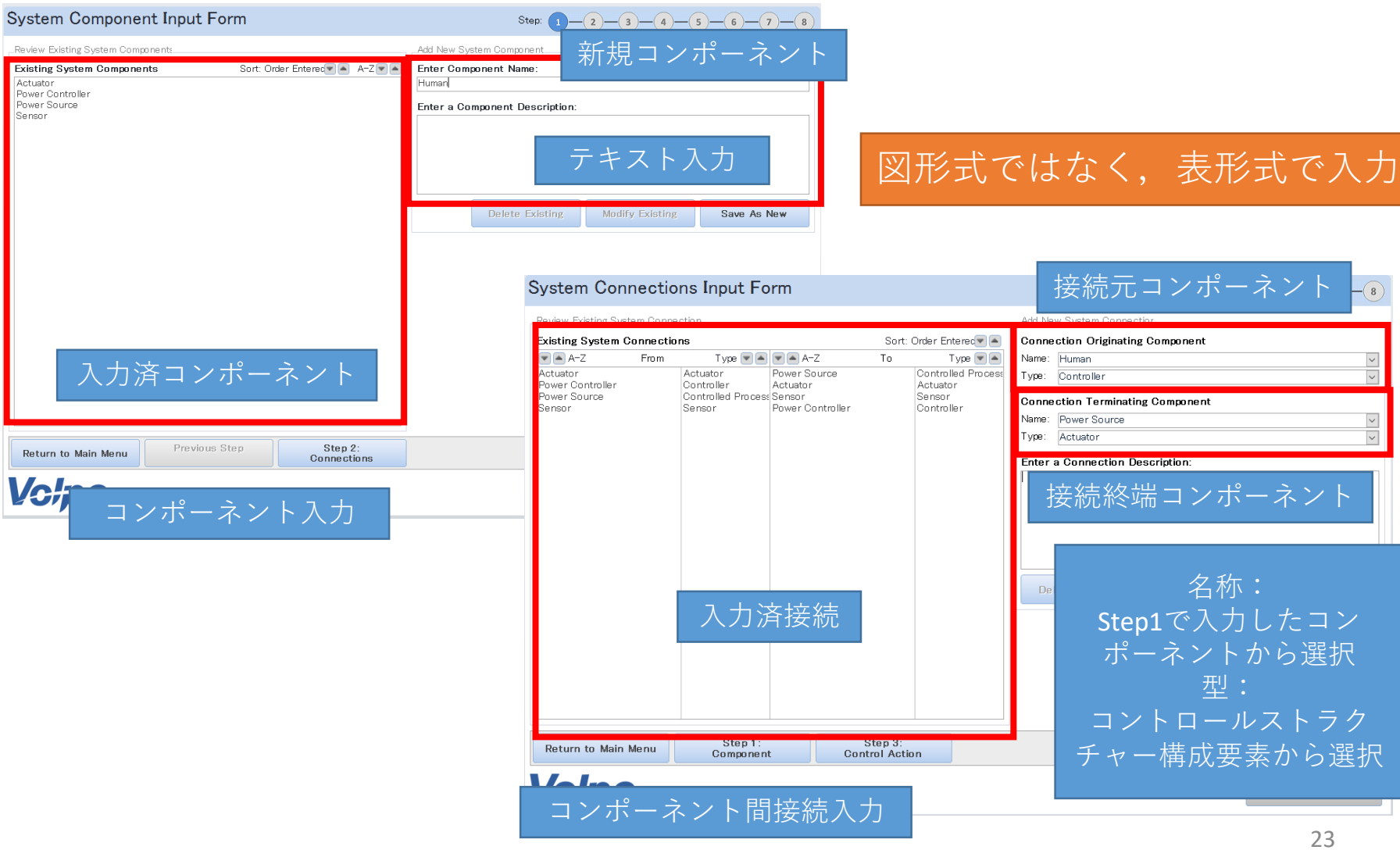
Refined Unsafe Control Actions

SafetyHAT

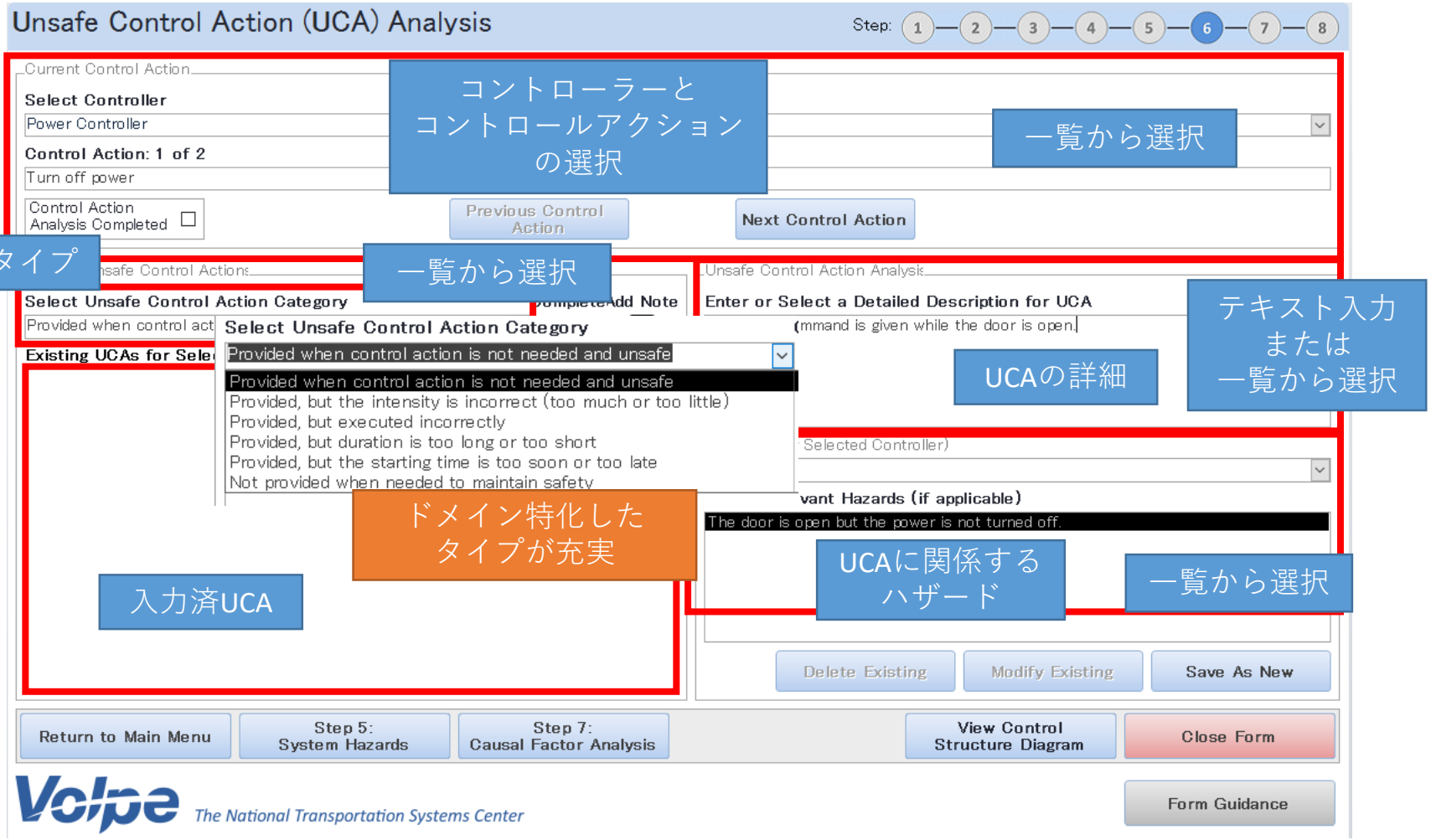
- A Transportation System Safety Hazard Analysis Tool
- データベース(Microsoft Access)と連携
- エクセル形式で分析結果を出力可能
- トランスポーテーションシステムに特化したタイプ(step1)とcausal factorのヒント(step2)を提供
- コンポーネントタイプやガイドワードをカスタマイズ可能
- 図形式でCSDが記述できない(図とのリンク可能)

- https://www.volpe.dot.gov/infrastructure-systems-and-technology/advanced-vehicle-technology/safetyhat-transportation-system
- [Hommes2014] The Volpe STPA Tool, 2014 STAMP Workshop

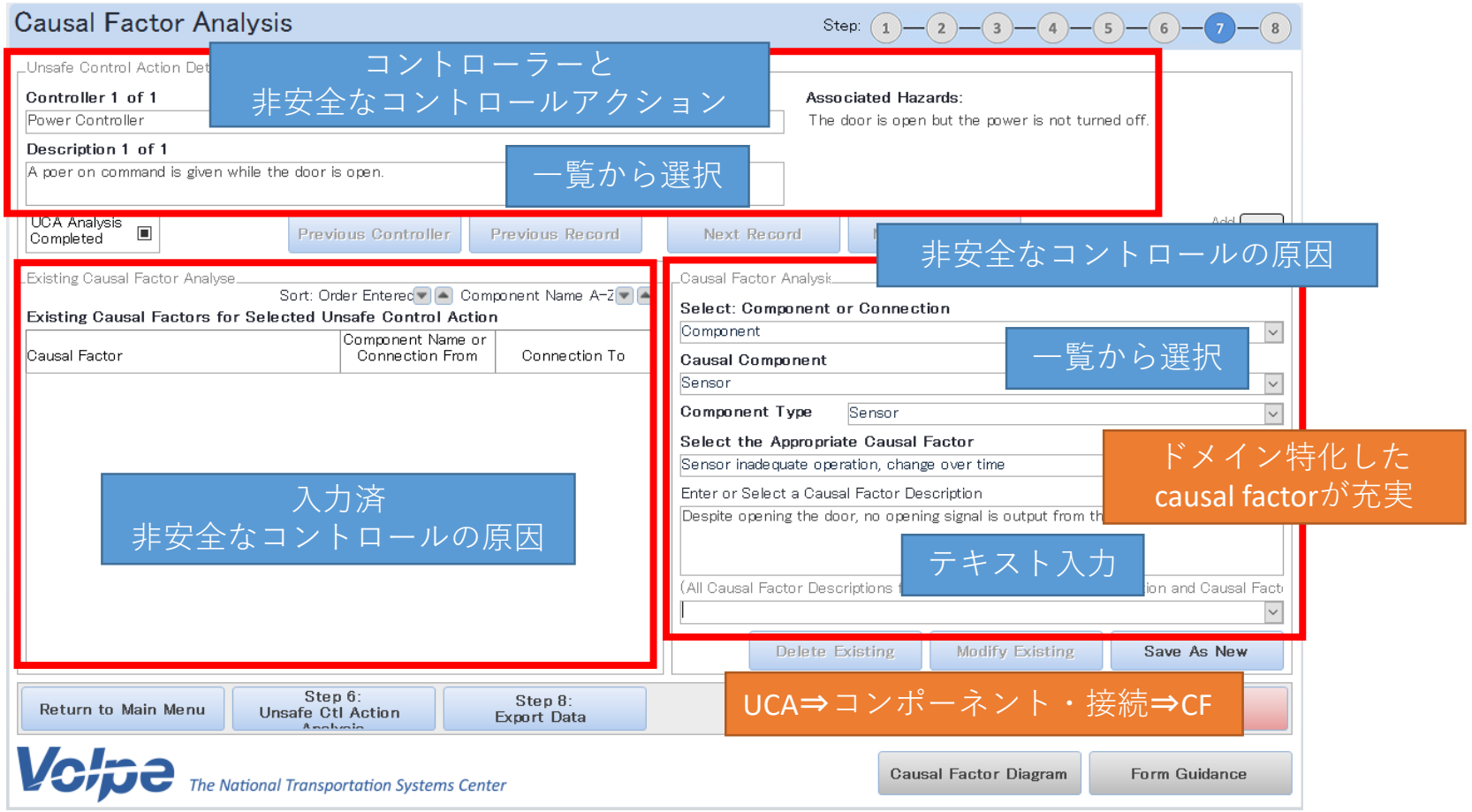
Step0-2 ：CSDの構築(SafetyHAT)



Step1：UCAの抽出 (SafetyHAT)



Step2：誘発要因の特定(SafetyHAT)



まとめ

- STAMP/STPAの概説
  - プロセス，出力形式，課題
- STAMP/STPA支援ツール紹介
  - 専用ツール以外のツールの流用
  - XSTAMPP，SafetyHAT

	XSTAMPP	SafetyHAT	i-STAMP(仮)
Step0準備1：出力	リスト(関連付け有)	リスト(関連付け有)	リスト(関連付け有)
Step0準備2：CSD	図	リスト(図関連付け可)	図
Step1：出力	UCA表	UCA表	UCA表
Step2：出力	CF表	CF表	CF表
その他	トーマス博士の拡張 Step1に対応(XSTPA) モデル検査連携 CAST,STPA-sec他対応	コンポーネントタイプ，ガイドワードの追加定義可能 データベース連携	Step2ガイドワード拡張に対応 ???