IPA Better Life with IT

IoT時代の安全分析手法STAMP/STPA

～STAMP支援ツールSTAMP Workbench～

IPA 社会基盤センター

調査役　石井 正悟

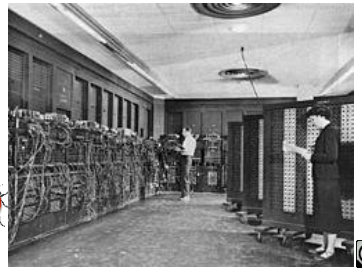
1. STAMPとは
2. STPAとは
3. STAMP/STPAガイドブック
4. STAMP支援ツール“STAMP Workbench”

新たな手法へのパラダイムシフト

IPA

従来の手法
FMEA, FTA, HAZOPなど

アクシデントは構成機器の故障や
オペレーションミスに起因すると仮定

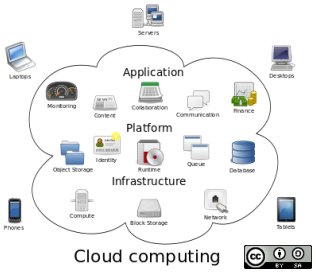


旧来は
ハードウェア主体

パラダイムシフト

新たな手法
STAMPに基づく分析

アクシデントは構成要素間の
相互作用から創発的に発生



1940 • FMEA → 1950 → 1960 • FTA • HAZOP • ETA → 1970 • Bow Tie (CCA) FTA+ETA → 1980 → 1990 → 2000 → 2010 • STAMP → 2020

既存のハザード分析手法
は40～65年前のもの

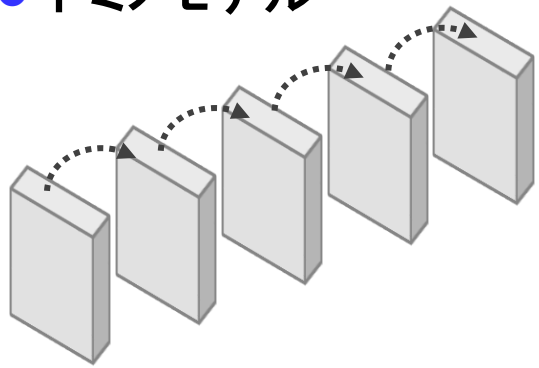
大規模・複雑化が進むIoT時代の
コンピューターシステムへの対応が求められる

現在の分析手法が確立されたのは40-65年前
コンピューターシステムはハードウェア主体からIoT時代へ

従来の事故モデル

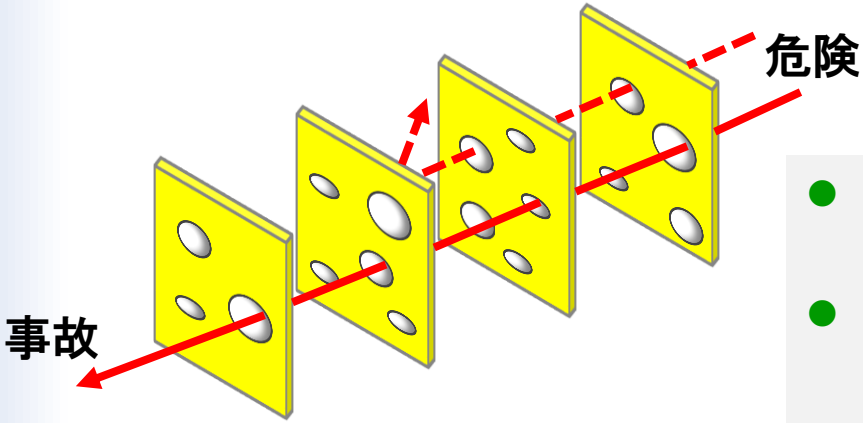
IPA

- 従来の事故モデル ・・・ 根本原因の影響が伝搬するイベントチェーンの形式
  - ドミノモデル



- 一つの根本原因が事故につながる
- 原因ー結果(次の原因)ー …の系列をドミノ倒しにたとえる
  このドミノ倒しのどこかで手を打てば事故が避けられるとする
- 根本原因分析といわれる事故分析の各手法は、この考えに立っている

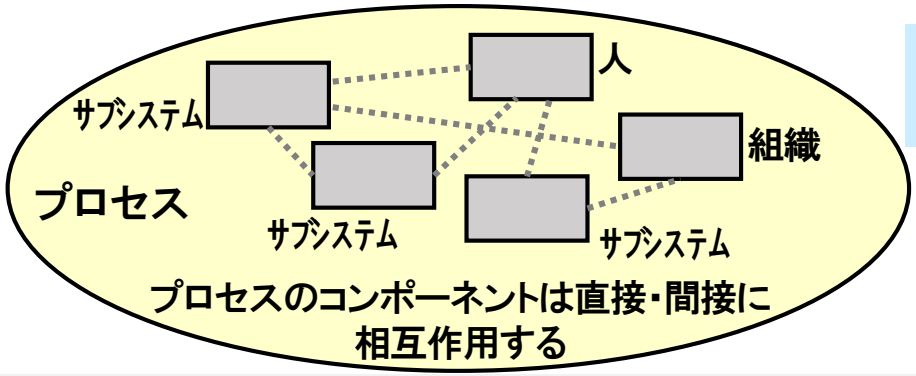
  - スイスチーズモデル



- いくつかのコンポーネントの不備が組合さると事故につながる
- 防御壁とそこでの漏れをチーズの穴にたとえる
  穴が重なって見通せたときに事故となる
- 個々の穴をふさぐことで対策とする

STAMP・・・新しい事故モデル

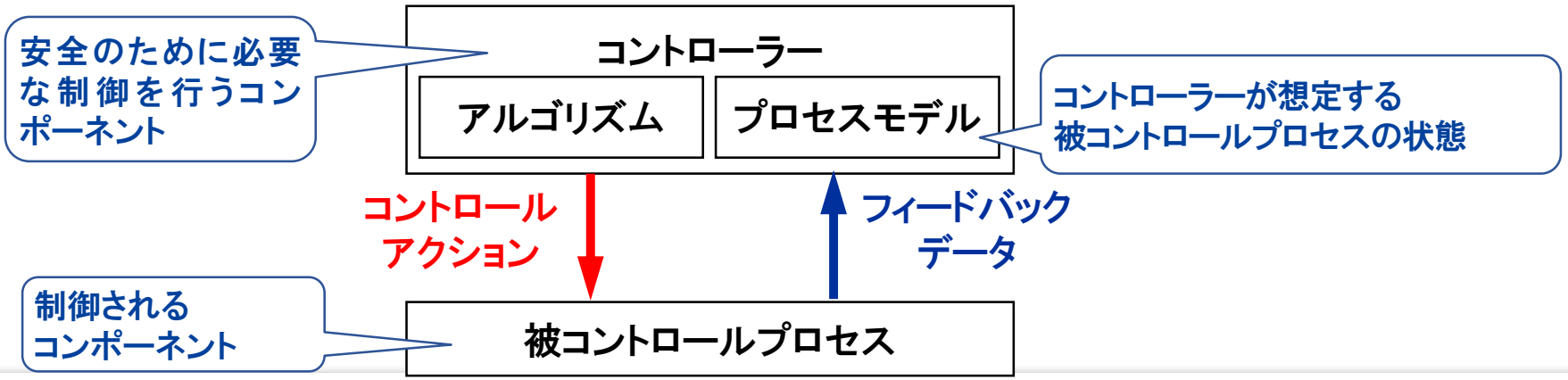
- Systems-Theoretic Accident Model and Processes
  「システム理論に基づく事故モデル」MITのＮａｎｃｙ Ｌｅｖｅｓｏｎ教授が提唱



複雑な相互作用に
起因する創発特性
→ 安全制約の乱れ
→ 事故につながる

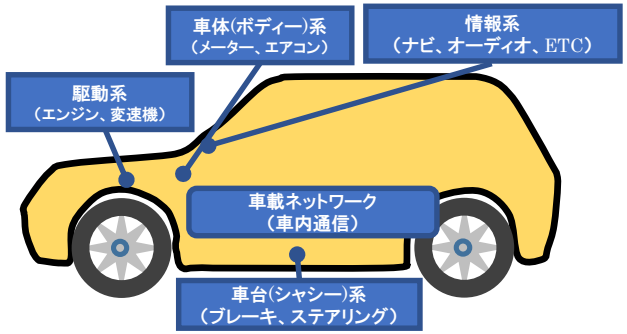
- はじめから根本原因に着目するのではなく、まず相互作用に着目する。
- 網羅的に相互作用に着目し、それぞれの相互作用が非安全になるタイプを網羅的に抽出する。

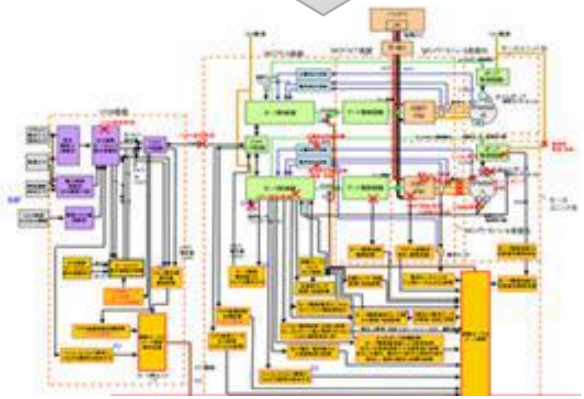
STAMPモデルの基本要素



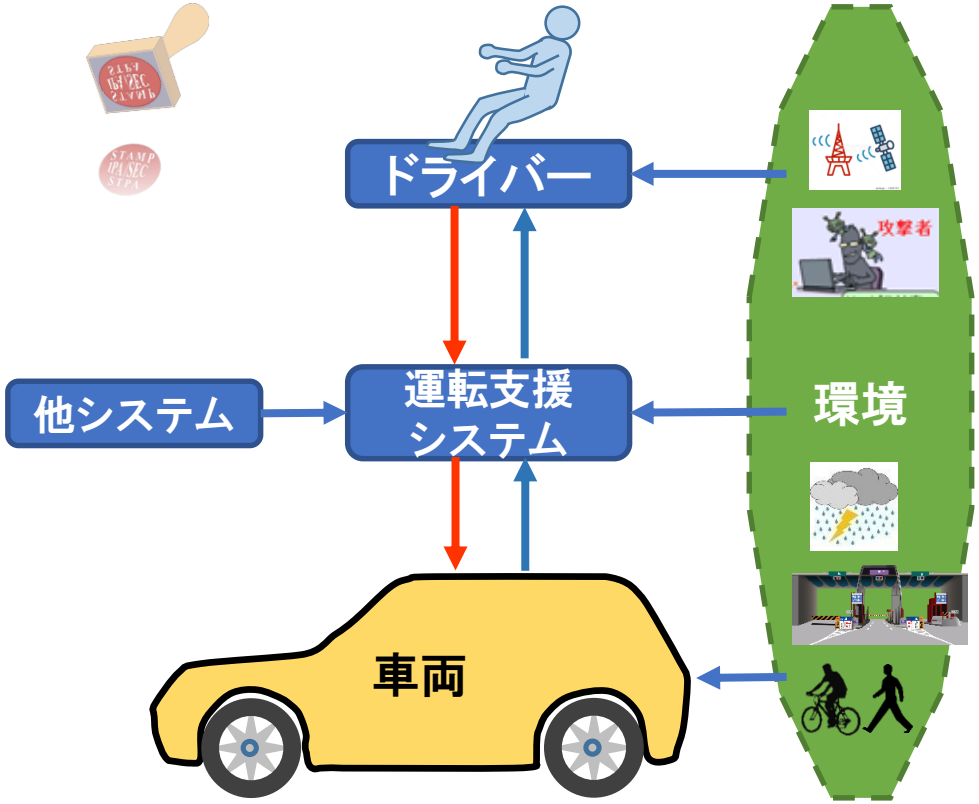
既存の考え方とSTAMPの考え方の違い ～システム理論に基づく新しい安全分析～

自動車システムを大規模な機能ブロック図等で表現し、システム中心視点の安全分析を行う





運転自動化が進むと更に大規模、複雑になり、人や環境、またそれらとの相互作用にも着目した安全分析が必要になる



STAMPのSTはSystems-Theoretic(システム理論に基づく)の略で、分析対象システムの安全に関係するすべてを含めて考えるべきと提唱しており、今後の複雑なシステムの安全分析に適している

1. STAMPとは
2. STPAとは
3. STAMP/STPAガイドブック
4. STAMP支援ツール“STAMP Workbench”

STPA・・・STAMPに基づくハザード分析手法

- Systems-Theoretic Process Analysis
  - 安全制約が破られうるシナリオを定義する支援に使用する
  - 許容リスクを確実にするのに必要な安全制約/要求を特定する
    （従来の解析と同じ）
  - 従来の解析手法にくらべ、
    - コンポーネント故障以上の要因にも着目する
    - より多くの事故シナリオを発見できる

手法名	分析方法	特 徴
従来手法（FTA，FMEA）	フォールトツリー図や影響分析表を用いて、トップダウンまたはボトムアップでハザード要因を分析	システムの構成要素と故障モードが決まるアーキテクチャ設計の段階から適用
STAMP/STPA	コントロールストラクチャーとコントロールループ図を用いてハザード要因を分析	システムの大まかな構成要素が決まる概念設計の段階から適用

STPAの概略手順

分析手順

Step 0(準備1):
アクシデント(望ましくない事象)、ハザード(アクシデントに至る状態)、安全制約の識別

↓

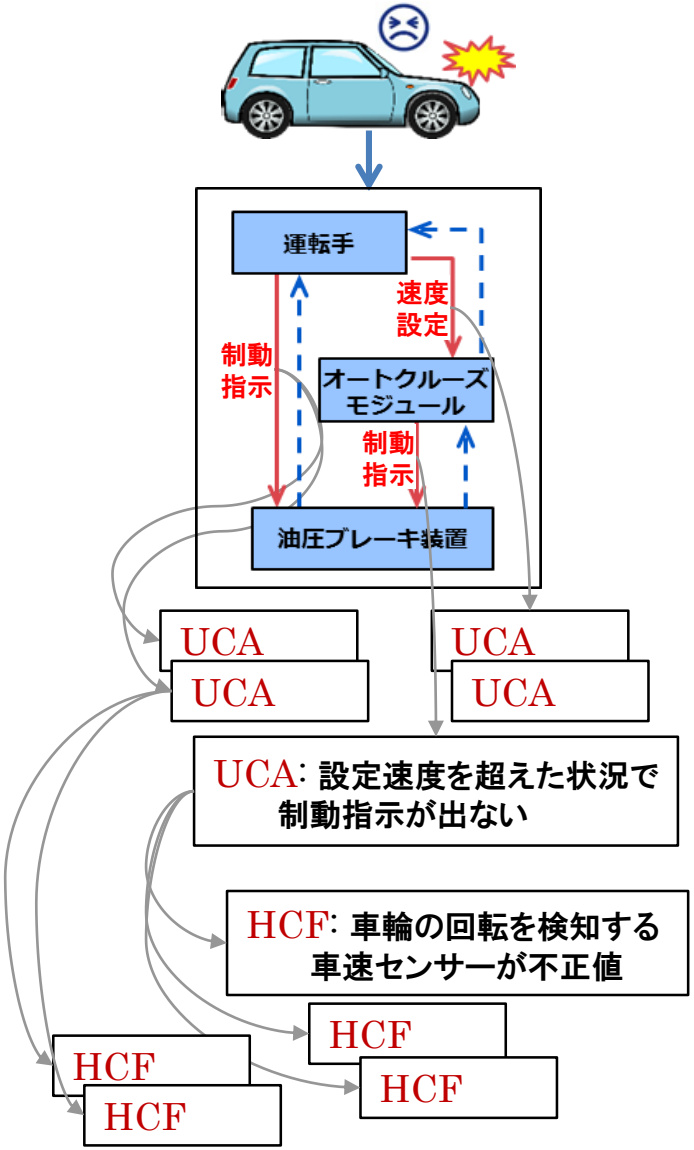
Step 0(準備2):
コンポーネントと相互作用から成るコントロールストラクチャーの構築

↓

Step 1:
非安全なコントロールアクション(UCA: Unsafe Control Action)の抽出

↓

Step 2:
UCA毎のコントロールループにガイドワード適用 → ハザード誘発要因(HCF: Hazard Causal Factor)の特定



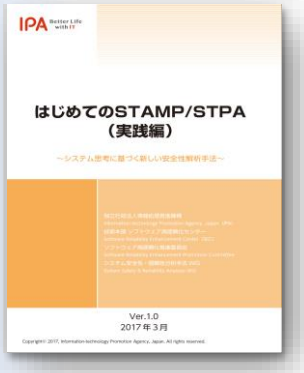
1. STAMPとは
2. STPAとは
3. STAMP/STPAガイドブック
4. STAMP支援ツール“STAMP Workbench”

STAMP/STPAガイドブック

「はじめてのSTAMP/STPA」入門編

- STAMPを**理解する**ためのSTPA手順解説書
- 教科書に近い分かり易い事例を用い、勘所を交えてSTPAの手順を具体的に解説

http://www.ipa.go.jp/sec/reports/20160428.html



「はじめてのSTAMP/STPA（実践編）」

- STAMPを**やってみる（実践）**ためのSTPA事例解説書
- **教科書通りにはいかない産業界の事例を用い、STPAの効果的な活用方法を具体的に解説**

http://www.ipa.go.jp/sec/reports/20170324.html

New！

「はじめてのSTAMP/STPA（活用編）」

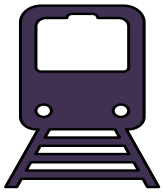
- STAMPを**当たり前にやる（活用定着）**ためのSTPA事例解説書
- 産業界での試行事例、人と機械の協調による安全制御の事例、セーフティとセキュリティの統合分析事例を解説
- 将来の複雑システムの安全解析の在り方に関するビジョンを提言

http://www.ipa.go.jp/sec/reports/20180328_2.html

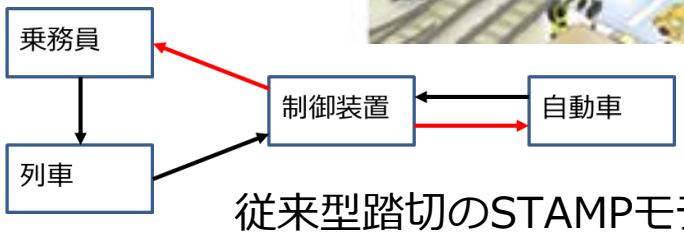
はじめてのSTAMP/STPA（活用編）

- 産業界においてSTAMP/STPAを役立てる際に参考となる**先進的な事例**
- 4分野の具体例で、**人と機械の協調による安全制御**の分析や安全とセキュリティーの統合分析などへの適用例を解説

鉄道



2つのタイプの踏切システムの安全性の違いをSTAMPで評価

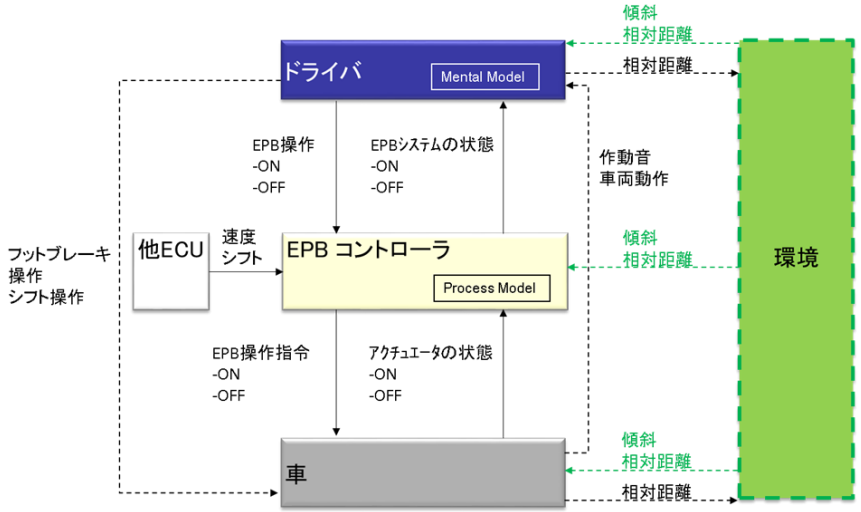


従来型踏切のSTAMPモデル

クローズドループ型踏切のSTAMPモデル

自動車

ISO 26262における安全分析へSTAMPを適用するための工夫を具体的事例で解説

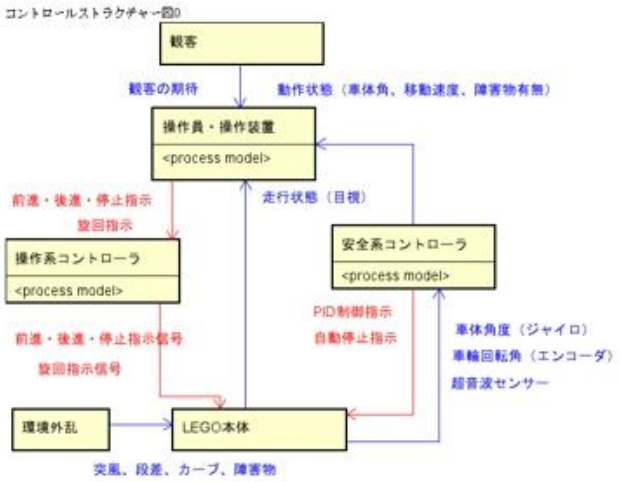


電動パーキングブレーキのSTAMPモデル

はじめてのSTAMP/STPA（活用編）

ロボット

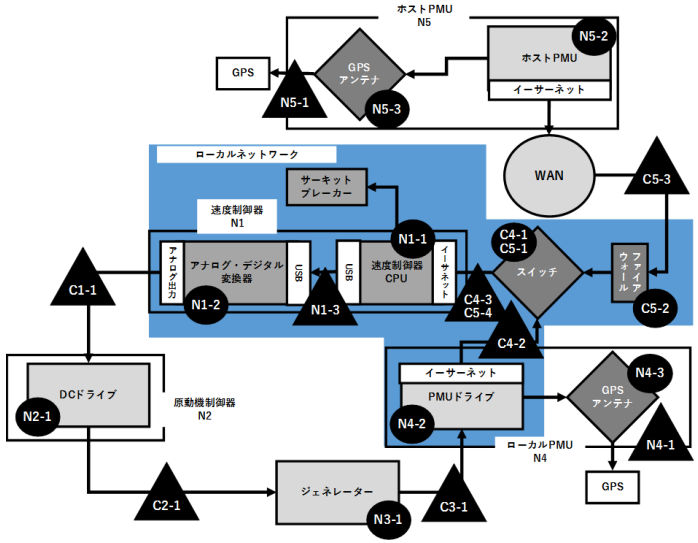
二輪倒立ロボットに対する人と
機械の協調制御のSTAMP分析事例



人と機械の協調制御を表すSTAMPモデル

電力網

マイクログリッドのセキュリティ
リスク分析へのSTAMP応用事例



セキュリティリスク分析に用いる
STAMPモデル

1. STAMPとは
2. STPAとは
3. STAMP/STPAガイドブック
4. **STAMP支援ツール“STAMP Workbench”**

NIPPON発
STAMPツール
2018.03公開

STAMP Workbench

https://www.ipa.go.jp/sec/tools/stamp_workbench.html

STAMP普及の課題と対策

IPA

【ガイドブックだけでは解決できない課題】

- STAMP/STPAは自由な発想を引き出す強制発想手法！
  なのに**思考に専念**できない
  - 図表の作成・編集に手間がかかる
  - 修正に伴う影響範囲の更新に手間がかかる
- ツール活用が有効！
  しかし、**分析を支援**するツールがない
  - 既存ツールはSTAMP研究者向けの清書ツール、お絵描きツール

【対策】

- IPAがSTAMP支援ツールを開発し、無償で公開
  - 公的機関がSTAMP支援ツールの協調領域機能を無償で提供し、STAMP適用のすそ野を広げる
  - オープンソースとしてソースコードを公開し、先行企業による適用最適化を推進

STAMP Workbenchの基本コンセプト

- STPA手順を誘導し、分析者は思考に専念できる
  - 可能な限り自動化
- 自由な発想を引き出し、積極的に繰り返し分析を支援
  - リアルタイムモデル連携により、分析者を図表修正の煩わしさから解放
- 分析結果の妥当性を説明するためのエビデンス作成を支援
  - CS図生成過程の情報を記録（図から表、表から図の双方向を支援）
    - 要求仕様を整理する表（コンポーネント抽出表）からCS図の雛型を自動生成 （表 ➡ 図）
    - CS図を編集すると、編集内容がコンポーネント抽出表に自動的かつリアルタイムに更新される （図 ➡ 表）

STAMP Workbench

- ツールがSTAMP/STPAの**手順を誘導**
- 要求仕様を整理するコンポーネント抽出表から、CS図の雛型を**自動生成**
- 人は**考えることだけに専念**できる

自然言語の要求仕様書 ⟹ 表形式で整理

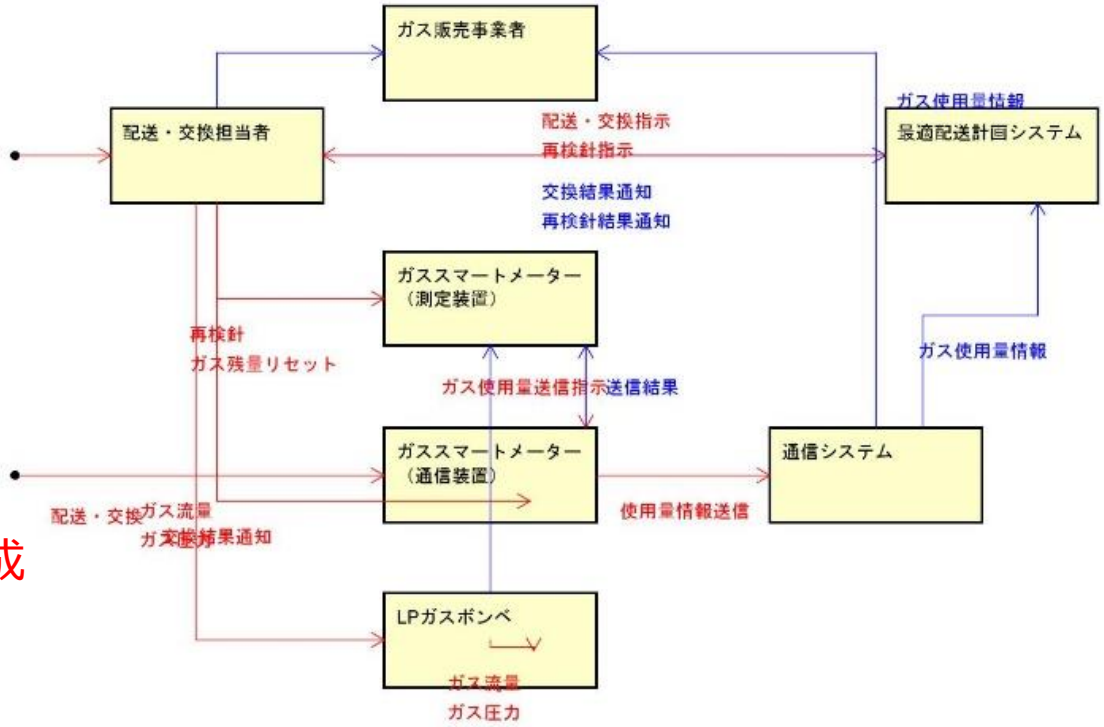
対象	登場人物	責務	コントロールア…	フィードバック	入出力	備考
☑	ガススマートメーター（測定装置）	ガス流量を測定し、流量累積情報を保持する（使用量情報の取得・保持）	ガス使用量送信指示 (To: ガススマートメーター（通信装置）)			ガス流量累積値とガス残量推定値はプロセスモデル
☑	ガススマートメーター（通信装置）	ガス使用量情報を通知する	使用量情報送信 (To: 通信システム)	送信結果 (To: ガススマートメーター（測定装置）)	(入力)ガス流量 (入力)ガス圧力	
☑	最適配送計画システム	最適配送計画を策定し、配送・交換を指示する	配送・交換指示 (To: 配送・交換担当者) 再検討指示 (To: 配送・交換担当者)			
☑	配送・交換担当者	配送・交換指示を受け、利用者の家庭にLPガスボンベを配送し、交換する	配送・交換 (To: LPガスボンベ) 再検討 (To: ガススマートメーター（測定装置）) ガス残量リセット (To: ガススマートメーター（測定装置）)	交換結果通知 (To: 最適配送計画システム) 再検討結果通知 (To: 最適配送計画システム)	(出力)交換結果通知	
☑	LPガスボンベ	LPガスを漏らさないように保持する ボンベのガスコックが開いたらLPガスを出す			(出力)ガス流量 (出力)ガス圧力	仕様書には書かれていない
☑	ガス販売事業者	ガス使用量に応じて課金する				
☑	通信システム	スマートメーターから受信したデータをガス販売事業者と最適配送計画システムに通知する		ガス使用量情報 (To: 最適配送計画システム) ガス使用量情報 (To: ガス販売事業者)		

STAMP Workbench

- ツールがSTAMP/STPAの手順を誘導
- 要求仕様を整理するコンポーネント抽出表から、CS図の雛型を自動生成
- 人は考えることだけに専念できる

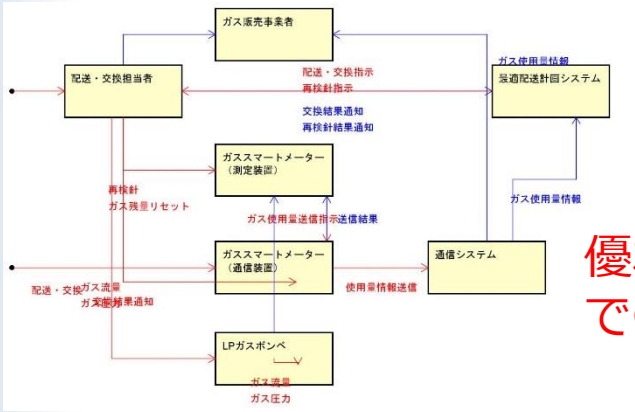
対象	登場人物	責務	コントロールア…	フィードバック	入出力	備考
☑	ガススマートメーター（測定装置）	ガス流量を測定し、流量関連情報を保持する（使用量情報の取得・保持）	ガス使用量送信指示 (To: ガススマートメーター（通信装置）)			ガス流量関連とガス残量推定値はプロセスモデル
☑	ガススマートメーター（通信装置）	ガス使用量情報を通知する	使用量情報送信 (To: 通信システム)	送信結果 (To: ガススマートメーター（測定装置）)	(入力)ガス流量 (入力)ガス圧力	
☑	最適配送計画システム	最適配送計画を策定し、配送・交換を指示する	配送・交換指示 (To: 配送・交換担当者) 再検針指示 (To: 配送・交換担当者)			
☑	配送・交換担当者	配送・交換指示を受け、利用者の家庭にLPガスボンベを配送し、交換する	配送・交換 (To: LPガスボンベ) 再検針 (To: ガススマートメーター（測定装置）) ガス残量リセット (To: ガススマートメーター（測定装置）)	交換結果通知 (To: 最適配送計画システム) 再検針結果通知 (To: 最適配送計画システム)	(出力)交換結果通知	
☑	LPガスボンベ	LPガスを漏らさないように保持する ボンベのガスコックが開いたらLPガスを出す			(出力)ガス流量 (出力)ガス圧力	仕様書には書かれていない
☑	ガス販売事業者	ガス使用量に応じて課金する				
☑	通信システム	スマートメーターから受信したデータをガス販売事業者と最適配送計画システムに通知する		ガス使用量情報 (To: 最適配送計画システム) ガス使用量情報 (To: ガス販売事業者)		

CS図の雛型を自動生成

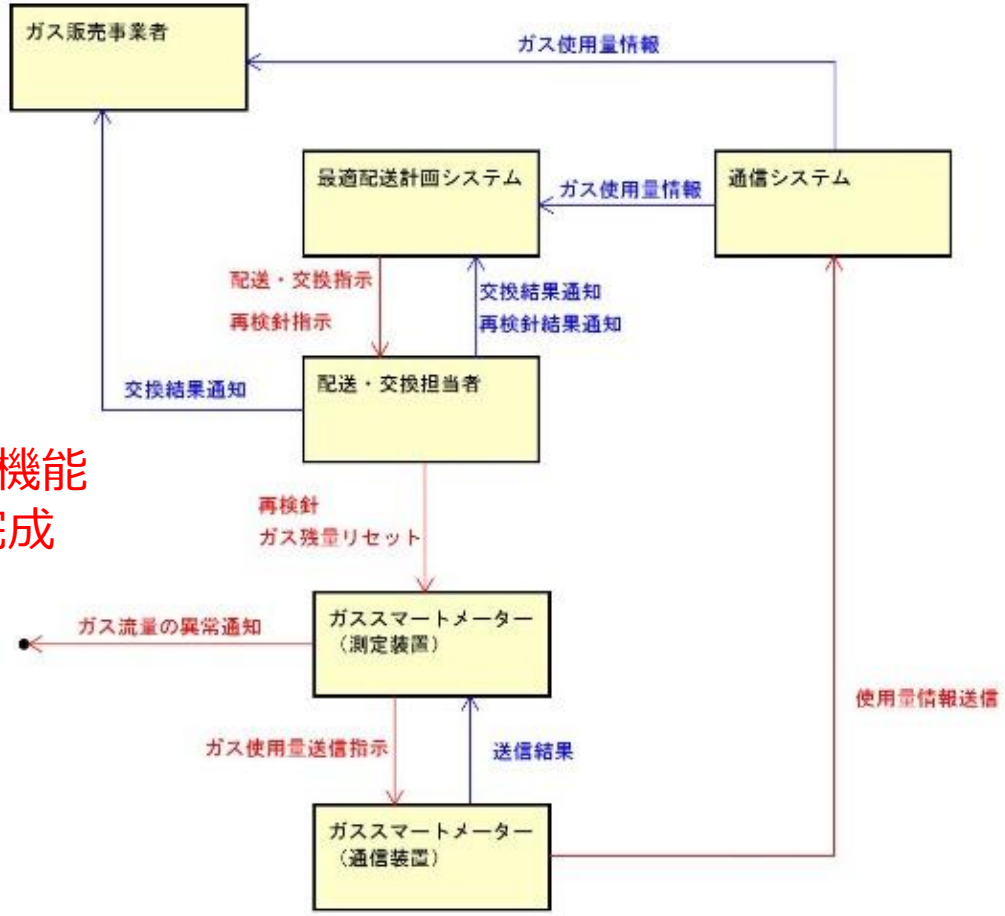


STAMP Workbench

- ツールがSTAMP/STPAの手順を誘導
- 要求仕様を整理するコンポーネント抽出表から、CS図の雛型を自動生成
- 人は考えることだけに専念できる

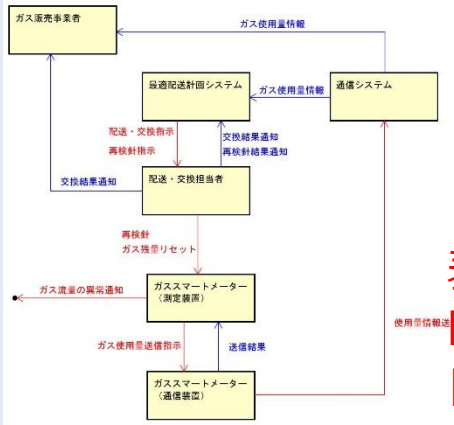


優れた編集機能
でCS図を完成

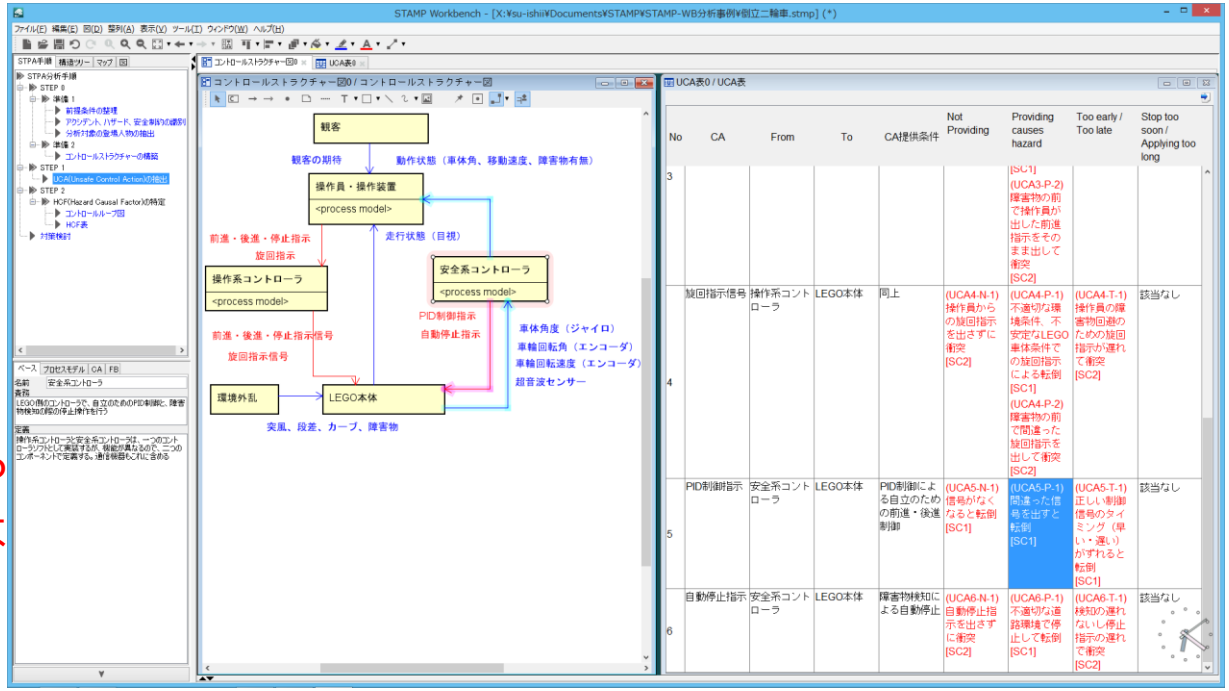


STAMP Workbench

- ツールがSTAMP/STPAの手順を誘導
- 要求仕様を整理するコンポーネント抽出表から、CS図の雛型を自動生成
- 人は考えることだけに専念できる



表作成やID採番は自動化



変更は全ての図表にリアルタイムに自動反映
IDの振り直しもリアルタイムに自動実行

STAMP Workbench

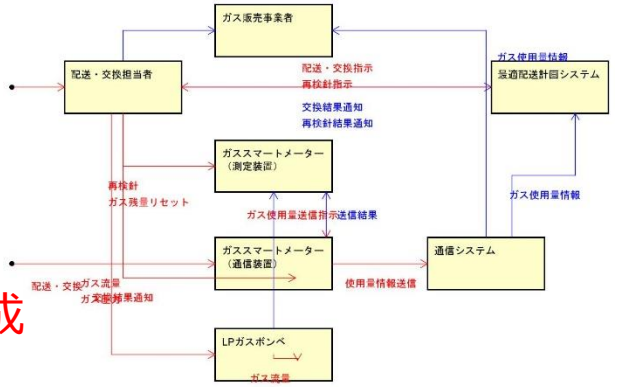
- ツールがSTAMP/STPAの手順を誘導
- 要求仕様を整理するコンポーネント抽出表から、CS図の雛型を自動生成
- 人は考えることだけに専念できる

自然言語の要求仕様書

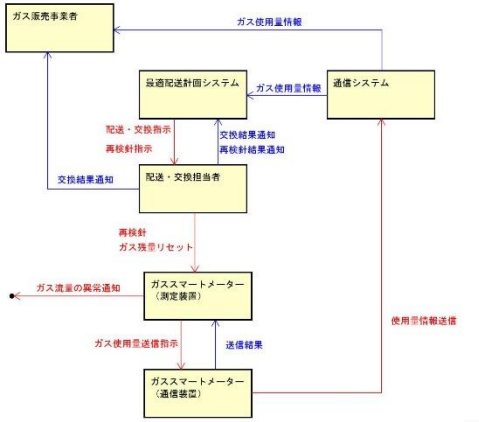
表形式で整理

対象	登場人物	責務	コントロールア…	フィードバック	入出力	備考
☑	ガススマートメーター（測定装置）	ガス流量を測定し、流量履歴情報を保持する（使用量情報の取得・保持）	ガス使用量送信指示 (To: ガススマートメーター（通信装置）)			ガス流量履歴とガス残量推定値はプロセスモデル
☑	ガススマートメーター（通信装置）	ガス使用量情報を通知する	使用量情報送信 (To: 通信システム)	送信結果 (To: ガススマートメーター（測定装置）)	(入力)ガス流量 (入力)ガス圧力	
☑	最適配送計画システム	最適配送計画を策定し、配送・交換を指示する	配送・交換指示 (To: 配送・交換担当者) 再検針指示 (To: 配送・交換担当者)			
☑	配送・交換担当者	配送・交換指示を受け、利用者の家庭にLPガスボンベを配送し、交換する	配送・交換 (To: LPガスボンベ) 再検針 (To: ガススマートメーター（測定装置）) ガス残量リセット (To: ガススマートメーター（測定装置）)	交換結果通知 (To: 最適配送計画システム) 再検針結果通知 (To: 最適配送計画システム)	(出力)交換結果通知	
☑	LPガスボンベ	LPガスを漏らさないように保持する ボンベへのガスコックが閉いたらLPガスを封じ			(出力)ガス流量 (出力)ガス圧力	仕様書には書かれていない
☑	ガス販売事業者	ガス使用量に応じて課金する				
☑	通信システム	スマートメーターから受信したデータをガス販売事業者と最適配送計画システムに通知する		ガス使用量情報 (To: 最適配送計画システム) ガス使用量情報 (To: ガス販売事業者)		

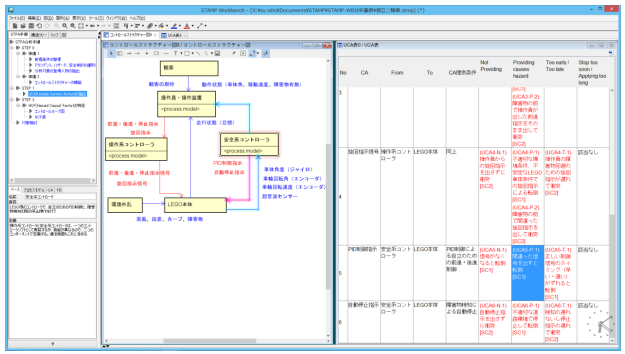
雛型を自動生成



優れた編集機能でCS図を完成



変更は全ての図表にリアルタイムに自動反映
IDの振り直しもリアルタイムに自動実行



表作成やID採番は自動化

ご静聴有難うございました

IPAブースにてSTAMP Workbenchを
実演しています

STAMP Workbenchブースプレゼン予定

STAMP支援ツールSTAMP Workbench について、開発者が詳しくご紹介します。

7月5日(木)	14:30-14:50	**STAMP Workbenchではじめる安全分析**
7月6日(金)	13:30-13:50	**STAMP Workbenchではじめる安全分析**

「ITSS+（プラス）」のお知らせ

第４次産業革命に向けた

スキル変革の羅針盤　ITSS+

ITSS＋

- IoTソリューション領域
- アジャイル領域
- データサイエンス領域
- セキュリティ領域

学び直し　スキル強化

- ITスキル標準（ITSS）
- 情報システムユーザースキル標準（UISS）

詳しくはこちら！

ITSS+

http://www.ipa.go.jp/jinzai/itss/itssplus.html

ご清聴ありがとうございました。