これからの組込みソフトウェア産業に求められること -IoT進展に伴う課題-

IPA/JEITA 共催セミナー

データが語るIoT時代を生き抜く組込みソフトウェア開発 in 仙台

2018年9月28日

仙台高等専門学校，IPA・IoTシステム安全性向上技術WG 委員

岡本圭史

概要

IoTの進展に伴いさまざまなものがつながるようになり，変革がもたらされる一方で，多くの課題が顕在化してきている．本講演では，IoTの進展に伴い，これからの組込みソフトウェア産業が直面する課題について述べる．特に，つながるシステムのハザード分析手法を紹介する．

目次

- はじめに
- 自己紹介・WG紹介
- IoTの動向・予想
- IoTの活用事例
- IoTの課題
- STAMP/STPA
  つながるシステムのためのハザード分析手法

自己紹介


文献の詳細情報

文献 J-GLOBAL ID：201802285925702032 整理番号：18A0602830

複雑システムの安全分析法STAMP 安全性モデリングとSTAMP/STPA,その最新ツール紹介

著者：岡本圭史 (仙台高専)、岡本圭史 (情報処理推進機構)、平鍋健児 (チェンジビジョン)
資料名：SEC Journal 巻：13 号：4 ページ：23-29
発行年：2018年03月01日

クリップする ツイート いいね！ ＋ ブックマーク・共有する 印刷・メールする

- 岡本 圭史
- 所属：仙台高等専門学校
- 委員：IPA・IoTシステム安全性向上技術WG
- 研究分野
  - 安全分析（STAMPの普及）
    - STAMP海外事例の紹介：STPA-SafeSec, 岡本圭史, 岡野浩三, 2018年3月, SEC journal Vol.13 No.4 pp.42-47
    - 安全性モデリングとSTAMP/STPA、その最新ツール紹介, 岡本圭史, 平鍋健児, 2018年3月, SEC journal Vol.13 No.4 pp.23-29
  - 形式手法（数理論理学・数理議論学）
    - A Bayesian Approach to Argument-Based Reasoning for Attack Estimation, Hiroyuki Kido and Keishi Okamoto, 2017年8月, Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence, IJCAI-17, pp.249—255

IoTシステム安全性向上技術WG

- 情報処理推進機構・社会基盤センターのWG
- 活動内容
  - 背景：構成要素の高機能化＋構成要素の接続・連携
  - 目的：安全性・信頼性・セキュリティ向上手法の調査・研究・普及
  - 「事後V&V」フレームワークの提案・普及
    - 複合要因に起因する障害原因を迅速かつ的確に診断
    - モデルに基づいた体系的な手法
  - STAMP/STPAの普及
    - 構成要素の相互接続に着目するハザード分析手法
    - STAMP：システム理論に基づく事故モデル
    - STPA：安全性解析手法
- https://www.ipa.go.jp/sec/about/committee.html#007

IoTの動向・予想

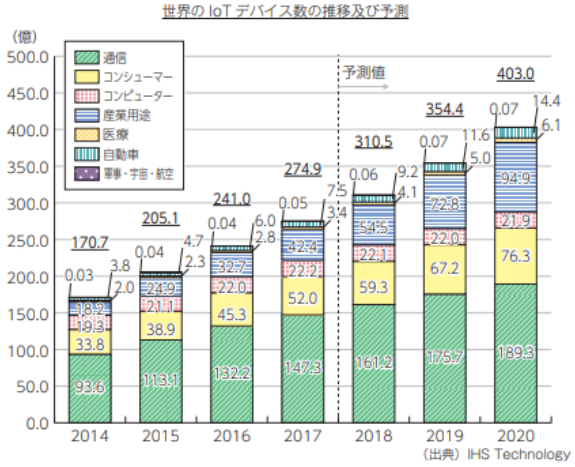
IoTとは？

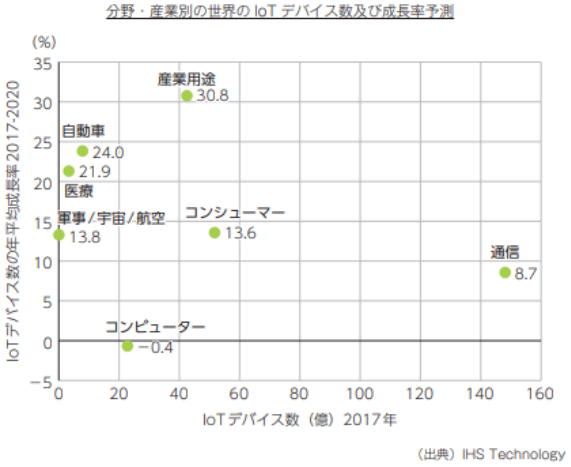
- コンピュータなどの情報・通信機器だけでなく，世の中に存在する様々な物体(モノ)に通信機能を持たせ，インターネットに接続したり相互に通信することにより，自動認識や自動制御，遠隔計測などを行うこと．（出典：IT用語辞典 e-Words）
- IoT?（参考：IoTとは何か，坂村健）
  - Thing=RFIDの付いた商品＠1999
  - ユビキタス・コンピューティング
  - Cyber-Physical Systems
  - などなど

IoTとは何か，坂村健，角川学芸出版，2016

IoTの今と今後

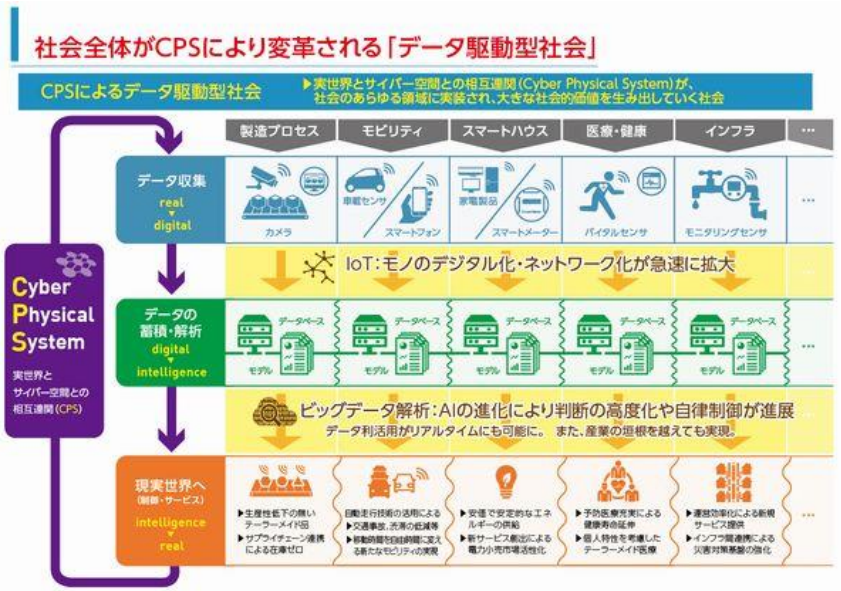
- 第4次産業革命(日本経済2016-2017,内閣府,2017)
  - IoT及びビッグデータ，AI
- 先進テクノロジのハイプ・サイクル(ガートナー)
  - 黎明期⇒「過度な期待」のピーク期⇒幻滅期⇒啓蒙活動期⇒生産性の安定期
- 平成 30 年版 情報通信白書(総務省)
  - IoT デバイス数は 2020 年には約 400 億の予測





IoTの応用領域

- 平成30年版 情報通信白書(総務省)
  - AI・IoTの活用をめぐる近年の動き
    - モビリティ領域(自動運転)
    - スマートシティ・スマートハウス領域
    - ウエルネス領域
- 情報経済小委員会 中間取りまとめ報告書(経産省)
  - 製造プロセス
  - モビリティ
  - スマートハウス
  - 医療・健康
  - インフラ

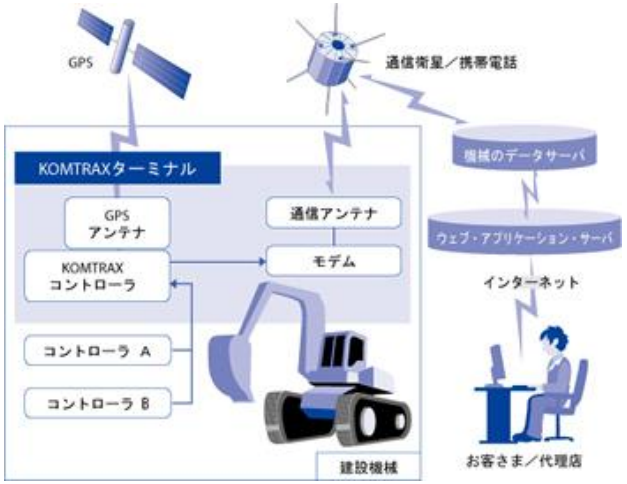


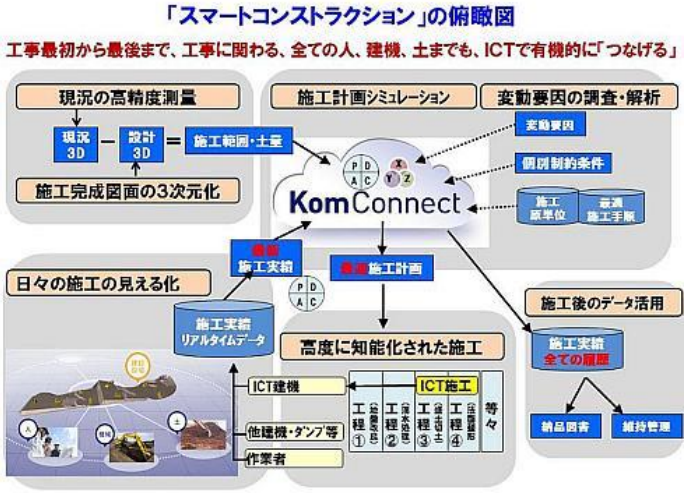
http://www.meti.go.jp/committee/sankoushin/shojo/johokeizai/report_001.html

IoTの活用事例

KOMTRAX

- コマツが開発した建設機械の情報を遠隔で確認するためのシステム(1999)
  - 保守管理（メンテナンス，予防保全），車両管理，稼動管理，車両位置確認，省エネ運転支援，帳票作成
- KOMTRAXの発展
  - スマートコンストラクション，KomConnect



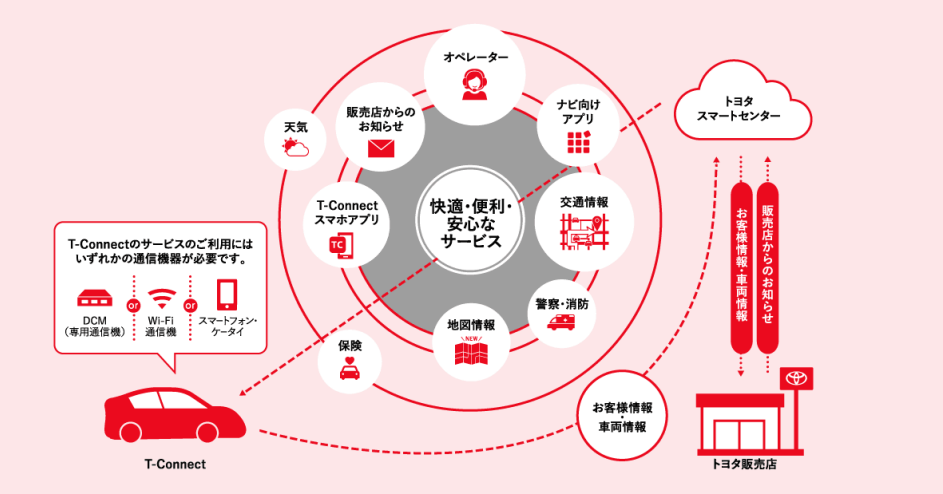


http://www.komatsu-kenki.co.jp/service/product/komtrax/

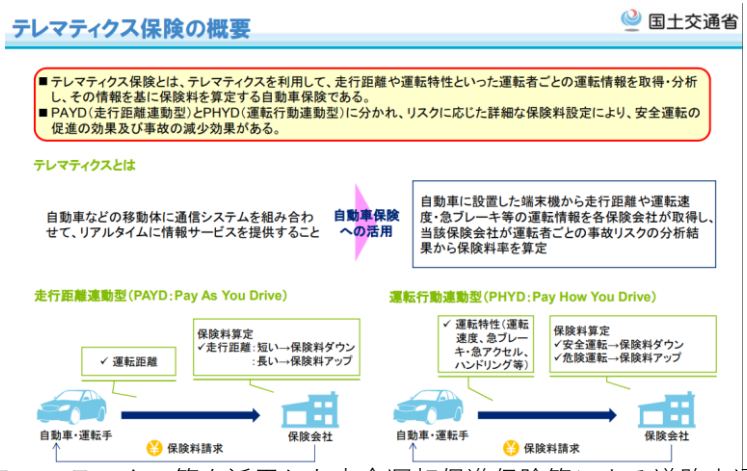
コネクテッドカー

- インターネットへの常時接続機能を具備した自動車
- 緊急通報システム「eCall」
  - 2018年3月31日から欧州連合（EU）では装備が義務化
- テレマティクス保険

  走行距離や運転特性等の運転者毎の運転情報を取得・分析し，その情報を基に保険料を算定する自動車保険



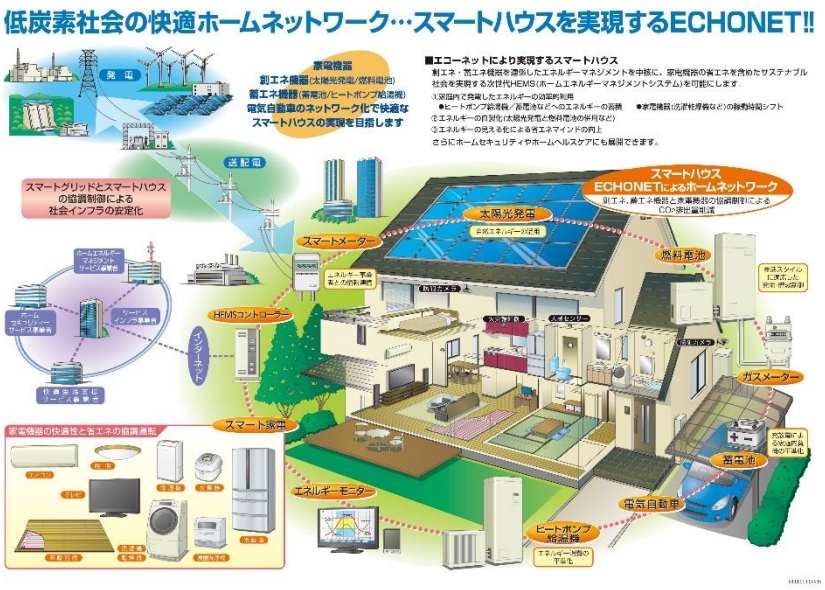
T-Connectとは, TOYOTA, https://toyota.jp/tconnectservice/about/



テレマティクス等を活用した安全運転促進保険等による道路交通の安全, 国土交通省(2014), http://www.mlit.go.jp/common/001061957.pdf[2]

スマートハウス

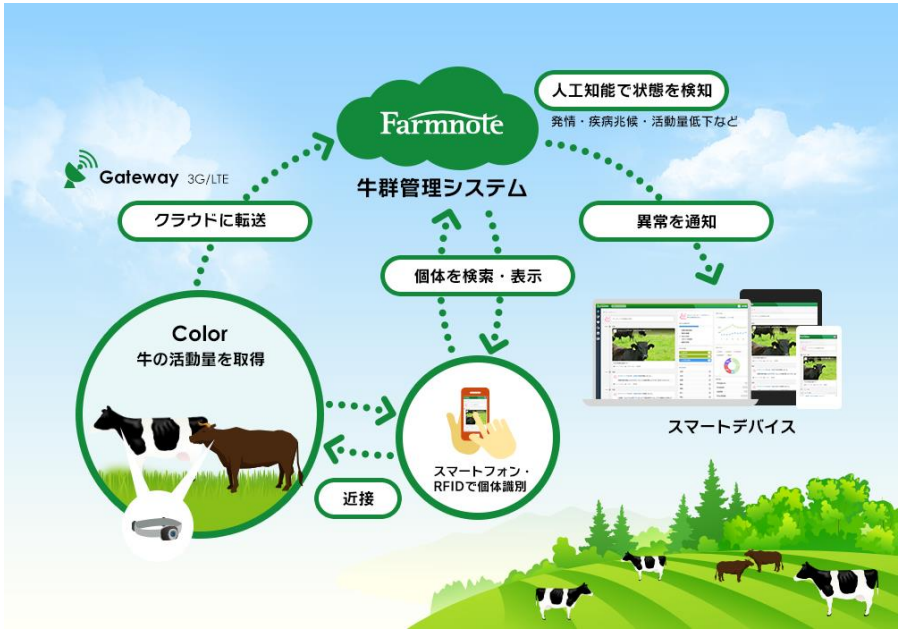
- 省エネ・節約を重視した住宅
- HEMS(Home Energy Management System)
  - 省エネ＋創(太陽光発電機等)＋蓄(家庭用蓄電池等)
  - ECHONET Lite：スマートハウス用通信プロトロル
- ⇒スマートグリッド(次世代送電網)+スマートシティ
- ≒スマートホーム：利便性を重視した住宅(IoT+α)



出典：ECHONET
https://echonet.jp/hems/

ファームノート

- 酪農・畜産向けクラウドサービス開発に特化
  - Internet of Animals
- Farmnote：クラウド型牛群管理システム
- Farmnote Color：牛の活動情報を収集し，通知
  - 注意すべき牛(発情，疾病兆候等)を自動的に選別



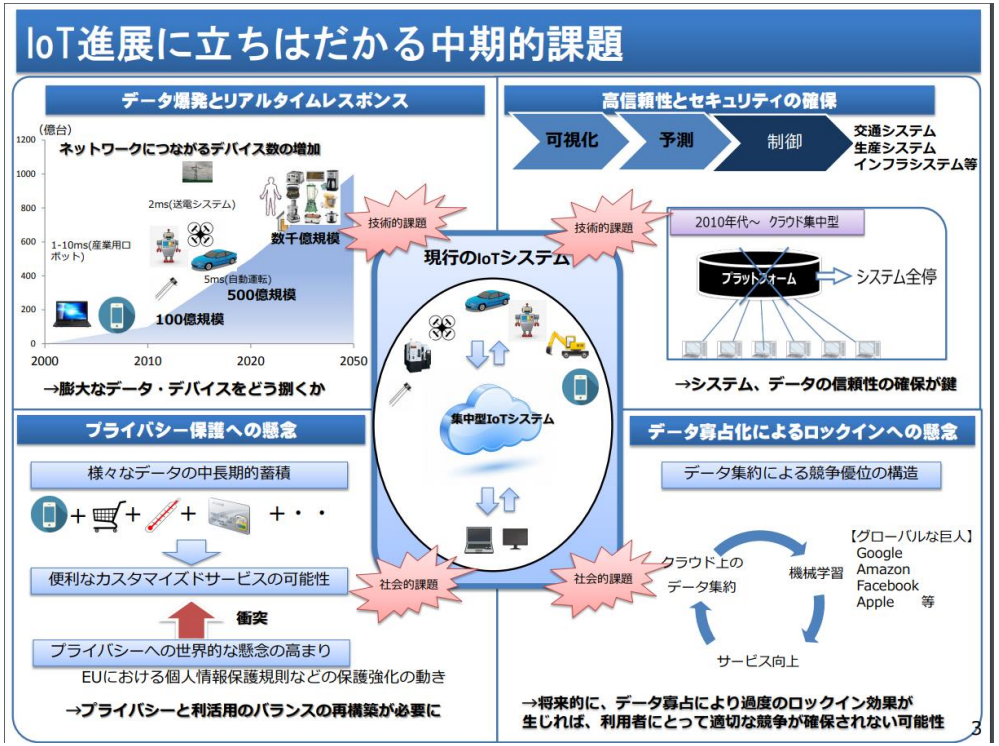
会社名 株式会社 ファームノート
本社 〒080-0847 北海道帯広市公園東町1-3-14
設立 2013年11月28日
資本金 1億1640万円
事業内容 酪農・畜産向け牛群管理システム
「Farmnote」の開発・提供

https://farmnote.jp/color/

IoTの課題

IoTの中期的課題

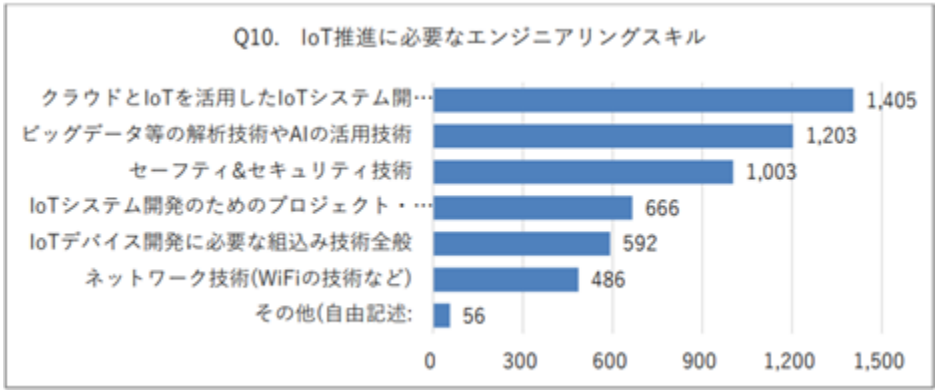
- データ爆発とリアルタイムレスポンス
- 高信頼性とセキュリティの確保
- プライバシー保護への懸念
- データ寡占化による
  ロックインへの懸念



IoT進展に立ちはだかる中期的課題への新たなアプローチ
平成28年12月 経済産業省 商務情報政策局

IoTの課題(人材・スキル)

- 人材に関する課題
  - 出典：日本企業のIoT推進に関する調査結果(ガートナー)
  - テクノロジ人材が不足していると感じるか
    - 調査対象全体(n=515)：Y 52.4%, N 32.2%, ? 15.3%
    - IoTの推進体制を確立済みの企業(n=61)：Y 68.9%, N 24.6%, ? 6.6%
- スキルに関する課題
  - 出典：IT コーディネータが見た 地域における IoT の活用状況と展開上の課題 調査報告書(IPA,ITCA, 2017)
  - IoT推進に必要なエンジニアリングスキルについて



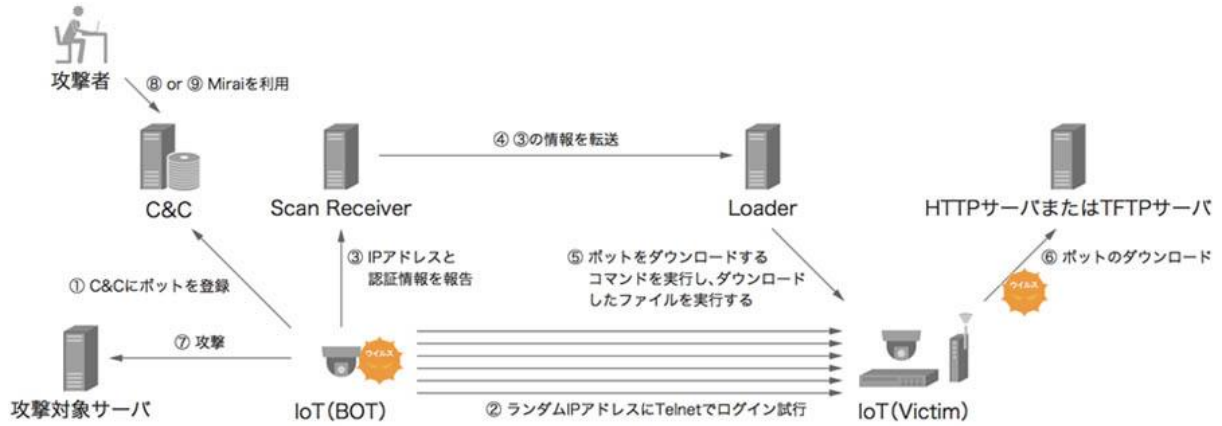
今後の方向性(全体)

- 組込みソフトウェア産業の
  動向や課題に見る今後の方向性
- 技術領域
  - AI技術，ビッグデータ技術の組込みシステムへの活用
  - システムズエンジニアリング技術，アジャイル開発技術の獲得・適用
  - セーフティ及びセキュリティ技術の高度化(IoT対応化)
  - 他の製品・システムとの接続を想定した検証技術の高度化
- 人材領域
  - IoT等新技術(セーフティ，セキュリティ，センサネットワーク，AI,ビッグデータ等)の専門技術者の不足
  - ビジネスをデザインできる人材の不足
  - 複数の応用分野をまたいでとりまとめができる人材の不足

出典：IoT時代の組込み産業の 課題と解決へのアプローチ 組込みソフトウェア産業実態調査（2016年度）
IPA/SEC 田丸喜一郎

課題：Mirai (マルウェア)

- セキュリティ系ブログがDDoS攻撃でダウン
- 攻撃の規模が極めて大きかった
- (PCではなく)IoTデバイスがターゲット
  - PCと比較して台数が極めて多い



Mirai Botnetのシステム構成（出典：Internet Infrastructure Review［IIR］Vol.33）

IoTデバイスを狙うマルウェア「Mirai」とは何か――その正体と対策, 宮田健, 2017

課題：セーフティ＆セキュリティ

- 事例：Jeep車両に対する遠隔からの走行系操作
  - 攻撃者 –モバイル網-> 車内無線LANサービス -CAN-> 走行系
  - セキュリティ侵害がセーフティを脅かす

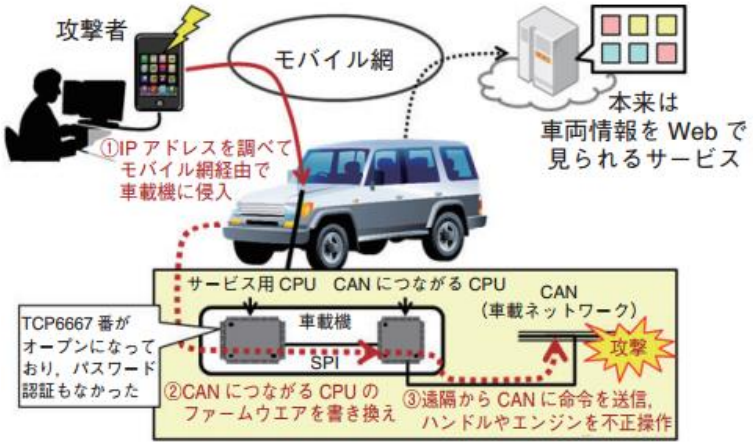
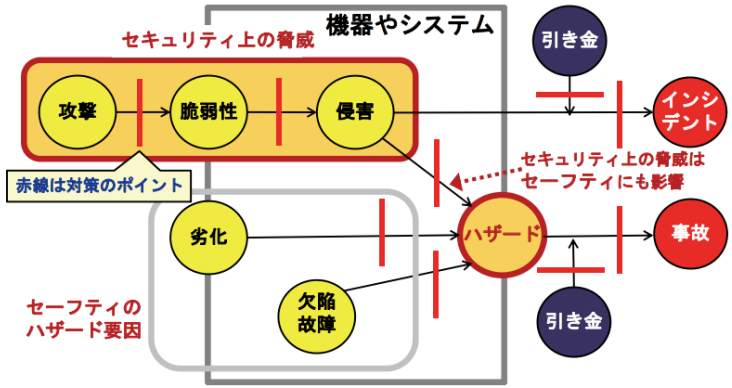


図 2　つながる自動車に対する不正アクセスの例

IoT（つながる組込み機器）における脅威の現状,
井上博之, 精密工学会誌 Vol.83, No.1, 2017, pp.46-49



出典：英国RSSB「The Yellow Book」及びSESAMOプロジェクト「SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS」を基に作成

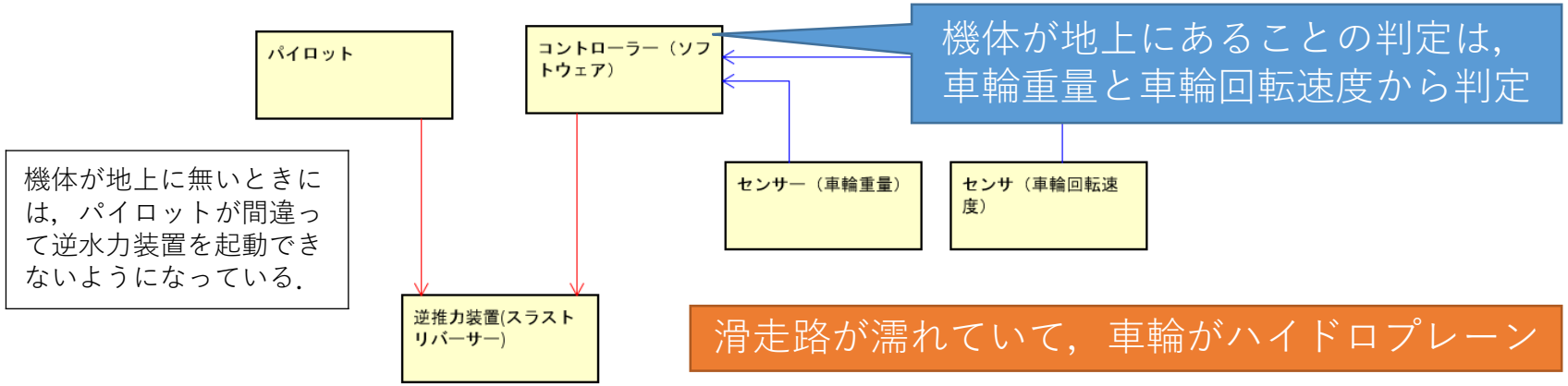
図 2-1　セーフティとセキュリティの被害の発生プロセス

「つながる世界のセーフティ＆セキュリティ設計入門」より

- セーフティとセキュリティに関する分析の統合
  - 「つながる世界のセーフティ＆セキュリティ設計入門」IPA

課題：事故モデル (故障に起因しないハザード)

- 事例：（航空機）の逆推力装置が作動せず
  - 故障も操作ミスもないがアクシデントへ至る
  - 故障・操作ミスに基づく分析法は不向き



- 構成要素間の相互作用に着目して分析
  - この事例の場合，プロセスモデルの不一致として識別 (車輪重量・車輪回転速度だけでは判定できない)

STPA Handbook pp.8の事例から

課題：事故モデル (間接的・全身的要因)

- 事例：ボパール化学工場事故
- イベントチェーンによる事故の記述　systematic(組織的)
  - **E1** 作業員はスリップブラインド(安全板)を挿入することなくパイプを洗浄する.
  - **E2** 水がMIC(イソシアン酸メチル)タンクに漏れる.
  - **E3** 爆発が起こる.
  - **E4** 安全弁が開く.
  - **E5** MICが大気中にまき散らされる.
  - **E6** 風がMICをプラント周辺の人口密集地域に運ぶ.
- 間接的・全身的(systemic)要因も考える
  - 例：効率向上に対する競争的・経済的圧力

課題後半のまとめ＋α

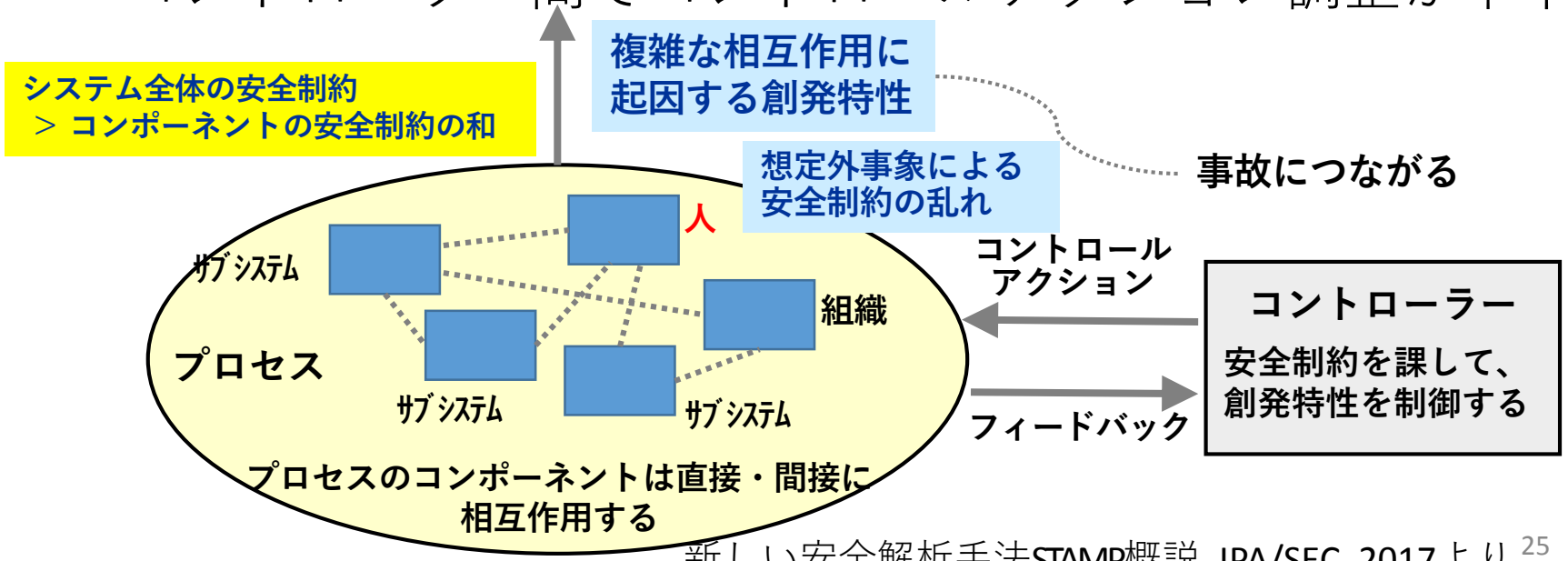
- ネットワークを通じてシステムが連携
  - 障害による影響範囲の拡大
  - 様々なサブシステムを組み合わせたシステム
  - サブシステムは仕様通りに動いているのに,
    システム全体として障害発生
- 物理的影響(センサ・アクチュエータ)
  - セキュリティ侵害が安全性を低下させる
  - 人間もシステムの一部
- 機器の耐用年数が長い
  - 気付かないまま放置される
  - システムの劣化(環境との不整合)

STAMP/STPA

繋がるシステムのためのハザード分析手法

STAMPの概要

- Systems-Theoretic Accident Model and Processes
- システム理論に基づく新しいアクシデントモデル
  - コントロールストラクチャーやコントロールアクションが安全制約を実施できない
  - コントロールストラクチャーが徐々に劣化
  - コントローラー間でコントロールアクション調整が不十分



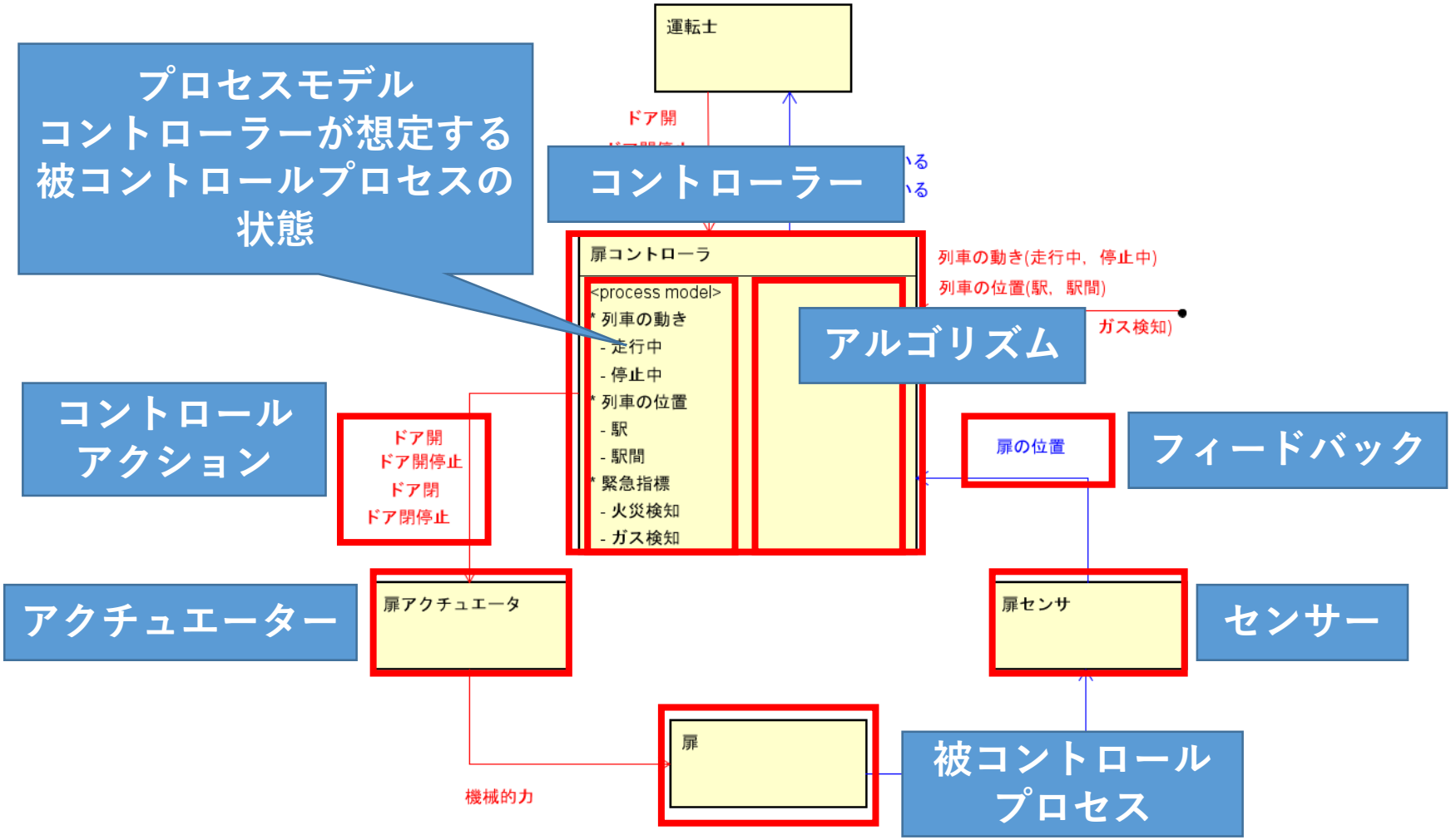
新しい安全解析手法STAMP概説, IPA/SEC, 2017より

STAMP/STPA参考資料

- MIT
  - Engineering a Safer World, 2012
  - STPA Primer, 2013
  - STPA Handbook, 2018 (実務家向け)
- IPA
  - はじめてのSTAMP/STPA, 2016
  - はじめてのSTAMP/STPA(実践編), 2017
  - はじめてのSTAMP/STPA(活用編), 2018
  - STAMP向けモデリングツールSTAMP Workbench

STAMP Workbench

STAMPの基本要素


プロセスモデル
コントローラーが想定する
被コントロールプロセスの
状態
運転士
ドア開
コントローラー
扉コントローラ
<process model>
* 列車の動き
- 走行中
- 停止中
* 列車の位置
- 駅
- 駅間
* 緊急指標
- 火災検知
- ガス検知
アルゴリズム
列車の動き(走行中，停止中)
列車の位置(駅，駅間)
ガス検知)
コントロール
アクション
ドア開
ドア開停止
ドア閉
ドア閉停止
扉の位置
フィードバック
アクチュエーター
扉アクチュエータ
扉センサ
センサー
扉
機械的力
被コントロール
プロセス

STPAの概要

- ハザード分析手法: System Theoretic Process Analysis

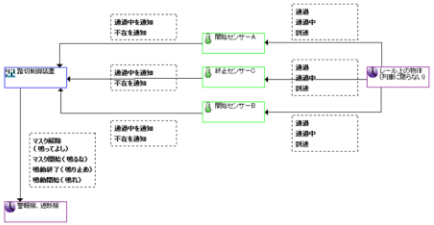
起きてほしくないことは？

危険な相互作用は？

危険な相互作用は
どうして起こった？

システム2	アクシデント	ハザード	安全制約
クルーズコントロール	2台の車が衝突する	自動車の前後に適切な車間距離をとっていない	自動車は定められた車間距離を破ってはならない
化学プラント	化学物質の流出によって人的被害が出る	化学物質が空気中や土壌へ流出する	化学物質が意図せずに放出されてはならない

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

コントロールアクション	与えられないとハザード	与えるとハザード	早すぎ，遅すぎ，順序でハザード	早すぎる停止，長すぎる適用でハザード
コマンド1	XX条件下で，コマンド1が提供されない場合，ハザードに至る(UCA1)	コマンド1の内容が誤っていた場合，処理は停止するが，ハザードには至らない	コマンド1の提供が，コマンド2よりも遅れた場合，指示が上書きされ，ハザードに至る(UCA2)	コマンド1が途中で停止した場合，ハザードには至らない
コマンド2	…	…	…	…

Step1: UCA (Unsafe Control Action) の抽出

	1.上位からの指示や外部情報の誤り・欠落	2.CA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 ・…		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)			・警報機の動作遅れ			・踏切制御装置の動作遅れ

Step2: ロス・シナリオの特定

STPAの手順

STPA(セーフティ)とSTPA-sec(セキュリティ)分析の統合が可能

分析対象のモデルは？

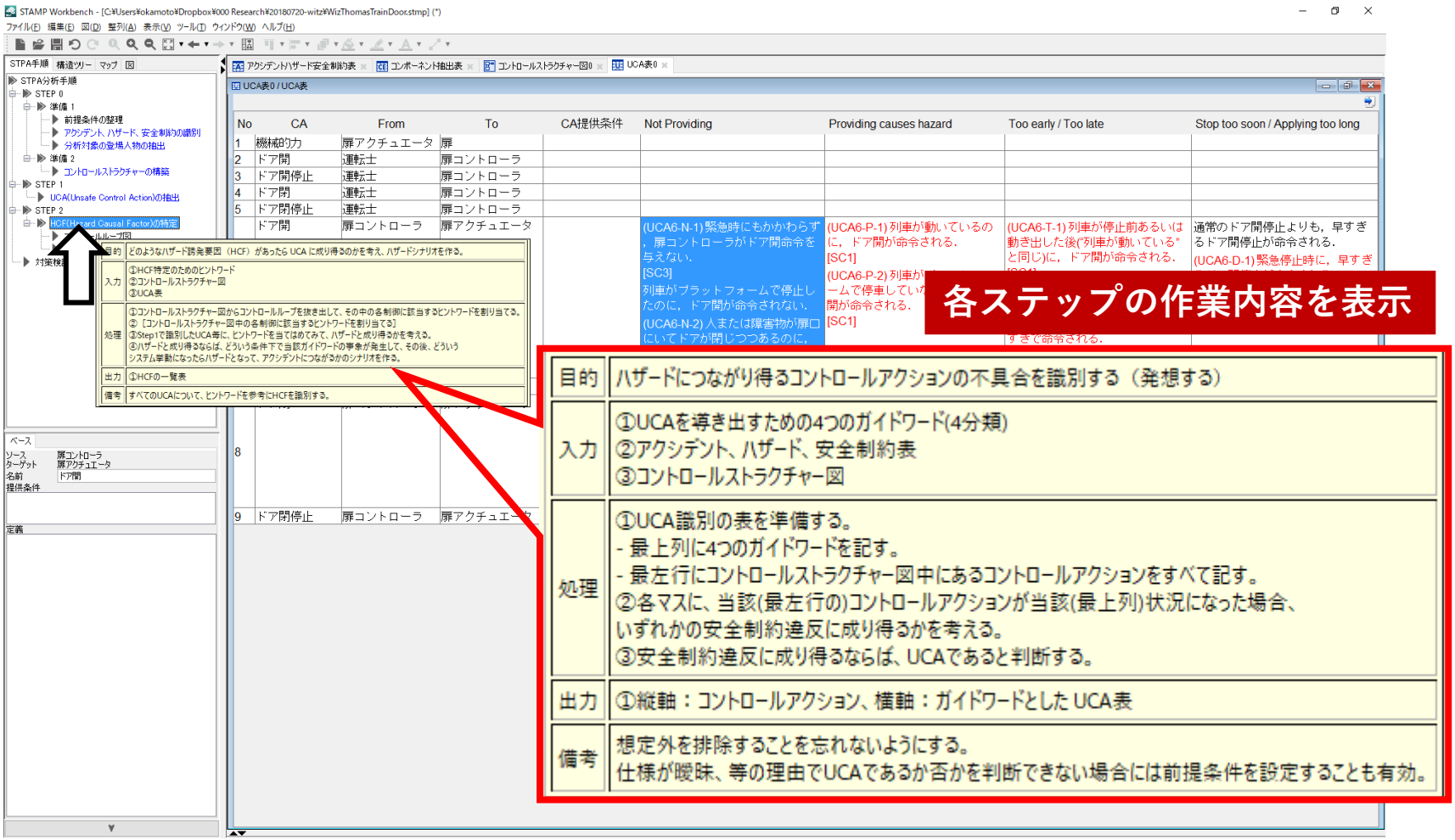
STAMP Workbench

- STAMP向けモデリングツール
  - 産業界で使えるSTAMPモデリングツール
- ガイド機能
  - STAMPの作業手順，用語を知らなくても安全解析可能
- 定型の単純作業は可能な限りツールで自動化
  - 分析者が思考を深められる！
- 普及目的のため無償で公開
  - ソースコードもオープンソースとして公開

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

この章では，STAMP Workbenchを使用してSTPAを実施している．

分析手順・内容の表示

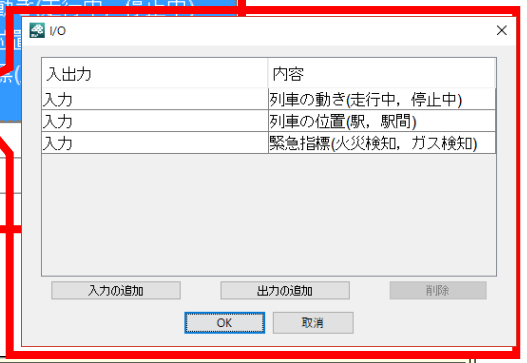

STAMP Workbench - [C:¥Users¥okamoto¥Dropbox¥000 Research¥20180720-witz¥WizThomasTrainDoor.stmp] (*)
STPA手順
STPA分析手順
STEP 0
準備 1
前提条件の整理
アクシデント、ハザード、安全制約の識別
分析対象の登場人物の抽出
準備 2
コントロールストラクチャーの構築
STEP 1
UCA(Unsafe Control Action)の抽出
STEP 2
HCF(Hazard Causal Factor)の特定
UCA表0 / UCA表
No CA From To CA提供条件 Not Providing Providing causes hazard Too early / Too late Stop too soon / Applying too long
1 機械的力 扉アクチュエータ 扉
2 ドア開 運転士 扉コントローラ
3 ドア開停止 運転士 扉コントローラ
4 ドア閉 運転士 扉コントローラ
5 ドア閉停止 運転士 扉コントローラ
ドア閉 扉コントローラ 扉アクチュエータ
(UCA6-N-1) 緊急時にもかかわらず，扉コントローラがドア開命令を与えない．
[SC3]
列車がプラットフォームで停止したのに，ドア開が命令されない．
(UCA6-N-2) 人または障害物が扉口にいてドアが閉じつつあるのに，
(UCA6-P-1) 列車が動いているのに，ドア開が命令される．
[SC1]
(UCA6-P-2) 列車が
ームで停車してい
開が命令される．
[SC1]
(UCA6-T-1) 列車が停止前あるいは動き出した後(“列車が動いている”と同じ)に，ドア開が命令される．
すぎで命令される．
通常のドア開停止よりも，早すぎるドア開停止が命令される．
(UCA6-D-1) 緊急停止時に，早すぎ
8
9 ドア閉停止 扉コントローラ 扉アクチュエータ
目的 どのようなハザード誘発要因（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特定のためのヒントワード
②コントロールストラクチャー図
③UCA表
処理 ①コントロールストラクチャー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ヒントワードを割り当てる。
②［コントロールストラクチャー図中の各制御に該当するヒントワードを割り当てる］
③Step1で識別したUCA等に、ヒントワードを当てはめてみて、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 ①HCFの一覧表
備考 すべてのUCAについて、ヒントワードを参考にHCFを識別する。
ベース
ソース 扉コントローラ
ターゲット 扉アクチュエータ
名前 ドア閉
提供条件
定義
各ステップの作業内容を表示
目的 ハザードにつながり得るコントロールアクション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、安全制約表
③コントロールストラクチャー図
処理 ①UCA識別の表を準備する。
- 最上列に4つのガイドワードを記す。
- 最左行にコントロールストラクチャー図中にあるコントロールアクションをすべて記す。
②各マスに、当該(最左行の)コントロールアクションが当該(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。
③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：コントロールアクション、横軸：ガイドワードとしたUCA表
備考 想定外を排除することを忘れないようにする。
仕様が曖昧、等の理由でUCAであるか否かを判断できない場合には前提条件を設定することも有効。

自動生成：表形式から図へ

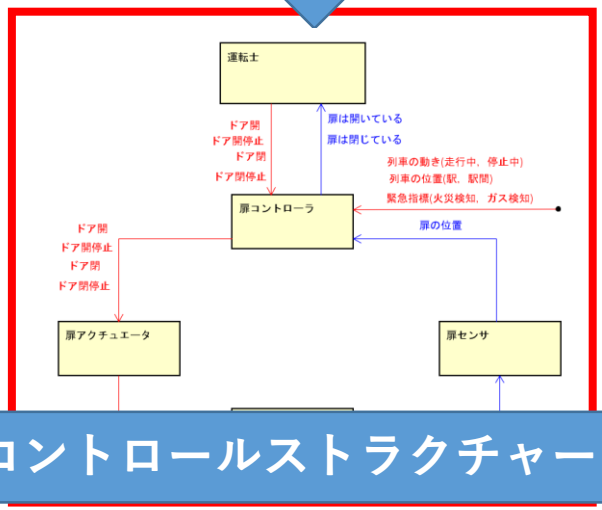
コンポーネント

関係

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	入出力	備考
☑	運転士		ドア開 (To: 扉コントローラ) ドア開停止 (To: 扉コントローラ) ドア閉 (To: 扉コントローラ) ドア閉停止 (To: 扉コントローラ)			
☑	扉コントローラ		ドア開 (To: 扉アクチュエータ) ドア開停止 (To: 扉アクチュエータ) ドア閉 (To: 扉アクチュエータ) ドア閉停止 (To: 扉アクチュエータ)	扉は開いている (To: 運転士) 扉は閉じている (To: 運転士)	(入力)列車の動き(走行中，停止中) (入力)列車の位 (入力)緊急指標(	
☑	扉アクチュエータ		機械的力 (To: 扉)			
☑	扉			機械的位置 (To: 扉センサ)		
☑	扉センサ			扉の位置 (To: 扉コントローラ)		



生成

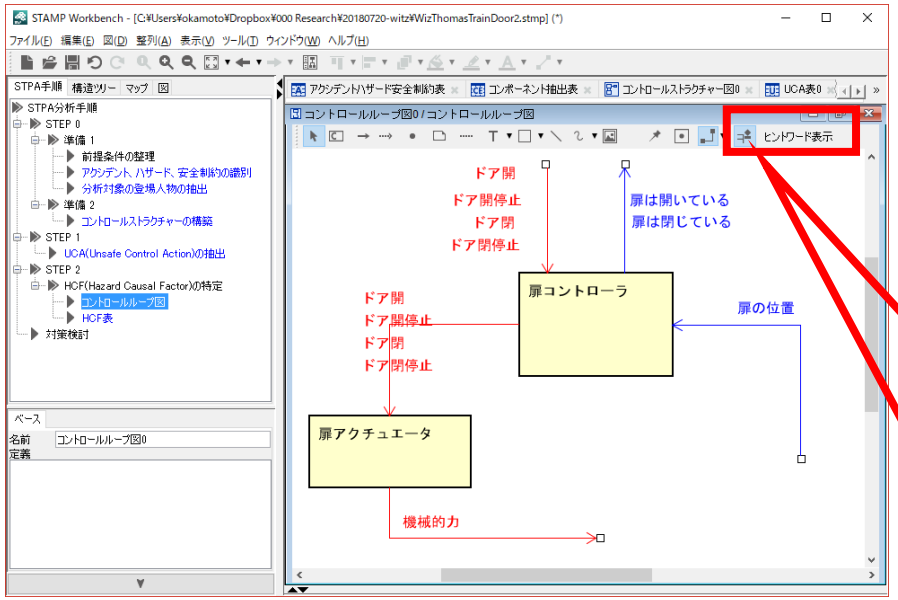


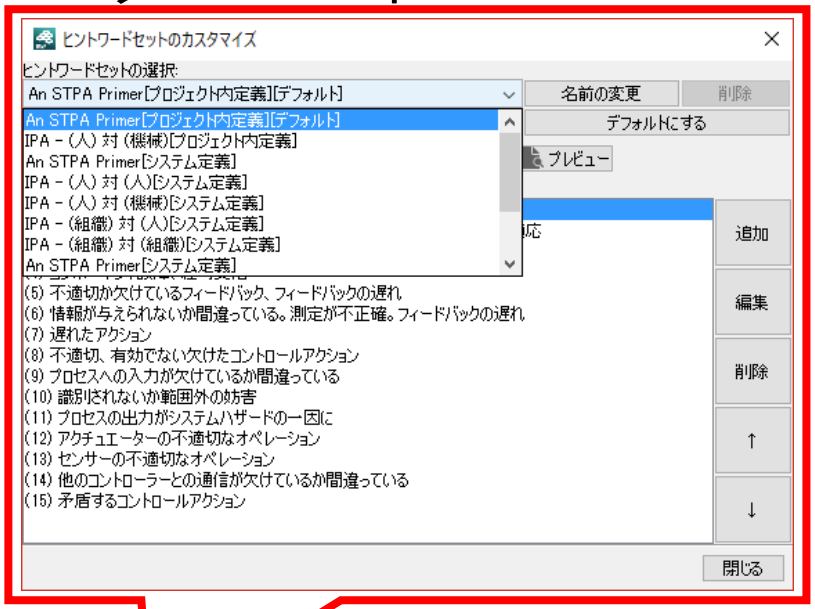
コントロールストラクチャー図

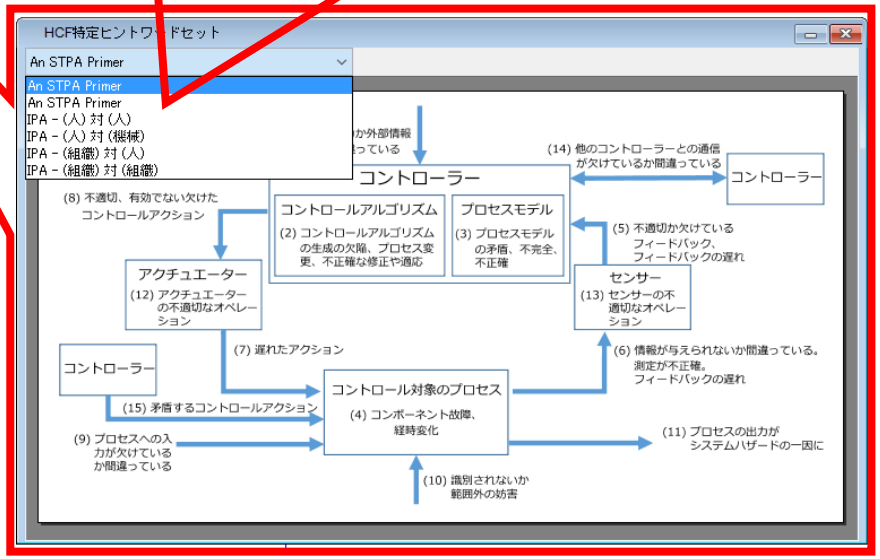
目的	要求仕様書から登場人物を抽出し、コントロールストラクチャー図作成の元となる情報を整理する。
入力	①要求仕様書
処理	①要求仕様書から登場人物(コンポーネント)を抽出する。 ②要求仕様書から各コンポーネントの役割を抽出する。 ③役割を果たすために必要な制御、役割を果たした結果のフィードバックを抽出する。 ④制御、入出力情報(情報を与えるのみで制御を行うわけではない)の違いを分別する。 ⑤登場人物が、今回の分析対象かどうかを決定する。
出力	①コンポーネント抽出表
備考	整理した分析対象の登場人物の情報を元に、コントロールストラクチャー図を生成できる。 コンポーネント抽出表とコントロールストラクチャー図を使いコントロールストラクチャーを明確にする。 全ての欄を埋める必要はない。この表からコントロールストラクチャー図を完成させようとは考えないこと。 この表をある程度記入したらコントロールストラクチャー図の雛型を生成し、その後は図を見て、図の編集をしながらコントロールストラクチャーを考える。

分析ヒントのカスタマイズ

ヒント(原因の例)を表示
ヒントセットは選択・追加可能







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/
  - https://github.com/asimabdulkhaleq/XSTAMPP
- SafetyHAT：DB連携，ガイドワード編集
  - The Volpe STPA Tool
- an STPA tool：拡張STPAをサポート
  - Tool assisted Hazard Analysis and Requirement Generation based on STPA
  - An STPA Tool
- SAHRA： Enterprise Architect拡張
  - http://sahra.ch/

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

まとめ

- はじめに
- IoTの動向・予想
- IoTの活用事例
- IoTの課題
- STAMP/STPA
  つながるシステムのためのハザード分析手法