最先端ソフトウェア工学ゼミ[個別ゼミ1] 成果報告

2022年7月14日

氏名：朴　龍勲
所属：キヤノンメディカルシステムズ

発表内容

1. 設定したテーマとその理由
   - テーマ設定
2. 調査方法
   - 自動運転領域の論文調査
3. 調査結果
   - 調査した論文のまとめ
4. 考察
   - 自動運転から医療への展開
5. まとめ

設定したテーマとその理由

- テーマ：AIシステムに対する複数のリスク分析手法の比較研究の調査
- 設定した理由
  - 今回のリスク分析手法を調査結果をプロフェッショナルスタディで活用したい
  - 先行分野(自動運転)での運用実績を活用して、医療分野への適用を検討したい
    - 2分野ともに人命にかかわるもので、安全性に対する要求が高い
    - 自動運転分野での実績が他の分野より多い

手法の紹介

- HAZOP
  - 標準化された「ガイドワード」とプロセスパラメータを使用して、プロセス機能の設計意図からの潜在的な逸脱を特定、逸脱の原因を推測し、考えられる結果を判断し、リスクを軽減するためのセーフガードアクションを示す
- FMEA
  - FMEAには構造化されたフレームワークがある。アイテムの説明、失敗、原因、重大度（S）、発生（O）、および検出（D）が含まれ、リスク優先順位をS、O、およびDの割り当てに基づいて計算され、RPNにより障害のリスクの定量的な優先順位付けが可能
- FRAM
  - システムハザード分析を実行するためのシステム機能の識別と各機能の6つの基本特性（入力、出力、時間、リソース、前提条件、および制御）　を構造的に記述
- STPA
  - 事故の原因となった不適切な制御と設計上の不適切な制御を見つける方法で、不十分/安全でない制御と原因となるシナリオを4つのステップで特定

調査方法

- リスク分析手法(HAZOP, FMEA, FRAM, STPA)+自動運転をキーワードとしてネットワークで論文を検索し、以下の2つ論文を絞り込んだ。
  - 論文① ：Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems
    - Yan-Fu Li, Tsinghua University, Enrico Zio ,PSL Research University
    - ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, SEPTEMBER 2022, Vol. 8 / 031104-1
  - 論文②：Comparison of hazard analysis methods with regard to the series development of autonomous vehicles
    - Greta Carlotta Kölln, Michael Klicker, Stephan Schmidt
    - ITSC’19: Intelligent Transportation Systems Conference

調査結果(論文①)

- 背景
  - 自律走行車(AV:autonomous vehicle)が複雑で相互接続されたシステムが含まれているようになり、システム間の相互作用を顧慮したシステム信頼性レベルが向上する必要があるが、ハザード分析の従来手法(HAZOP,FMEA)と新規手法(FRAM,STPA)の包括的比較は不足
- 研究目的
  - **HAZOP、FMEA、FRAM、STPAの利点/欠点をAV体表的な安全機能である自動緊急ブレーキシステム(AEB)のケーススティで検討する**
    - ①AVシステムの解析について、HAZOP、FMEA、FRAM、STPAの使い方
    - ②AVシステムのハザード分析の4つの方法を実行する際の類似点と相違点は何か？
    - ③相互作用が増加する複雑なAVシステムに最も適したハザード分析戦略は何か？

調査結果(論文①)

■ 分析手法の比較

属性	HAZOP	FMEA	FRAM	STPA
ハザード特定	部分的	部分的	包括的	包括的
根本原因特定	Y	Y	Y	Y
定性的/定量的	定性的/定量的(偏差)	定性的/定量的(優先順位)	定性的	定性的
危険原因要因	偏差からHW/SW障害	HW/SW障害	共振（HW / SW / ヒューマン/インターフェース障害）	インターフェース（HW / SW / 人間などの制御コマンド）
詳細レベル	詳細	詳細	調整可能	調整可能

分析結果の比較

属性	HAZOP	FMEA	FRAM	STPA
ライフサイクルフェーズ	設計段階、製造、および設置段階	設計段階、製造、および設置段階	設計段階から変更および改造段階	設計段階から変更および改造段階
必要なスキル	工学（電気/機械/ソフトウェアなど）	工学（電気/機械/ソフトウェアなど）	システムアーキテクチャとエンジニアリング（電気/機械/ソフトウェアなど）	システムアーキテクチャとエンジニアリング（電気/機械/ソフトウェアなど）
必要なリソース（時間とコスト）	少	少	多	多
複雑さ/難しさ	簡単	簡単	複雑	複雑

分析プロセスの比較

属性	HAZOP	FMEA	FRAM	STPA
帰納的(I)/演繹的(D)	I（効果）/D（原因）	I	I（上流）/D（下流）	I（制御ループ）/D（シナリオ）
起点	機能	失敗例	機能/アクション	損失/システムレベルの危険
必要ツール	ワークシート	ワークシート	FRAMプログラム	ワークシート/STPAプログラム
抽象的/具体的	具体的	具体的	具体的/抽象的	抽象的
必要なデータ	関数と説明 例：フローチャート	関数と説明 例：機能図面	局部を含む機能説明	制御ループの説明

分析ステップの比較

全体的なアーキテクチャ	製品設計	製造設計	テスト設計	メンテナンス設計
ハードウェアシステム(機械的)	FMEA	FMEA	HAZOP/FMEA	FMEA
電子システム	HAZOP/FMEA	FMEA	HAZOP/FMEA	HAZOP/FMEA
検出器システム	HAZOP/FMEA/FRAM	FMEA	HAZOP/FMEA/FRAM	FMEA/FRAM
ソフトウェアシステム	FRAM/STPA	FRAM/STPA	STPA	FRAM/STPA
V2X通信システム	FRAM/STPA	FRAM/STPA	HAZOP/FRAM/STPA	FRAM/STPA

メソッドの適用と組み合わせ (AVシステム)

論文「Comparison of the HAZOP, FMEA, FRAM, and STPA Methods for the Hazard Analysis of Automatic Emergency Brake Systems」から翻訳して引用

調査結果(論文①)

- 結論
  - ① AVシステムの解析について、HAZOP、FMEA、FRAM、STPAの使い方
    - 各手法を利用して分析実施し、使い方をまとめた
  - ②AVシステムのハザード分析の4つの方法を実行する際の類似点と相違点
    - 共通点：分析の流れが類似
    - 相違点：フォーカスと原理が違う
  - ③相互作用が増加する複雑なAVシステムに最も適したハザード分析戦略
    - マルチメソッドの組み合わせおよび/またはメソッド拡張の形でのメソッドアプリケーションに関する研究が必要。
    - ソフトウェアシステムのテストケースの設計やリスク受容基準の設定を研究が必要

調査結果(論文②)

- 背景
  - ISO 26262などの自動車に関する安全性要求
    - ハザード分析を含むが，ソフトウェア中心のシステムで有効か？
    - 開発サイクルが速く，設計の自由度が高い
    - 複雑で因果関係の列が線形でない
  - 2018年のUber事故
    - FMEA/FTAで扱うようなハードウェア故障ではない
    - オブジェクト認識の誤りや条件
    - 人間と機械の相互作用も影響
- 研究目的
  - 自動運転分野での従来手法と新規手法STPAを比較する
    - SPTAに期待：安全性を故障ではなく制御問題ととらえる

調査結果(論文②)

- 自動運転におけるハザード分析の要件
  - R1. 開発の早期に使うことができる
    - 安全性に関する設計を反映できるように
  - R2. 対象システムの深い理解が必要ない
    - 分析専門家が多くのシステムに携われるように
  - R3. ソフトウェアのerror・相互作用によるerrorを扱える
    - ハードウェア故障以外が主流に
  - R4. 人間との相互作用を扱える
    - 自動運転スタイルがドライバーの意識と合わない場合など
  - R5. システムをまたがるイベントを統合できる
    - 法規制などシステムにまたがる組織，車両間影響などを考慮
  - R6. 分析の終了条件が明確である
    - 完全性を得やすくなる
  - R7. 導入される手段に応じてerrorを分類できる
    - 発生確率や検出確率，影響確率を踏まえて優先付けをしたい
  - R8. 分析手順がしっかり制限されている
    - 専門家の知識に依存しない
  - R9. 手法の専門家が必要条件ではない
    - 短期間で学習でき効果的に適用可能であるべき

調査結果(論文②)

- 分析手法の比較

	STPA	FTA	FMEA
対象システムの深い理解が必要ない	X		
開発早期に並行に利用可能	X	X	
ソフトウェアerror・相互作用errorを扱える	X		X
人間との相互作用を扱える	X	(X)	
導入される手段に応じてerrorを分類できる			X
システムをまたがるイベントを扱える	X		
研究室などの資源を要さない	X	X	
終了条件が明確	X		
手法の専門家が必要条件ではない	X		

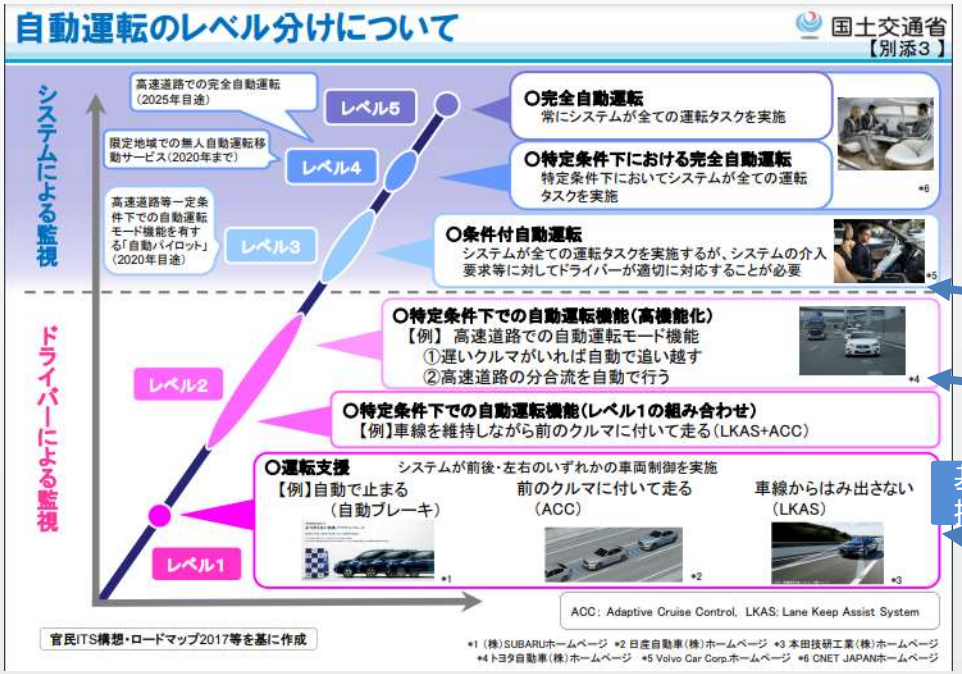
論文「 Comparison of hazard analysis methods with regard to the series development of autonomous vehicles 」から翻訳して引用

考察

- 論文①と②結果から自動運転では人との相互作用の分析はSTPAが有効であるがわかった。
  - 医療意思決定支援でも人との相互作用が重要であることで、STPAが医療に展開するとき有効と考えられる
- 医療意思決定支援と自動運転での人との相互作用の方法が違う
  - STPAを医療へ適用に向け、医療での相互作用に適切な変更＆方法の検討が必要と考えられる

考察

■ 自動運転と医療意思決定のレベル対応関係

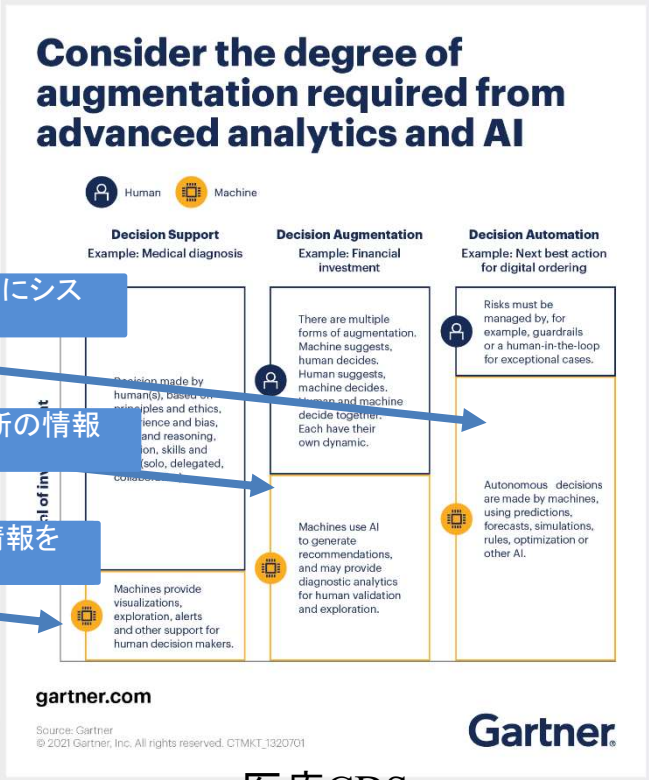


自動運転

一部が完全にシステムで実施

高度な判断の情報を提供

基本な判断の情報を提供



医療CDS

自動運転：国土交通省の「自動運転の実現に向けた国土交通省の取組」から引用(https://www.mlit.go.jp/common/001227121.pdf)
医療CDS：Gartnerの「Would You Let Artificial Intelligence Make Your Pay Decisions?」から引用(https://www.gartner.com/smarterwithgartner/would-you-let-artificial-intelligence-make-your-pay-decisions)

考察

- 人との相互作用での自動運転と医療意思決定支援の類似点と相違点
  - 類似点
    - 人の監視が必要である
    - 安全性に対する要求が非常に高い
  - 相違点
    - 医療では人間(医師)の最終確認が必要。
    - 自動運転は直接機械を動かすに対して、医療では結果を医師に提示する

考察(医療分野への分析手法調査)

- Using FRAM to explore sources of performance variability in intravenous infusion administration in ICU : a non- normative approach to systems contradictions.
  - 背景
    - ICUでは医学、看護、薬学、安全、IT、ヒューマンファクターなどの専門家のチームを作成して診療を行う
    - チームではルール、アドバイスの矛盾、目標コンフリクト、需要と実際のミスマッチなどが矛盾が色々ある。
  - 研究目的
    - ICUでのシステム矛盾の管理方法をFRAMで評価可否を調査
  - 結果
    - FRAMを利用して矛盾の内在を調べ、性能の変動や動的にトレードオフの管理、安全性確保に有効である。

医療分野ではチーム医療の人と人の間の評価などでFRAMを利用するケースがあるが、AIシステムなどでの評価するケースが少ない

考察

- STPAを医療に適用時に検討すべき点（例）
  - ステップ0 準備1：アクシデント、ハザード、安全制約の識別
    - 最終的には患者に対するアクシデントやハザードになるが、これを引き起こす医師に対するシステムの安全制約を定義が必要
  - ステップ0 準備2：コントロールストラクチャーの構築
    - 医師(人)を含むコントロールストラクチャーを構築する必要がある。
  - ステップ1：安全でないコントロールアクションの抽出
    - 患者に対する意思決定は医師が決定するので、医師が意思決定するための安全でないシステムコントロールアクションを検討する必要がある。
  - ステップ2：非安全なコントロールの原因の特定
    - 医師のミスを引き起こすシステムの原因も特定が必要

まとめ

- 論文①：分析対象のシステムや分析対象フェーズによって利用手法が違う。人間との制御はSTPAが有効である
- 論文②：自動運転のような人間を含む複雑な相互接続のシステムではSTPAなどの新規分析手法が有効である
- 考察：医療分野でも自動運転分野のように人間を含む複雑で相互接続されたシステムが多いので、新規リスク分析手法(STPA)が医療分野でも有効であることが想像できるが、実際の分析では医療特有性を顧慮する必要がある

ありがとうございました。