演習コースIII

ｾｰﾌﾃｨ&ｾｷｭﾘﾃｨ開発における STAMP/STPA の有効性検証

An efficacy investigation of STAMP/STPA for Safety and Security Development

リーダー：西澤　賢一（GE ﾍﾙｽｹｱ・ｼﾞｬﾊﾟﾝ）
研 究 員：大森　淳夫（パイオニア）　　中嶋　良秀（ノーリツ）
田中　基大（ナブテスコ）　　畑　久美子（インテック）
仲田　謙太郎（東京精密）　　渡邉　泰宙（コニカミノルタ）
主査：金子　朋子（情報ｾｷｭﾘﾃｨ大学院大学）　副 主 査：髙橋　雄志（アイダック）
アドバイザー：佐々木　良一（東京電機大学）

研究概要
IoT 時代を迎えるにあたって，セーフティとセキュリティのバランスの取れた開発方法論が必要である．しかしながら，バランスの取れた方法論は確立されておらず，既存のセーフティにおける開発手法や，セキュリティにおける開発手法がどの程度バランスの取れた設計手法として使えるのかの検証もされていなかった．昨年，セーフティとセキュリティのバランスの取れた開発方法論として STAMP/STPA に STRIDE のヒントワードを拡張する手法を提案した．この手法により，対象分野の専門知識を持たない技術者でも，セーフティとセキュリティ両面のリスクを同時に分析し検証できることを示した．しかしながら，この手法を用いた場合と用いない場合のリスク分析に差があるかの検証はできていなかった．そこで本稿では，この手法を用いた場合と用いない場合でリスク分析に差があることを検証した結果,この手法がセーフティ&セキュリティ開発において有効であることが分かったので報告する．

1. はじめに

インターネットが普及する以前は,1つの機能が1つのモノで完結して実現されており，機能そのものの構成要素も少なかった．それに対し，近年は，1 つの機能が複雑化するに伴い機能の構成要素が増えた．さらに，多くのモノがネットワークにつながり相互にやり取りをすることで 1 つの巨大なシステムとして人々の利便性を大きく高めている．IoT（Internet of Things）時代といわれる所以である．

このような状況の下，システム障害は個々の構成要素の故障のみならず，しばしば構成要素同士の間，ないし，システムと人間との間の複雑な相互作用によって引き起こされることがある．つまり，各構成要素は正常に動作しているが，それらを組み合わせたシステムにおいてコミュニケーションミスマッチを起こし機能を実現出来なくなるケースがある．例えば，制御する側が制御される側の状態を誤って認識したため，誤った制御指示を与える．その結果，最終的に障害につながってしまうことが挙げられる．

また，システムがネットワークに接続することにより，個々のシステムが故障しないことを目的としたセーフティ設計だけでなく，外部からの悪意を持った攻撃により損失を防ぐことを目的としたセキュリティ設計も同時に求められている．しかし,「セーフティとセキュリティを考慮した設計の必要性を認識しつつも，半数以上の企業では基本方針が設けられていない」など開発上の取り組みは不十分な状態にある[1]．なお，本研究では，セーフティとは，偶発的なミス，故障などの悪意のない危険に対する安全を示し，セキュリティとは，悪意を持って行われる脅威に対しての安全を示すものとする．

我々はこれまでに，自動車の自動運転サービスを取り上げ，STAMP/STPA に STRIDE のヒントワードを拡張することで，対象分野の専門知識を持たない技術者でも，セーフティとセキュリティ両面のリスクを分析し検証できるという事例を示した[2]．しかしながら，STAMP/STPA の手順を用いた場合と用いない場合のリスク分析に差があるかの検証はできていなかった．そこで，本稿では，下記を示すこととした．

RQ1: セーフティ&セキュリティのリスク洗い出しにおいて，STAMP/STPA の手順に沿って実施する場合とそうでない場合との差はあるのか.
さらに，セーフティとセキュリティの開発は新規開発のみではなく，派生開発でも求められることから，下記も示すこととした.
RQ2: 一度モデル化した STAMP のコントロールストラクチャー（以下，CS）が再利用可能であるか.

2. 関連技術

2.1. STAMP/STPA

ソフトウェア設計のリスク分析において，前述したシステム構成要素間のやりとりに着目し，検証しようとするのが，安全解析手法 STAMP/STPA（Systems-Theoretic Accident Model and Processes / System-Theoretic Process Analysis）である. STAMP とは，システム理論に基づく事故モデルのことであり，その STAMP アクシデントモデルを前提とし，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のことを STPA と呼ぶ[3].
STAMP/STPA では前提として，システム事故の多くは，構成要素の故障ではなく，システムの中で安全のための制御を行う制御要素と被制御要素の相互作用が働かないことによって起きるとしている. その前提を持って，要素（コンポーネント）と相互作用（CA:Control Action）に着目してメカニズムを説明し，アクションが働かない原因が CA の不適切な作用に等しいという視点を持つことで原因を有限化している[4]. STAMP/STPA を用いることで，はじめにで述べたような複雑なシステムのリスク分析ができると期待されている.

2.2. STRIDE

STRIDE とはマイクロソフト社が定義する脅威モデルである. システムに対するセキュリティ上の脅威は様々なものがある. STRIDE では，Spoofing identity(なりすまし），Tampering(改ざん），Repudiation(否認），Information Disclosure(情報の暴露），Denial of Service(サービス不能），Elevation of Privilege(権限の昇格)という 6 つのカテゴリに分類している. 名称は各カテゴリの頭文字を現したものである. STRIDE 分類を要因分析のヒントワードとして用いる STAMP/STPA の脅威分析の拡張提案がなされている[4] [5].

3. 比較実験

3.1. 実験概要

RQ1 を確認するために，自動車の自動運転に焦点を当て，自動車の専門家ではない被験者を，STAMP/STPA を知らない被験者が行うリスクの洗い出し（以下，STAMP を用いない分析）と，STAMP/STPA を知っている被験者が行うリスク洗い出し（以下，STAMP を用いた分析）に分けて，リスクの洗い出しを行い，その差を確認することとした. 今回 STAMP による分析を行った被験者は，本コースなどで数時間から数日程度学習はしたが，実務では実施していない STAMP 初心者である.
参考文献[1]で対象とした自動運転のブレーキシステムをリスク洗い出しの対象システムとするが，STAMP を用いない分析を行う被験者から出てくるリスクが発散すると考えるため,「自動車自動運転レベル 3 の，夕暮れ時かつ雨天のシーンにおけるブレーキ周り」という条件を付けることとした.

3.2. 実験手順

【手順 1】質問紙調査
STAMP/STPA の経験を問う設問と，特定シーンを想定したセーフティ&セキュリティのリスクと対策を考える問からなる質問紙を作成し質問紙調査を行った. 質問内容は，以下のとおりである.
問 1:STAMP/STPA を知っていますか？（※他者に説明を求められたときに，説明ができる場合に「はい」).
問 2:STAMP/STPA を使った分析を過去にしたことがありますか？（※ツールハンズオ

ンや演習などでのトライアルを含む).

問 3: 自動車自動運転レベル 3 の，夕暮れ時かつ雨天のシーンにおけるブレーキ回りのセーフティ並びにセキュリティ上のリスクを 5 つ以上思いつく限り挙げてください（※レベル 3 とは自動運転と手動運転が混在するものである).

問 4:問 3 で上げたリスクに対する対策をお答えください.

【手順 2】質問紙の集計ならびにパラメータの設定

質問紙調査の回答で得られたリスクについては，そのリスクがセーフティまたはセキュリティどちらに基づくリスクであるのか，リスクに対する対策の有無を判別する．対策については，該当するリスクがあるのかを判別する.

【手順 3】集計結果のグルーピング

手順 2 で判別したリスクについて，以下で示す原因や攻撃方法に基づいてグルーピングを行う．セキュリティの分類は 2.2 節で紹介した STRIDE を使用した.

セーフティ: 人とシステムの認識の違い，センサーの誤検出または故障，システムの性能限界，ヒューマンエラー，その他

セキュリティ: S(なりすまし)，T(改ざん)，R(否認)，I(情報の暴露)，D(サービス不能)，E(権限の昇格)，その他

【手順 4】データ集計

手順 3 のグルーピングをもとに被験者ごと，STAMP を用いない分析と STAMP を用いた分析の全体でリスクのグループごとに洗い出しができた件数を集計する.

【手順 5】傾向性の考察

手順 4 の集計結果から STAMP を用いない分析と STAMP を用いた分析の結果にどのような傾向性があるかを考察する.

3.3. 実験結果

【手順 1】質問紙調査

本稿の執筆者 7 名の所属先から 30 名に質問紙調査を行った．手順 1 では問 1 と問 2 の結果を表 1 に示す．このうち問 1 並びに問 2 の回答が共に「はい」となった被験者は 6 名であり，この 6 名が STAMP を用いた分析を実施した．それ以外のうち問 1 問 2 の回答が共に「いいえ」となった 22 名が STAMP を用いない分析を実施した.

表 1 質問紙調査: 問 1 と問 2 への回答結果

		問 1	
		はい	いいえ
問 2	はい	6 名	1 名
	いいえ	1 名	22 名

問 3: 1 人当たりのリスク件数は STAMP を用いた分析では 70.7 件，STAMP を用いない分析では 6.1 件であった.問 4: 1 人当たりのリスク対策の件数は STAMP を用いた分析では 33.0 件，STAMP を用いない分析では 4.1 件であった（表 2).

表 2 被験者 1 人当たりのリスク件数

	STAMP を用いた分析	STAMP を用いない分析
平均（件数）	70.7	6.1

【手順 2】質問紙の集計ならびにパラメータの設定

質問紙調査の回答で得られたリスクについてそのリスクがセーフティまたはセキュリティのどちらに基づくリスクであるか(図 1)，また，リスクに対する対策の有無（表 3）を示す.

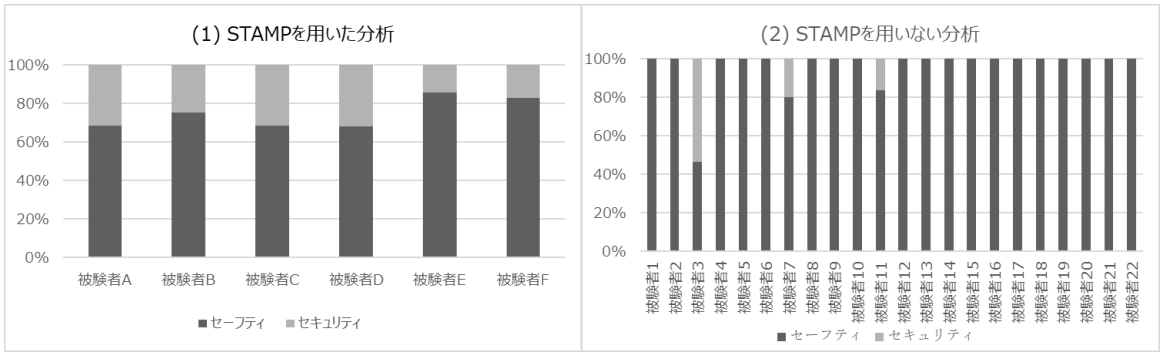

図 1 抽出したリスクのセーフティ/セキュリティの割合

表 3 抽出リスクの対策の有無

	STAMP を用いた分析		STAMP を用いない分析	
	対策あり	対策なし	対策あり	対策なし
平均（件数）	63.8	6.8	4.4	1.7
平均（%）	90.3%	9.7%	79.4%	20.6%

【手順 3，4，5】集計結果のグルーピング及びデータ集計

手順 2 で分析されたセキュリティ，セーフティのリスクをさらに手順 3 で示したグループを用いて分類した結果を図 2，図 3，図 4 に示す.

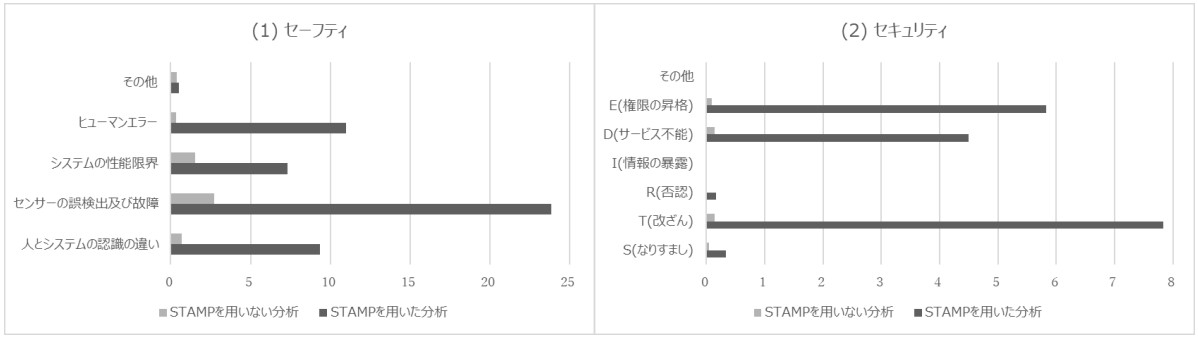

図 2 被験者 1 人当たりのリスク件数の内訳

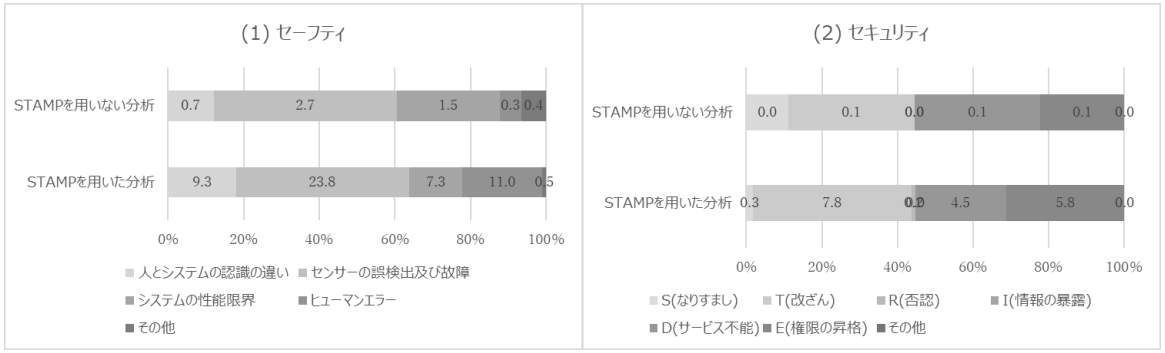

図 3 被験者一人当たりのリスクの割合

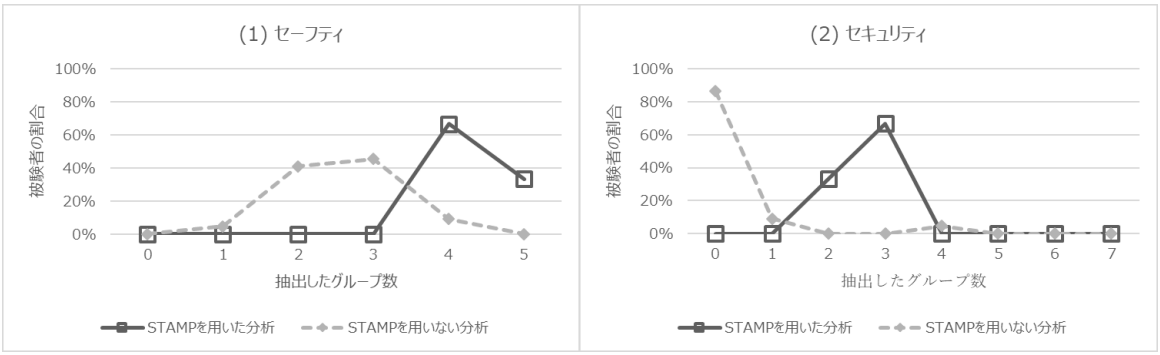

図 4 抽出したグループ数ごとの被験者の割合

4. STAMP/STPA を用いたリスク洗い出し手順

3.2 節【手順 1】STAMP を用いた分析の結果を用いて，RQ2 を確認する．参考文献[2]と同じく自動運転のブレーキシステムの事例で，3 章で示した比較実験のために，「自動車自動運転レベル 3 の，夕暮れ時かつ雨天のシーンにおけるブレーキ周り」という条件を加えた．以下，STAMP/STPA の手順に沿ってリスクの洗い出しを行った結果を示す．なお，本手順は STAMP Workbench[6]を用いて行った．

【手順 1】アシュアランスケースによる保証全体像の決定

参考文献[2]と同じく，保証する範囲を，人命・財産喪失という重大アクシデントに限定し，保証全体像を示す論理モデルとして，GSN(Goal Structuring Notation)を決定した．

【手順 2】STAMP/STPA の Step 0（アクシデント，ハザード，安全制約の識別，コントロールストラクチャーの構築）を実施する

識別したアクシデント，ハザード，安全制約を表 4， CS を図 5 に示す．

【手順 3】STAMP/STPA の Step1(UCA の抽出)を実施する

手順 2 で識別した CS に基づき識別した UCA(Unsafe Control Action)のうちセンシング補助モジュールがコントローラーとなる CA9 を表 5 に示す．

【手順 4】STAMP/STPA の Step2（HCF の特定）を実施する

手順 3 の結果から識別した HCF(Hazard Causal Factor)のうち一部を以下に示す．

- 運転手が意図せずに，ブレーキペダルを踏み込み，自動運転が解除される．かつ運転手が自動運転解除警報に気が付かず，手動で運転していない（HCF-1)．
- 人工知能モジュールに侵入されて，ブレーキの指示アルゴリズムを改ざんされ，減速指示をなしにさせられる（HCF-2)．

【手順 5】 GSN を用いてハザードと UCA を整理

手順 2 から 4 の結果を，GSN を用いて整理した．自動運転におけるブレーキ操作に関するアクシデントをハザードと UCA により整理した結果を図 6 に示す．

表 4 アクシデント，ハザード，安全制約の一覧（一部抜粋）

アクシデント	ハザード	安全制約
(A1) 自動車が外部環境（歩行者/他の車/周辺物）と衝突/接触する	(H1)自動車が，ブレーキをかけても，外部環境の前で停止できない	(SC1)自動車が，外部環境と衝突しないようにブレーキをかける(外部環境までの距離や相対速度を制御する)
	(H2)ブレーキがかからない	(SC2)運転手と自動車の両方がブレーキをかけられない状態にならない
	(H3) 急ブレーキにより後方車両から追突される	(SC3)SC1 に違反しない程度に緩やかに減速する

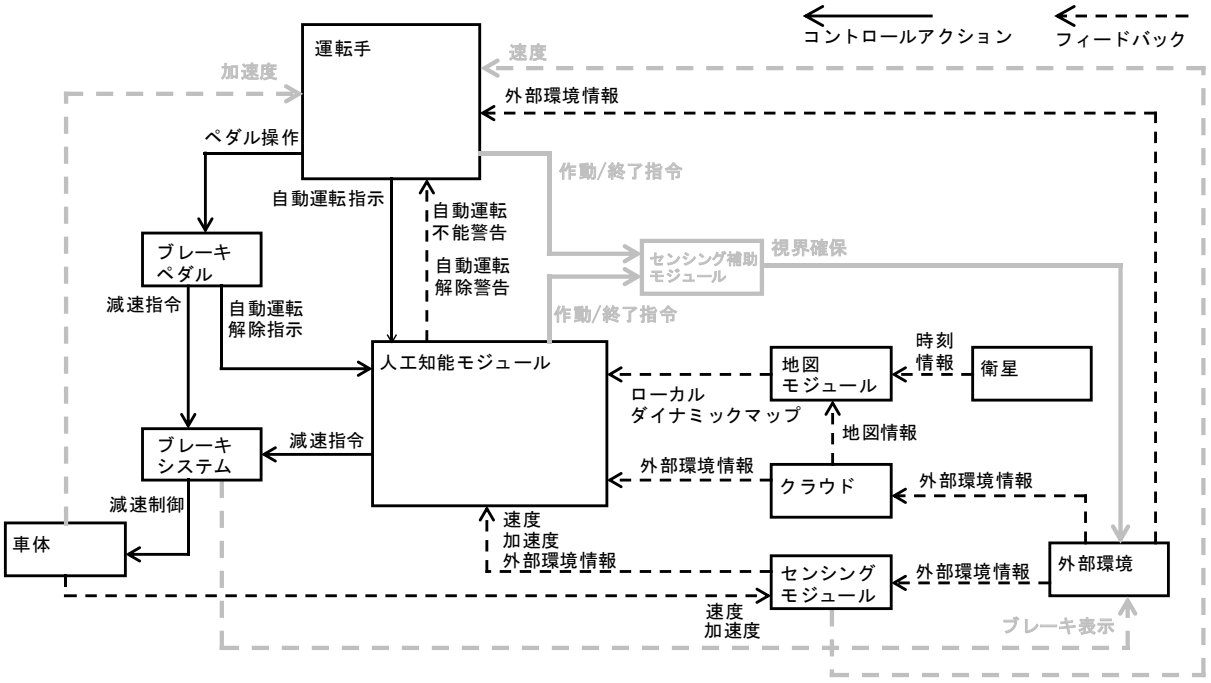

図 5 焦点を当てる自動運転機能の CS

表 5 センシング補助モジュールに関する UCA の一覧（一部抜粋）

CA	Not Providing (与えられないとハザード)	Providing causes hazard (与えられるとハザード)	Too early / Too late (早過ぎ,遅過ぎ,誤順序)	Stop too soon / Applying too long (早過ぎ,長過ぎの適用)
CA9:視界確保	(UCA19-N-1) 視界の確保が行われないと，運転手/人工知能が外部環境を認識できず，ブレーキをかけずに衝突する [SC1][SC2]	(UCA19-P-1) 運転手/人工知能が外部環境を認識できないほど視界の確保機能が働き，ブレーキをかけずに衝突する [SC1][SC2]	(UCA19-T-1) 視界の確保作動のタイミングが遅すぎ，運転手/人工知能が外部環境を認識できない状態となり，ブレーキをかけずに衝突する [SC1][SC2]	-

5. 考察

5.1. RQ1 についての考察

以下のように STAMP を用いた分析は,STAMP を用いない分析よりも良好な結果となった.

(1) 被験者 1 人当たりのリスク件数は STAMP を用いた分析の方が 11.6 倍多い（表 2).

(2) STAMP を用いた分析は，セーフティにおいて多くのグループでリスクを検出している（図 4 において，グラフのピークが，右側，すなわちグループ数の大きな方にあることから示される).

(3) STAMP を用いない分析では，多くの被験者でセキュリティ・リスクが抽出できていないのに対して，STAMP を用いた分析では，全員抽出できている.（図 1)

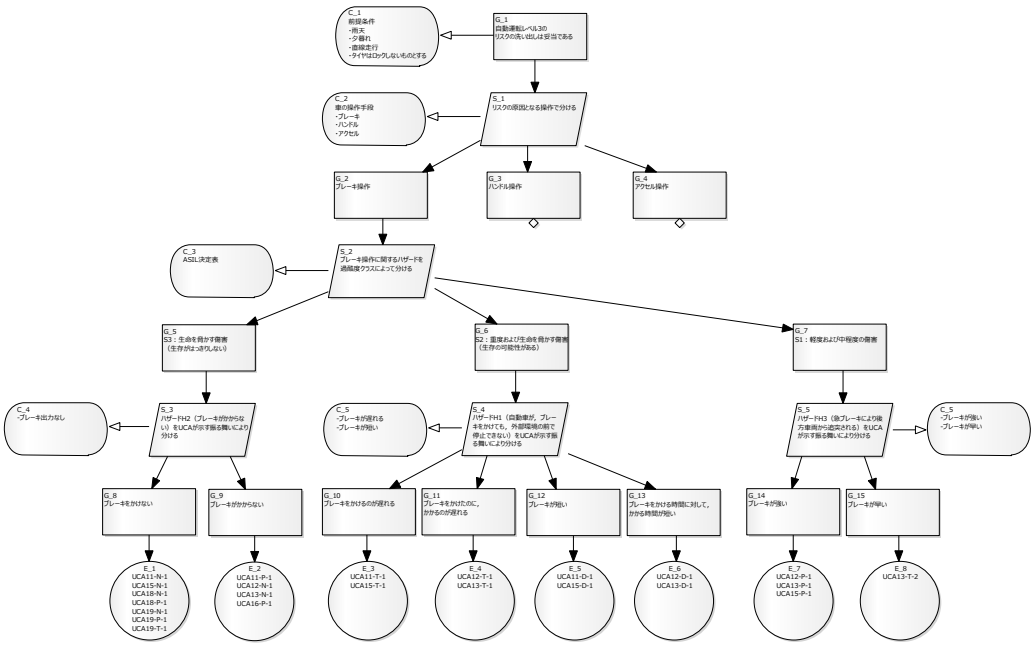

図 6 GSN によるハザードの整理

(1) 及び(2)について，STAMP を用いた分析に以下の特徴があることが要因と考える．

- STAMP を用いた分析は，CS を利用して手順通りに分析を進めるため，すべてのコンポーネントを考慮できている．
- STAMP を用いた分析は，システムだけではなく，人間も分析対象としている．これは，図 2，図 3 でヒューマンエラーや人とシステムの認識の違いが STMAP を用いない分析より非常に多く挙げられていることから分かる．
- STAMP を用いた分析は，システム内部の要素のやり取りも分析対象としている．同じく，図 2，図 3 で人とシステムの認識の違いが非常に多く挙げられていることから分かる．
- STAMP を用いた分析は，ガイドワード及びヒントワードを利用している．何もないところからリスクを導き出すことは難しいが，これらのワードがあることで導出しやすくなっていると考える．

(3)について，STRIDE をヒントワードとして拡張することが，有効に作用している．

5.2. RQ2 についての考察

図 5 で示した CS は，参考文献[2]で作成した CS に比べて，以下が追加されている（追加されているものは図 5 においてグレーでハイライトしている）．

(1) センシング補助モジュール コンポーネント
(2) センシング補助モジュール コンポーネントに関連する CA
(3) フィードバック

追加のみで CS を作成できたことにより，再利用できていると考える．なお，(1)及び(2)について，「夕暮れ時かつ雨天のシーン」という条件の追加，(3)について参考文献[2]からの詳細化が要因と考える．

5.3. 実験を通して気がついたこと

STAMP を用いた分析を実施した結果， 4 章【手順 4】で示したリスクを抽出できた．このうち，HCF-1 は CS で人とのインタラクションを考えたことで抽出され，HCF-2 は CS を考えたことで抽出されたと考える．これらは CS を用いて複雑なシステムを分析する STAMP/STPA を用いたことで抽出できたのである．また STAMP を用いた分析では，「どこで，どのようなことが発生するか」が CS 図上で明確になるため，挙げられた対策も具体化でき

ている.また,同一の CS 図上でセーフティとセキュリティを同時に検討できることは,我々が目指すセーフティとセキュリティのバランスの取れた開発方法の要件にマッチしている.

5.4. 有識者へのヒアリング結果

抽出されたリスクに対して，セーフティならびにセキュリティ分野の有識者よりコメントをいただいた.

セキュリティの有識者からは「STAMP を用いた分析の方は，どこでどのようなことがあったのかが分かった.リアリティのあるよい題材となっている」,「同じリスクであっても，どこでリスクが発生しているのかによって対策は異なる．STAMP を用いた分析の方は，発生個所が特定されているので，対策が具体化されているようだ」,「マルウェアや多段攻撃が考慮できていない」,「運用時の運転だけではなく，製造・保守・破棄のフェーズもあるので，考慮するとよい」との知見を得ることができた.

また，セーフティの有識者より本実験の分析について「手法の有用性として，リスクの捕捉率があるとよい．すべてのリスクを洗い出すのは困難だが，全員で抽出できたリスクを総和して，さらに議論して新たなリスクを考えれば全リスクと類似できるではないか」,「抽出されるリスクの有効性を論じることができるとよい．容易に気が付くかどうかをレベル付けして,集計するとわかるのではないか」というコメントをいただくことができた.

6. 今後の課題

5.4 節のヒアリング結果に基づき,「マルウェアや多段攻撃が考慮できていない」について，階層化して詳細を考慮すると，抽出可能と考えるので，階層化して分析を行うことを実施したい．また,「運転時のみではなくその他のフェーズについても考慮に入れる」について，アクシデントの識別方法を検討する必要がある.

さらに,セーフティ&セキュリティのチェックリストは,確認できる限り存在していないが，チェックリストを用いる場合と本実験の結果との比較を行うことで有効性を主張できると考える．一方で，セーフティまたはセキュリティのチェックリストを用いた場合との比較は可能であるので今後比較を行うことを課題とする．これらは今後，STAMP/STPA 分析の効果をより具体的に測る上での課題である.

7. まとめ

本稿では，自動車の自動運転システムを取り上げ，STAMP/STPA を用いたリスク分析と，質問紙調査による STMAP/STPA を用いない自由なリスク分析を行い,結果を比較することにより，STAMP/STPA を用いたリスク分析が良好な結果が得られることを示した．また，参考文献[2]で用いた分析条件に対し，条件を付加して分析を行うことにより，既に作成した CS が再利用可能であることを示した．今後，6 章で述べた課題に取り組むと共に，更なる事例作成，普及展開を図る.

参考文献

[1] IPA/SEC，セーフティ設計・セキュリティ設計に関する実態調査結果，2015
[2] 大森淳夫・中嶋良秀・西村伸吾・久連石圭・柴引涼・邱章傑・久木元豊・松本江里加・荒井文昭・細谷雅樹・神田圭・太郎田裕介，セーフティ＆セキュリティ開発のための技術統合提案と事例作成，日本科学技術連盟 SQiP 研究会分科会報告書，2018
[3] システム安全性解析手法 WG,はじめての STAMP/STPA～システム思考に基づく新しい安全性解析手法～，Ver1.0，2016.3
[4] 金子朋子･高橋雄志･大久保隆夫･勅使河原可海･佐々木良一,安全解析手法 STAMP/STPA に対するセキュリティ視点からの脅威分析の拡張提案,Computer Security Symposium 2017, pp.1273-1279，2017.10
[5] Tomoko Kaneko, Yuji Takahashi, Takao Okubo and Ryoichii Sasaki, “Threat analysis using STRIDE with STAMP/STPA”, The International Workshop on Evidence-based Security and Privacy in the Wild 2018
[6] IPA/SEC, STAMP Workbench, https://www.ipa.go.jp/sec/tools/stamp_workbench.html, 2018，2019 年 1 月 12 日アクセス確認