STAMP モデリングのスマートシティに対する安全性分析への適応

Adaptation of STAMP Modeling to Smart Cities for Safety Analysis

リーダー：畠山　剛（三菱電機）　　鎌田　桂太郎（アイホン）
研 究 員：和田　久（NTT ｺﾐｭﾆｹｰｼｮﾝｽﾞ）　　福田　秀樹（TIS）
　　小長谷　義浩（TIS）　　浜田　淳（ﾃｯｸｽｴﾝｼﾞｿﾘｭｰｼｮﾝｽﾞ）
　　菅野　浩司（ｴﾌﾟｿﾝｱｳﾞｧｼｽ）
主　査　：金子　朋子（国立情報学研究所）
副 主 査：髙橋　雄志（日本 AI システムサービス）
アドバイザー：佐々木　良一（東京電機大学）

研究概要
スマートシティは少子高齢化・災害・感染症・インフラの老朽化などの社会課題を解決するとともに，新たな価値を創造する取り組みとして期待されている．この取組みに向け政府機関等からスマートシティに関する指針が示されている．しかし，その指針には安全性(セーフティ)に関する記述がない．加えて，スマートシティでは多くの公共・民間サービスが存在するが，各サービスが連携する部分については安全性の考慮がされていない．そこで，本稿では自動運転車両を例に STAMP S&S を用いて，スマートシティにおける公共・民間サービス間の連携を明確にした．そして，アクシデントモデルとその安全性解析手法である STAMP/STPA を活用し，各サービス間の連携に潜む安全性分析を行った．その結果，消防から警察への救急車出動情報の連携不良で救急車と自動運転車両の事故に繋がるなど，サービス間の連携によって自動運転車両へ間接的にもたらされるリスクを検出した．

Abstract.
Smart cities are expected to solve social issues such as declining birthrate and aging population, disasters, infectious diseases, and aging infrastructure, as well as to create new value. Government agencies and others have provided guidelines for smart cities for this initiative. However, there is no description about safety in the guideline. In addition, although there are many public and private services in smart cities, safety is not taken into consideration for the parts where each service is linked. Therefore, in this paper, we used STAMP S & S with the theme of self-driving vehicles to clarify the cooperation between public and private services in smart cities. Then, using the accident model and its safety analysis method, STAMP / STPA, we performed a safety analysis hidden in the cooperation between each service. As a result, we detected the risk indirectly brought to the autonomous driving vehicle by the cooperation between services, such as the poor coordination of the ambulance dispatch information from the fire department to the police leading to the accident between the ambulance and the autonomous driving vehicle.

1. はじめに

スマートシティは，IoT や AI などの先端技術の活用により，少子高齢化，災害の頻発，感染症のリスク，インフラの老朽化など，様々な社会課題を解決するとともに，新たな価値を創造する取り組みとして期待されている[1]．また，自治体や企業といった様々な公共・

民間組織がスマートシティへのサービス提供を検討している[2].

政府機関では，内閣府・総務省・経済産業省・国土交通省によってスマートシティガイドブック[1]が作成されている．この中で，セキュリティについては定義されている[3]もののスマートシティ全体に対する安全性(セーフティ)については指針が示されていない．安全性とは「許容不可能なリスクがないこと」[4]と定義され，人の生命や健康に関わる「事故や損失がないこと」[5]を指す．「安全・安心なスマートシティの実現」に向けて，スマートシティのリスク分析・対応の指針は重要である．

スマートシティでは，交通や防災などにおいて多種多様なサービスが存在し，関連する公共・民間サービス提供者が，独自に要素毎の安全性分析を実施している．しかし，自身の責任範囲に限定した分析に留まっており，スマートシティ全体の公共・民間サービスやシステムが連携／関与する相互作用については考慮されていない．

そこで我々は，多種多様なサービスが連携／関与する特性を STAMP（System-Theoretic Accident Model and Processes）の制御構造図（以降，CS 図と表記）と，金子らによって提唱されている STAMP S&S[6]の 5 階層モデルを用いることでモデリングできるようになると考えた．本稿では，自動運転車両を例に，安全性分析の初期段階であるリスクの検出を行うことが可能であるか検証することを目的とし,前述のサービスやシステムが連携／関与する相互作用に着目した安全性分析を実施した．この一環で公共・民間サービス間の連携によって自動運転車両へ間接的にもたらされる，安全性を損なうリスクの検出を実施した．

2. 関連研究・技術

2.1. STAMP

Nancy Leveson が提唱した STAMP モデルでは，システムの様々な階層でコントローラと被コントロールプロセスに該当する要素が存在しており，それらの相互作用が適切に働くことによりシステムの安全が実現されるとする．STAMP モデルは，アクシデントは相互作用が適切に働かないことによって起こるとしている．たとえコントローラも被コントロールプロセスも故障せずに，仕様通りに正しく動作していても，不適切な制御指示（Control Action：以降，CA と表記）が与えられることによって，最終的にアクシデントにつながるというモデルなのである[7]．また，コンポーネント間の CA，フィードバックデータといった相互作用を分析するために， CS 図を構築する．CS 図はコンポーネント間の制御，被制御，情報のフィードバックを図示できるもので，制御の流れや情報の流れを容易に把握できる価値・効果がある．

2.1.1. STPA (System-Theoretic Process Analysis)

Leveson らが提唱した STPA は STAMP アクシデントモデルを前提として，システムのアクシデントの可能性が潜在している状態（以降，ハザードと表記）とその要因を事前に分析するための安全性分析手法である[7]．従来は，FTA（Fault Tree Analysis）や FMEA（Failure Mode and Effect Analysis）の手法が用いられてきたが，これらは，単一コンポーネントの分析には有用であるが，スマートシティ等，相互作用が複雑なシステムの安全性分析においては十分ではないため，新しいアクシデントモデルによる分析手法が必要とされた．

STPA では，4 種類のガイドワードによって安全でない CA を抽出することが可能である．この手法を利用することで，スマートシティに関係する公共・民間サービス同士の連携においても，安全性を損なう連携を相互作用として抽出できるのではないかと考えた．

2.1.2. STAMP S&S

STAMP S&S は従来の STAMP を応用した金子らの提案である．S&S は，Safety，Security の他，Society，Stakeholder，Service，System，Software の 5 階層と，Specification，Standard，Scenario の略称を指す[6]．その方法は分析対象を 5 層にモデル化し，自然環境

や社会規範などの社会自体や公共・民間サービス・AI システムを含めた世界をシステム思考で捉え，対象間の相互作用を詳細化し，安全性分析に役立てる方法である．

我々は，この手法の 5 層モデルをスマートシティに適用することで Society から Software に至るまでの階層および，各階層に属する様々な構成要素において，それらの間の関係を考慮した分析が可能になると考えた．定義を表 1 に示す．

表 1　STAMP S&S の詳細定義

階層	説明
Society	社会環境・社会生活（規則，基準，習慣）・自然環境（天候などの自然環境）
Stakeholder	ビジネスプロセス．企業や組織が責任を持つ単位
Service	人，サービス，および人と組織によって提供されるサービス
System	コンピュータシステム，ハードウェア，通信機器，半導体チップ
Software	プログラム（アプリケーションソフトウェア，OS，およびその他のソフトウェア），サイバー情報，データ，AI

すなわち，STAMP S&S の 5 階層モデルにスマートシティを構成する各要素を割り当て，CS 図でその相互関係を明確にし，CA を抽出することによって安全性を脅かすリスクが分析できるのではないかと仮説を立てた．

3. 安全性分析方法の検証実験

本実験では，自動運転車両を例にスマートシティにおける公共・民間サービスを中心としたシステムの安全性分析を行う．この一環で，公共・民間サービス間の連携によって自動運転車両へ間接的にもたらされる，安全性を損なうリスクを検証する．具体的な分析内容については，手順を追って説明する．

3.1. 実験の手順

3.1.1.　手順 1：スマートシティと自動運転車両の関係を構成する要素（Society, Stakeholder, Service, System, Software）を STAMP S&S モデルの考え方を用いて抽出する．この時点で要素の数や，その関係の複雑性が高過ぎると考えられる場合には，分析の前提条件を追加し，抽出した要素やその関係の中から除外できるものを検討する．

3.1.2.　手順 2：抽出した要素に対し，STAMP/STPA の手法を利用してリスク分析を実施する．

(1) Step0：(準備 1) アクシデント，ハザード，安全制約の識別

(a) 前提条件の整理

手順 1 で抽出した要素を踏まえた CS 図をベースに，どの領域を重点的に分析するか，どのような前提を置くかを整理．

(b) アクシデントハザード安全制約表の検討

重点的な分析対象となったコンポーネントに対し，発生してはならないアクシデントと，それを発生させるハザードを検討する．検討したハザードを発生させないために課すべき安全制約を導き出す．

(c) 分析対象のコンポーネントの抽出

分析対象となるコンポーネントを抽出し，それらの責務，CA，フィードバックを導き出す．

(2) Step0：(準備 2) CS 図の構築

安全性分析をしたい具体的な対象について，想定するシチュエーションを検討する．そして，そのシチュエーションにおいて登場する要素を抽出し，CS 図を作成する．

今回は，CS 図の作成に STAMP Workbench[8]を利用した．

(3) Step1：Unsafe Control Action（以降，UCA と表記）の抽出

ハザードにつながる CA を抽出.それぞれのコンポーネント間の CA に対し，過去のアクシデント事例に基づいた 4 つのガイドワードを用いて UCA を抽出する.

(4) Step2：UCA の発生要因（Hazard Causal Factor）（以降，HCF と表記）の特定

UCA を引き起こす HCF を，ドメインエキスパートでない人でも分析できるヒントワードを用いて特定する．HCF の特定後，どのようなシナリオで HCF が発生するかを文章にて表現する．このシナリオが安全性のリスクに該当する.

3.2. 実験結果

スマートシティにおいて多種多様な公共・民間サービス提供者（行政・サービス提供者・関係者）が存在する様を明らかにした．また，公共・民間サービスやそれらに関連するシステムが連携／関与する部分に着目して安全性分析を行うことで，消防から警察への救急車出動情報の連携不良で救急車と自動運転車両の事故に繋がるなど，スマートシティ特有のリスクを抽出できた.

手順 1 の結果，図 1 のように Society で 5 件，Stakeholder で 24 件，Service で 25 件の要素を抽出した.

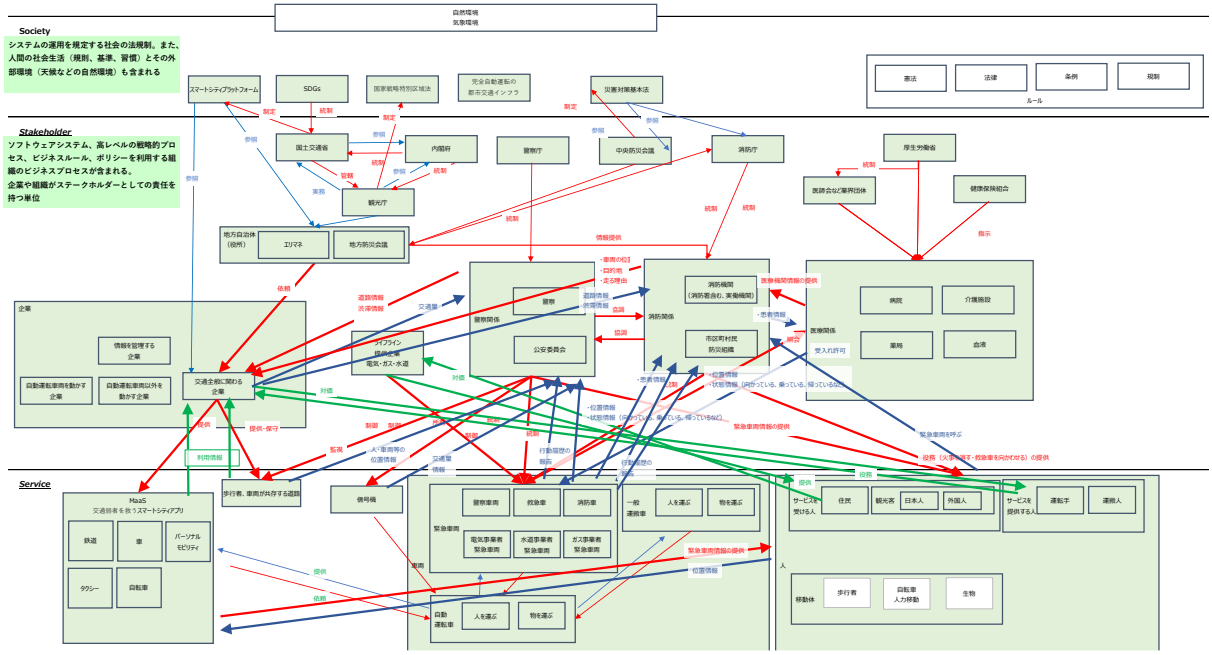

図 1　CS 図 整理前

(5 階層のうち Society，Stakeholder，Service 部分を抜粋．詳細は参考文献[9]を参照)

コンポーネント間の関係性を精緻に抽出すると,コンポーネント数が増えれば増えるほど関係性が複雑になるため，一度抽出した関係性のうち，特に人命に係る関係として，「救急車が，消防署から出発して，傷病者のいる現場（自動車専用ではないところ）まで向かい,傷病者を収容して病院に搬送し,再び消防署に戻る」というシチュエーションに絞り，救急車が自動運転車両と衝突したり，自動運転車両によって進路を阻害されたりするリスクを分析することとした.

次に，手順 2 の結果として以下の分析結果を得た.

Step0：準備 1 にて 5 層モデルを使用し，図 2 のように分析を進める上で必要な仮定や前提条件を 31 件整理した．スマートシティに関連する公共・民間サービス提供者，自動運転車両に関連した条件を多く整理した．整理した前提条件から公共・民間サービスやそれらに関連するシステムが連携／関与する部分に着目し，Stakeholder 間，Stakeholder-Service 間のリスク分析を行った.

ID	
Pre-1	人命・財産にかかわる問題を取り扱う
Pre-2	対策の検討はしない
Pre-3	Stakeholder間、 Stakeholder - Service間 の連携に関するリスクを分析する
Pre-4	鉄道はすべて高架上か、地下のどちらかしか走らない。
Pre-5	電柱はなく、ケーブルは地下埋め込みとする。
Pre-6	歩道・車道間の段差はすべてスロープになっているものとする。
Pre-7	自動車道、自転車道、歩道の3種類の道があるものとする。
Pre-8	自動車道、自転車道、歩道の3種類の道があるが、あらゆる場所でこれらを分離はできておらず、混在しているものとする。
Pre-9	イーパレットなどの多目的自動運転車両の運用に関係しないリスクは分析対象外とする。
Pre-10	物流用の輸送車両は地下を走行しているものとする。
Pre-11	ドローンが飛んでいる可能性がある。
Pre-12	スマートシティ内はどの領域でも情報通信網に接続できているものとする。
Pre-13	あらゆる利用設備において、電源切れ・燃料切れは考慮しないものとする。
Pre-14	情報通信網の通信帯域は十分に確保され、不足しないものとする。
Pre-15	車両の故障はありうるものとする。
Pre-16	車両単体のシステムとして、S/W不具合の可能性は考慮する。
Pre-17	地震、噴火、落雷、津波は発生しないものとする。
Pre-18	火事、交通事故、急病人などがあるものとする。
Pre-19	日本の標識を知らない人がいるものとする。
Pre-20	日本の道路交通法規を知らない人がいるものとする。
Pre-21	道路の経年劣化、破壊、陥没などはあるものとする。
Pre-22	車いすや、介助が必要な人がいるものとする。
Pre-23	利益・ビジネスの継続性に関することは検討しない（赤字なのでやらない、、、など）
Pre-24	道路交通法は、現在（2021年）の法律とする
Pre-25	ただし、多目的自動運転車両は運用OKとする
Pre-26	多目的自動運転車両の乗車率は50-80%とする
Pre-27	他の移動体（人・自動車など）は交通ルールを違反する場合がある
Pre-28	バス等の支払はキャッシュレスで行うものとする
Pre-29	車道と歩道の間は柵で隔てられている箇所も、そうでない箇所もある。
Pre-30	自動運転車両において、信号機情報は無線通信によって得られているものとする。
Pre-31	自動運転車両の制御はカメラベースとする。※Teslaの車両をイメージしています。

Pre-3	Stakeholder間、 Stakeholder - Service間 の連携に関するリスクを分析する

図 2　前提条件(詳細は参考文献[9]を参照)

Step0：準備 2 にて，前提条件から図 3 のように CS 図を作成.

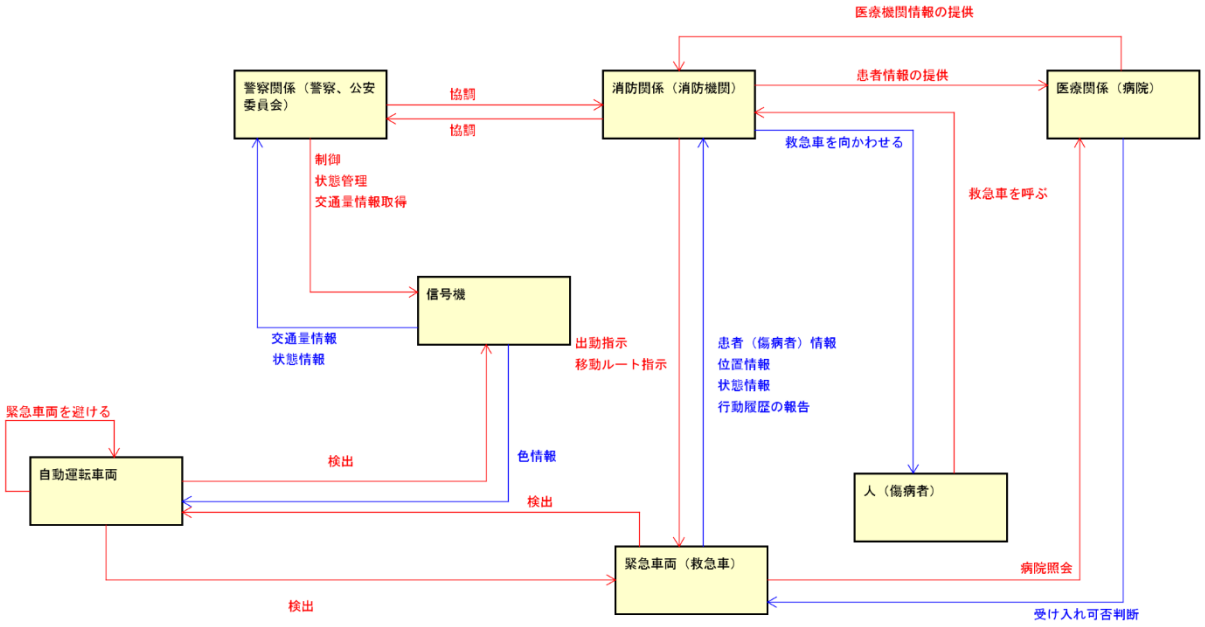

図 3　CS 図 整理後（詳細は参考文献[9]を参照）

Step1 にて，表 2 のように UCA を 32 件抽出.

表 2　UCA 表（詳細は参考文献[9]を参照）

No	CA	From	To	CAI提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
7	交通量情報取得	警察関係（警察、公安委員会）	信号機		(UCA7-N-1) 交通量情報を把握できなくなり、交通渋滞が解消されにくくなる [SC3]	(UCA7-P-1) 誤った交通量情報に基づいた信号制御がなされ、交通渋滞が発生しやすくなる。 [SC3]	-	-
8	協調	消防関係（消防機関）	警察関係（警察、公安委員会）	定期的?	(UCA8-N-1) 緊急車両(救急車)の出動情報(経路含む)が、警察関係へ伝達されず、信号が緊急用に切り替わらない [SC4][SC5][SC6]	(UCA8-P-1) 誤った緊急車両(救急車)の出動情報(経路含む)が、警察関係へ伝達される [SC4][SC5][SC6]	(UCA8-T-1) 救急車両(救急車)の出動情報が、警察関係へ遅れて伝達される [SC4][SC5][SC6]	-
9	患者情報の提供	消防関係（消防機関）	医療関係（病院）	救急車の出動要請を受けた場合にCAを発動する？（現地で救護者の状態を見てから救急隊員側からではないのか？）				
10	出動指示	消防関係（消防機関）	緊急車両（救急車）	救急車の出動要請を受けた場合にCAを発動する	(UCA10-N-1) 救急車に対して出動指示が発出されない	(UCA10-P-1) 誤った出動要請を受け、出動指示が発出される (UCA10-P-2) 出動要請が無いにもかかわらず、出動指示が発出される	(UCA10-T-1) 救急車に対する出動指示が遅れて発出される (UCA10-T-2) 救急車に対して、待機指示があるにも関わらず、出動指示が発出される	-
11	移動ルート指示	消防関係（消防機関）	緊急車両（救急車）	救急車の出動要請を受けた場合にCAを発動する	(UCA11-N-1) 救急車に対して目的地が指示されていない (UCA11-N-2) 救急車に対して移動ルートが指示されていない	(UCA11-P-1) 救急車に対して、誤った目的地が指示される (UCA11-P-2) 救急車に対して、誤った移動ルートが指示される (UCA11-P-3) 救急車に対して、渋滞している移動ルートが指示される (UCA11-P-4) 救急車に対して、通行できない移動ルートが指示される	(UCA11-T-1) 移動中の救急車に対して、通行止め情報が遅れて伝達される (UCA11-T-2) 移動中の救急車に対して、渋滞情報が遅れて伝達される (UCA11-T-3) 移動中の救急車に対して、解消されていない通行止めが、解消されたと伝達される (UCA11-T-4) 移動中の救急車に対して、解消されていない渋滞が、解消されたと伝達される	-

Step2 にて，表 3 のように HCF を 56 件特定.

表 3　HCF 表（詳細は参考文献[9]を参照）

ID	HCF	ヒントワード	シナリオ
HCF8-N-1-1	基準があいまいで、警察関係者へ緊急車両の出動情報が伝達されない	(1) Not Providing(指示がでない)	消防から警察への伝達方法、手段があいまいで、警察関係者へ緊急車両の出動情報が伝達されない。その結果、信号が緊急用に切り替わらない。
HCF8-N-1-2	伝達手段が故障し、警察関係者に緊急車両の出動情報が伝達されない	(5) 指示(口頭・電話・メール・FAXなど光、音、旗)	消防から警察への伝達手段が故障し、警察関係者へ緊急車両の出動情報が伝達されない。その結果、信号が緊急用に切り替わらない。

HCF を特定する際，STPA では発想を促す目的でヒントワードを用いる．STAMP Workbench には，分析対象に応じて選択可能なヒントワードのセットが複数用意されており，今回はその内の「An STPA Primer」を主として活用した．しかし，シナリオと整合性がとりにくいヒントワードもあったため，HCF によっては「IPA-（組織）対（組織）」を選択したものもある．この結果，HCF に繋がるシナリオ 58 件を特定することができた.

3.3. 考察

今回の分析では公共・民間サービス間の関係を分析することによって，直接的なコントローラ/被コントロールプロセス間だけでなく，間接的な影響による自動運転車両の衝突リスクを数多く検出することができた．例えば，消防と警察との連携不良により，交通管制が適切に行われず，その結果緊急車両と自動運転車両の衝突に繋がるリスクがある(表 3)，などである．分析によって HCF が特定できれば，それを引き起こすシナリオを防ぐ対策の検討に繋げられる.

また，STAMP S&S の 5 層モデルに基づいてスマートシティの階層をモデリングすることにより，公共・民間サービス提供者の関係性を精緻化することができた(図 1)．但し，コンポーネントが増えれば増えるほど関係性が複雑になるため，いったん精緻化した関係性のうち，どこから分析の詳細化を図るかについては，CS 図を眺めながらよく吟味する必要がある．加えて，CS 図を描く際に粒度の検討が難しく，分析者によってその粒度がばらつくと，結果も変わる可能性があるといった注意点もある.

分析対象とするコントロールから，過去のアクシデント事例に基づいたガイドワード，ヒントワードを用いて UCA の抽出，HCF の特定を実施した．その結果この分析手法は 5 層モデルの上位層・下位層に依らず活用が可能であり，分析の初心者であっても比較的容易に分析を進めることができることを確認できた．但し，ガイドワードのセットは一律ではなく，分析対象のドメインや階層によって適切な用語を利用することで，より精緻な分析ができると考えられる．今回の実験においても，担当者によってはデフォルトのヒントワードではなく，組織対組織のヒントワードを利用した者もいた．また，「早すぎる停止，長すぎる適用でハザード」のガイドワードに関しては，Society，Stakeholder，Service といった社会・環境・組織・サービス等へこのガイドワードを適用しても，有用な UCA を抽出

できなかった．この階層には別の観点を持つガイドワードが必要であると考える．

ヒントワードは HCF の特定で利用するが，ヒントワードを使うことによって，CS 図を作成する際，どのような CA があるべきか，といった気付きを得られることも分かった．システム設計レベルにおいても，H/W 機器間でどのような関係があるかを整理する際に有用であるなど，どの階層の分析でも活用できると考える．

分析の実施にあたって，対象の多さから分析を複数人で分担した．分担作業とする場合，UCF や HCF の表現に揺らぎが生じる恐れがある．前提条件の置き方や分析観点の設定，分析対象の絞り込みにおいては事前に十分認識合わせをしてから作業に取り掛かる必要がある．また，スマートシティではコンポーネントが多様になるため，多対多の関係性で分析しようとすると分析作業そのものが膨大となる．前提条件や分析対象の絞り込みを行い，最も防ぎたいハザードから順に分析を施すのが良いと考える．優先順位付けにはハザードの発生確率と発生時の影響度を勘案すると良いと考える．

4. 今後の課題

本稿では，分析の発散を防ぐ目的で，最初に分析対象を「自動運転車両へ間接的にもたらされる，安全性を損なうリスク」に限定している．さらに，STAMP S&S の活用によって得られた，自動運転車両を取巻く Stakeholder，Service のうち，緊急車両とその運用に関わる組織に対象を限定している．よって，実際にスマートシティ全体の開発を進める際は，こうした分析対象の限定を取り払い，広範な分析対象全てに対して安全性分析を実施する必要があると考える．

また，STAMP/STPA は安全性分析手法であり，明らかになった非安全性に対する対策を検討する手法は含まれていない．このため，スマートシティ全体に対して本実験と同様に安全性分析ができたとしても，公共・民間サービス提供者が妥当かつ一貫性のある対策を検討するための手段が必要と考えられる．しかし，Society，Stakeholder，Service の領域では，まだこうした手法の研究例はなく，対策立案に向けた新たな手法の検討が必要である．

Society の領域まで含めた分析はしなかった．これは，自動運転車両に関連して発生する事故を中心として考えたためであり，Society 領域まで汎化して考えると関係性が薄くなりすぎ，有意義な知見の獲得が見込みにくいと判断したためである．よって，STAMP/STPA の「UCA の抽出」および「HCF の特定」をする際に用いる各種ガイドワード・ヒントワードが，同領域に対する分析では有効でない可能性がある．今後の実験にて，それが明らかになった場合に，Society の領域に最適なガイドワード・ヒントワードを新たに検討する必要がある．

また，UCA の抽出，HCF の特定，およびハザードシナリオのいずれの分析フェーズにおいても，分析結果の文章構造は分析者の自由である．このため，大勢で分析を分担するような場合に，こうした文章構造に揺らぎが生まれ，分析の一貫性を維持しにくくなるという問題がある．分析結果の定型的な書き方を示すことで，誤解なく表現できるようにする工夫が必要であると考える．

5. まとめ

スマートシティにおける公共・民間サービスやシステムが連携／関与する部分について，本稿では自動運転車両に着目し，STAMP を活用して，安全性分析を行い，自動運転車両へ間接的にもたらされるリスクを検出することができた．

STAMP S&S の適用によって，スマートシティの開発にあたって考慮すべき，組織間の連携を明らかにすることができた．STAMP/STPA の CS 図を用いることで，複雑な構成要素間の関係を考慮して分析することができた．STAMP Workbench でガイドワード・ヒントワー

ドを利用することによって，最終的に構成要素間の連携に的を絞った安全性を損なうリスクを抽出することができた.

今後は 4 章で述べた課題に取り組んでいく予定である.

参考文献

[1] 内閣府・総務省・経済産業省・国土交通省 スマートシティ官民連携プラットフォーム，スマートシティガイドブック，https://www8.cao.go.jp/cstp/society5_0/smartcity/00_scguide_s.pdf，2021 年 12 月 31 日アクセス確認

[2] 官民連携プラットフォーム，https://www.mlit.go.jp/scpf/，2021 年 12 月 31 日アクセス確認

[3] 総務省，スマートシティセキュリティガイドライン(第 2.0 版)，https://www.soumu.go.jp/main_content/000757800.pdf，2022 年 1 月 1 日アクセス確認

[4] ISO：ISO/IEC Guide 51:2014，https://www.iso.org/standard/53940.html

[5] ナンシー・G・レブソン著，松原友夫 監訳・訳，片平真史，吉岡律夫，西康晴，青木美津江 訳：『セーフウェア　安全・安心なシステムとソフトウェアをめざして』，翔泳社，2009 年

[6] Kaneko, Tomoko; Yoshioka, Nobukazu; Sasaki, Ryoichi. “STAMP S&S: Layered Modeling for the complexed system in the society of AI/IoT”, 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2020, 2020.12.11-14

[7] 独立行政法人 情報処理推進機構(IPA),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～ Ver.1.0，https://www.ipa.go.jp/sec/reports/20160428.html，2021 年 12 月 31 日アクセス確認

[8] 独立行政法人 情報処理推進機構(IPA),STAMP Workbench Ver.2.0.0，https://www.ipa.go.jp/sec/tools/stamp_workbench.html，2021 年 12 月 31 日アクセス確認

[9] 日科技連ソフトウェア品質管理（SQiP）研究会第 38 年度研究コース 6，論文付録資料 スマートシティの安全性分析実験データ，2022. 2.25

[1] 内閣府，内閣府の政策　＞ 科学技術・イノベーション　＞ Society 5.0　＞ スマートシティ，https://www8.cao.go.jp/cstp/society5_0/smartcity/00_scguide_s.pdf，2021 年 12 月 31 日アクセス確認
[2] スマートシティ官民連携プラットフォーム，　https://www.mlit.go.jp/scpf/，2021 年 12 月 29 日アクセス確認
[3] 総務省，スマートシティセキュリティガイドライン(第 2.0 版)，https://www.soumu.go.jp/main_content/000757800.pdf，2022 年 1 月 1 日アクセス確認
[4] ISO：ISO/IEC Guide 51:2014，https://www.iso.org/standard/53940.html
[5] ナンシー・G・レブソン著，松原友夫 監訳・訳，片平真史，吉岡律夫,西康晴，青木美津江 訳：『セーフウェア　安全・安心なシステムとソフトウェアをめざして』，翔泳社，2009 年。
[6] Kaneko, Tomoko; Yoshioka, Nobukazu; Sasaki, Ryoichi. “STAMP S&S: Layered Modeling for the complexed system in the society of AI/IoT”, 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), 2020, 2020.12.11-14
[7] 独立行政法人 情報処理推進機構(IPA),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～ Ver.1.0,
https://www.ipa.go.jp/sec/reports/20160428.html，2021 年 12 月 29 日アクセス確認
[8] 独立行政法人 情報処理推進機構(IPA),STAMP Workbench Ver.2.0.0,
https://www.ipa.go.jp/sec/tools/stamp_workbench.html
[9] 日科技連ソフトウェア品質管理（SQiP）研究会第 38 年度研究コース 6，論文付録資料 スマートシティの安全性分析実験データ，2022. 2.25