一般車両システムへの ACC システム追加における STAMP/STPA 適用の試み

林 啓弘[1]　吉田 貴信[2]　井上 樹[2]　内田 功志[3]

受付日 2021 年 12 月 9 日，採録日 2021 年 12 月 9 日

「アダプティブ・クルーズコントロールシステム（ACC システム）」を題材に「Automotive SPICE プロセスアセスメントモデル／プロセス参照モデル」の「システムエンジニアリングプロセス群」に基づく MBSE の適用を行った．この際，ACC システムとベースとなる自動車システムとの協調動作において，「想定外の障害」や「想定外の想定外の障害」を発生させてはならないため，仕様として精度の高い ACC 規格に STAMP/STPA を組み合わせる形で安全面の検討を行った．本論文ではこの過程での気づきと課題を紹介する．

キーワード：STAMP/STPA, System of systems, ACC, MBSE

An attempt to apply STAMP/STPA in adding ACC system to general vehicle system

YOSHIHIRO HAYASHI[1]　TAKANOBU YOSHIDA[2]
TATSUKI INOUE[2]　ISASHI UCHIDA[3]

Received: December 9, 2021, Accepted: December 9, 2021

Abstract: We applied MBSE based on the "System Engineering Process Group" of the "Automotive SPICE Process Assessment Model/Process Reference Model" to the subject of "Adaptive Cruise Control System (ACC System)".In this study, since the cooperative behavior between the ACC system and the base automobile system must not cause "unexpected failures" or "Unknown unknown obstacles," the safety aspect was studied by combining the ACC standard, which is highly accurate as a specification, with STAMP/STPA. In this paper, we present our findings and challenges in this process.

Keywords: STAMP/STPA, System of systems, ACC, MBSE

1. はじめに

一般社団法人システムズエンジニアリング研究会（SERA）の MBSE ハンドブック[7][8]の例題で STAMP／STPA[1] [a)]を適用した．その際，STAMP／STPA の利活用について紹介されている各書籍を調べた．どれも扱っているドメインは大きく，そのドメインの「安全制約の識別」は難しいと感じていた．

次の SERA での取り組みは「アダプティブ・クルーズコントロールシステム（ACC システム）の規格[9]」を題材に「Automotive SPICE プロセスアセスメントモデル／プロセス参照モデル（AS）」の「システムエンジニアリングプロセス群（SYS）」を参照し，MBSE を適用する研究を行った．

1 アンリツ株式会社
Anritsu Corporation
2 株式会社豆蔵
Mamezou Co., Ltd.
3 一般社団法人システムズエンジニアリング研究会
Systems Engineering Research Association

a) STAMP/STPA
2012 年,マサチューセッツ工科大学（MIT）教授のナンシー・レブソン（Nancy Leveson）氏が提唱した

b) STAMP workbench
安全解析手法 STAMP の導入を容易にするモデリングツール．
「STAMP Workbench」は IPA の登録商標です［登録第 6121191 号]

この研究では，既存の自動車システムに ACC システムを追加するという想定で MBSE を適用しているため,システム間の想定外の障害が発生しないようにハザード／リスク分析する必要があるので STAMP／STPA の考え方を適用することにした．また,この規格を遵守することが安全性につながり，規格というドメインの大きさが理解しやすく，規格の文章や用語を使うことで,安全制約を識別しやすいと考えた．

2. STAMP／STPA メソッドの概要

(1) STAMP/STPA の基本的なステップ

STAMP/STPA の基本的なステップは，「①解析目的の定義」「②コントロールストラクチャーのモデル化」「③非安全なコントロールアクションの識別」「④損失シナリオの識別」という４つのステップから成る．「①解析目的の定義」では，「1.損失を識別する」「2.システムレベルのハザードを識別する」「3.システムレベルの安全制約を識別する」「4.ハザードの精密化」を行い，解析目的を明らかにする．「②コントロールストラクチャーのモデル化」では，当該システムを構成するコントローラを明らかにし,各コントローラ間に現れるコントロールアクションとフィードバックをモデル化する．「③非安全なコントロールアクションの識別」では，コントロール対象のプロセスに対するコントロールアクションが非安全なコントロールアクションとなった場合にどのようになるのかを検討する．その非安全なコントロールアクションは，４つのガイドワードを使ってハザードにつながるかどうかを検討する．「④損失シナリオの識別」では，洗い出した非安全なコントロールアクションが「なぜ起こるのか」あるいは「なぜコントロールアクションは不適切に実行される，または実行されずハザードに至るのか」を検討する．本研究で対象としているようなシステムオブシステムズでは構成するシステム間の関係，システムでは構成するコントローラ間の関係を明らかにする．各システムや各コントローラは当該正しい動作をしているが，コントロールするタイミングのずれにより，システム全体では誤った結果となるので，そのような状態になっていないことを検証する．

2.1 STAMP workbench [b]の活用

本研究では STAMP/STPA のためのツールとして, IPA で公開されている STAMP workbench を活用する．

STEP0　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」．

STEP0　準備２「コントロールストラクチャーの構築」．

STEP1 では，UCA(Unsafe Control Action)を抽出する．コントロールストラクチャー図中の各コントロールアクションについて，４つのガイドワード（７つの誤ったタイミング）を使って非安全なコントロールアクション(UCA)を設定する．その際，その UCA によって引き起こされることまでは書かないようにする．

STEP2 では，HCF(Hazard Causal Factor)の特定する．これらをもとに対策を検討する．

3. ACC 規格に対する STAMP／STPA の適用

本研究の STAMP／STPA の適用のアプローチは，つぎの通りとした．

① ACC システム規格からの安全制約の導出

[9]序文には「ACC システムの最終目的は，適切な方法で運転者を楽にし，支援することを目指したものであり，運転者の運転負荷の軽減のために，縦方向車両制御の部分的自動化を行うことである」とある．つまり規格の最終目的を満足するための安全制約が記載されている．そこで「3.2 STEP0 準備１「アクシデント，ハザード，安全制約の識別」」では，まず STAMP／STPA の手順に従って「アクシデント，ハザード，安全制約」の順で導出を行う．その後，ACC システム規格中の「安全制約」を拾い出して書き出していくことにした．(3.2 参照)

② システムエンジニアリングプロセスの活用

STEP2 の HCF の特定までは実施するが以降の「対策」の検討は，「システムエンジニアリングプロセス群（SYS）」へフィードバックし、システムエンジニアリングプロセスを活用する形の手順とした。

3.1 STEP0　準備１「前提条件の整理」

前提条件は ACC 規格 [9]の「適用範囲」「要求事項」から抽出した．「適用範囲」の「ACC システムは基本的には，連続的に走行できる円滑な交通条件下で自動車専用道路（自動車以外の車両及び歩行者の通行が禁止された道路）を走行しているとき，装置を搭載した車両への縦方向制御の提供」．「要求事項」では「基本的制御方針」「機能要件」から前提条件を抽出した．このとき，「前提条件」と判断できる文章を，できるだけ単一な文として拾い出した．

表 1 前提条件表

ID	前提条件
Pre-1	JIS D 0801：2012（ISO15622：2010）の範囲とする
Pre-2	ACCシステムは，基本的には，連続的に走行できる円滑な交通条件下で自動車専用道路（自動車以外の車両及び歩行者の通行が禁止された道路）を走行しているとき，装置を搭載した車両への縦方向制御の提供を目的とするもの。 （1．適用範囲）
Pre-3	ACCシステムは，前方障害物警報など他の機能と併用して機能拡張してもよい。 （1．適用範囲）
Pre-4	ACCシステムタイプは，能動的ブレーキ制御（不要：1、要：2）、手動のクラッチ操作（不要：b、要：a）のタイプ1 a、1 b、2 a、2 bの４つである。 （5.1 ＡＣＣ）
Pre-5	ACCシステムの曲線道路対応能力の種類は，つぎの４つの性能クラスである．（性能クラス１：曲線への対応能力は要求されない，性能クラス２：曲線半径500m以上，性能クラス３：曲線半径250m以上，性能クラス４：曲線半径125m以上）（5.2 曲線道路対応能力の種類）
Pre-6	当該車両速度は目標車両との車間距離を維持するか又は設定速度を維持するか、いずれか低い方でACCシステムによって自動的に制御しなければならない （6.1 基本的制御方針）
Pre-7	定常状態における車間距離は，システムが自動調整するか，または運転者が調整可能でなければならない （6.1 基本的制御方針）
Pre-8	２台以上の前方車両が存在する場合は，追従すべき車両を自動的に選択しなければならない （6.1 基本的制御方針）
Pre-9	自己診断の後，手動及び／又は自動で遷移。手動による遷移とは，スイッチによってACC機能を待機状態又は停止状態にすることを意味する。故障時は，自動停止してもよい （6.1 基本的制御方針）
Pre-10	ACCシステムは静止目標物に反応しないように設計されることは要求事項ではない （6.2.3 静止目標物）

3.2 STEP0　準備１「アクシデント(A)，ハザード(H)，安全制約(SC)の識別」

ACC 規格の序文に「ACC システムの主な機能は，次の情報を使用して車両の走行速度を前方車両に適応するよう制御するものである」とある．つまり「車両への縦方向制御」であるため，「アクシデント(An)」は「(A1)自車が前方車両に衝突する」「(A2)他車（後続車）が自車に衝突する」とし

た.「ハザード(Hn)」は，アクシデントが発生する前の条件と考え，「衝突」(A1)に至る前の「(H1) 前方車両に近づき過ぎる」「(H2)車両コントロールを喪失する」とした. また「(A2)他車が自車に衝突する」は，他車の前で，喪失をしていないまでも「(H3)自車が予想外の動きになる」とした．これらのハザードに対する「安全制約(SCn)」は「(SC1)前方車両に近づき過ぎてはならない」「(SC2)車両コントロールが喪失してはならない」「(SC3)車両が予想外の動きになってはならない」とした.

表 2 アクシデント/ハザード/安全制約表

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	前方車両に衝突する	H1	前方車両に近づき過ぎる	SC1	前方車両に近づき過ぎてはならない
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC2	車両コントロールが喪失してはならない
A2	他車が自車に衝突する	H3	車両が予想外の動きになる	SC3	車両が予想外の動きになってはならない

ここで，さらに ACC 規格[9]「要求事項」の「6.2 機能要件」「6.3 基本的運転者インタフェース及び運転者による操作介入機能」から安全制約を抽出した.
その一部を紹介する.
・「追従制御と速度制御は自動的に行わなければならない（[9]6.2.1　制御モード)」
・「当該車両の速度を決定できなければならない（[9]6.2.2 当該車両の速度)」
・「過渡状態においては，車間距離は一時的に最小車間距離未満に接近しても差し支えない．そのような状況が発生した場合は，システムは車間距離が要求車間距離に戻るように調節しなければならない（[9]6.2.4　追従能力　6.2.4.1)」
・「前方車両と当該車両間との車間距離を測定しなければならない（[9]6.2.4　追従能力　6.2.4.2)」
「運転者が希望する設定車速を選定できる手段を備えていなければならない．([9]6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.1)」
「運転者によって発生されたブレーキカ要求が，ACC システムが発生したブレーキカより大きいときは，運転者によるブレーキ操作によって ACC の機能は作動を休止（ACC 待機状態に遷移）しなければならない ([9]6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.2)」

表 3 アクシデント/ハザード/ ACC 規格安全制約表の一部

アクシデントID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC10	車両コントロールを喪失してはならない
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC11	運転者が希望する設定車速を選定できる手段を備えていなければならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.1）
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC12	運転者によって発生されたブレーキカ要求が、ACCシステムが発生したブレーキカより大きいとき、運転者によるブレーキ操作によってACCの機能は作動を休止（ACC待機状態に遷移）しなければならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.2）
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC13	ACCシステムが自動的にブレーキをかけているときであっても、運転者のブレーキペダルによる介入に対して、一時的なブレーキカの大幅な減少があってはならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.2）
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC14	ACCシステムは、運転環境（悪天候など）に対応するため、運転者が行う操作なしに自動的に車間距離を調節してもよい。しかし、その調節した車間距離は、運転者の選定した最小車間距離以下になってはならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.2）
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC15	サブシステムが故障した場合に必要な動作は、表 4 及び表 5 のとおりでなければならない。（6.6 故障時の動作）
A1	前方車両に衝突する	H2	車両コントロールが喪失する	SC16	ACCシステムの故障は、イグニションのオン・オフ、又はACCシステムの起動・停止のいずれかによって実行される自己診断が問題なく完了するまで禁止されなければならない。（6.6 故障時の動作）
A2	他車が自車に衝突する	H3	車両が予想外の動きになる	SC17	車両が予想外の動きになってはならない
A2	他車が自車に衝突する	H3	車両が予想外の動きになる	SC18	ブレーキの自動作動（ACCタイプ2システム）で、アンチロック装置（ABS）が作動するよりも前に、車輪をロックさせてはならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.3）
A2	他車が自車に衝突する	H3	車両が予想外の動きになる	SC19	ACCシステムによる自動加力制御は、トラクション制御の作動するより高精度の速度なライドスリップを生じさせてはならない。（6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.4）

3.3 STEP0　準備２「コントロールストラクチャーの構築」

この ACC 規格には, [9]図 1(ACC システムの機能要素)と[9]図 6(縦方向制御の作動装置)の２つの図から図 3 のコントロールストラクチャーを構築した．[9]図 1 中の「〇〇検知」は，当該〇〇検知システム（コントローラ）と命名した．「ACC システム」「縦方向制御の作動システム」「ドライバー」「ドライバー情報表示システム」「当該車両の挙動検知システム」「前方車両とその車間距離の検知システム」「エンジン」「トランスミッション」「ブレーキ」「クラッチ」「スロットル」のコントローラを特定した．このコントローラ間のコントロールアクションは「〇〇制御情報」，フィードバックは「〇〇状態情報」と命名した．ACC システムには，表 4 ([9]表 2(ACC システムタイプによる分類))の通り，４つのタイプがある．図 3 コントロールストラクチャーには，４つのタイプとも含まれており，分析する際は不便である．よって，ここでは，「手動のクラッチ操作・不要」「能動的ブレーキ制御・要」のタイプ 2B を選択して図 4 のコントロールストラクチャーを構築した.

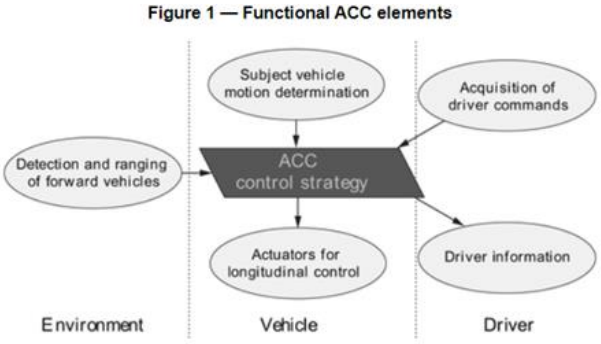


図 1　[9]図 1 ACC システムの機能要素

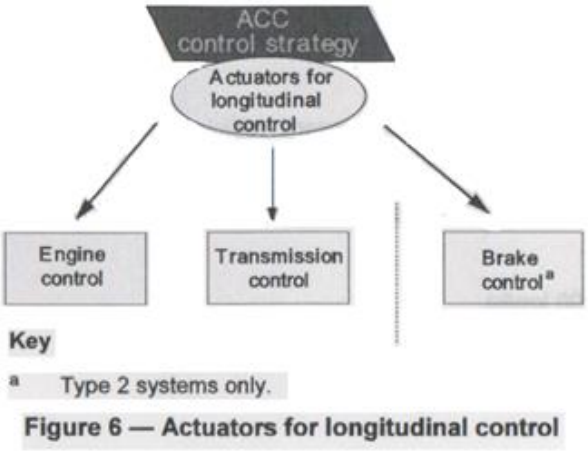


図 2 [9]図 6 縦方向制御の作動装置

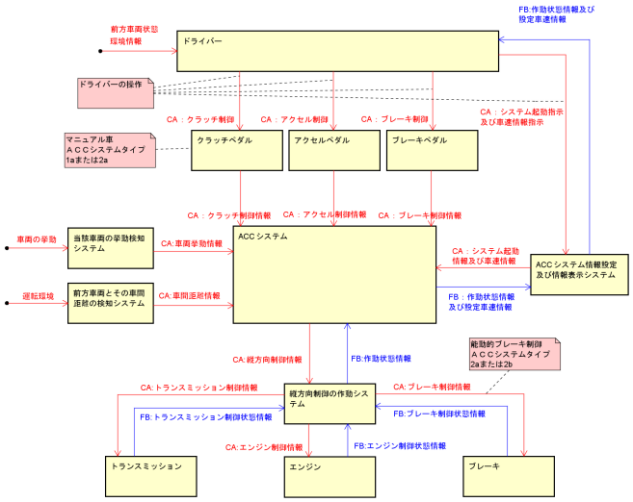


図 3 コントロールストラクチャー

3.3.1 ACC 規格の登場人物

[9]6.3.1.4 に「出力要求でエンジンの出力操作（例えばスロットル操作）を行う」とあるので，エンジンのコントローラにスロットル制御が含まれるとした．

ドライバーが操作するクラッチペダル，アクセルペダル，ブレーキペダルをモデルの上部へもってきた．

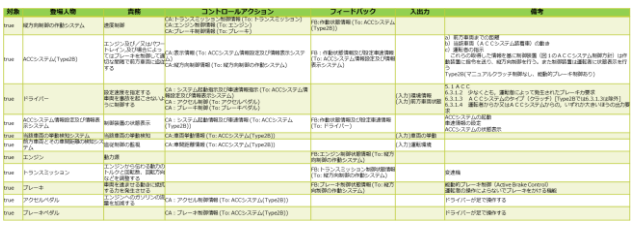
「クラッチの有無」と「ACC システムによるブレーキ制御有無」の組み合わせは 4 タイプある．この研究ではコントロールストラクチャー図の構成をタイプ 2b の一つに絞る．

表 4 [9]表 2-ACC システムタイプによる分類

表2-ACCシステムタイプによる分類		
タイプ	手動のクラッチ操作必要	能動的ブレーキ制御
1a	要	不要
1b	不要	不要
2a	要	要
2b	不要	要

登場人物は，規格を構成するモノを記載する．責務は，規格の文章（用語）を使って記載する．コントロールアクションは対象を制御する動作指示なので，当該コントロール，当該コマンドあるいは当該制御情報と命名することにした．フィードバックは，当該フィードバック，当該レスポンスあるいは当該状態情報と命名することにした．「備考」欄に規格と関連する内容を記載し,トレーサビリティを確保した．

表 5 コンポーネント抽出表(タイプ 2B)



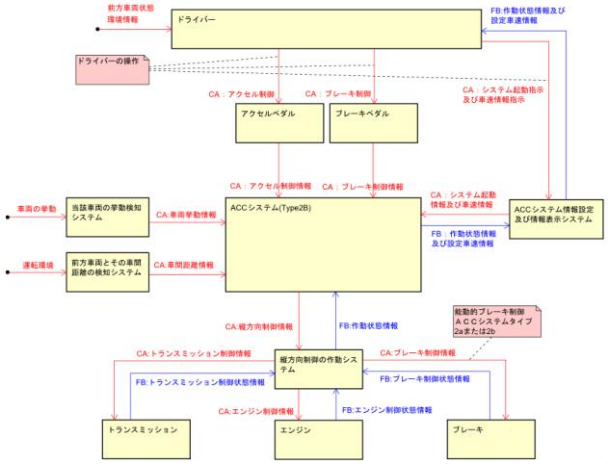


図 4 コントロールストラクチャー(タイプ 2B)

3.4 STEP1 UCA(Unsafe Control Action)の抽出

コントロールストラクチャー図中の各コントロールアクションについて，４つのガイドワード（７つの誤ったタイミング）を使って非安全なコントロールアクション(UCA)を導出する．その際，その UCA によって引き起こされることまでは書かないようにする．

表 6 非安全なコントロールアクション(UCA)の抽出表

3.5 STEP2 HCF(Hazard Causal Factor)の特定

個々の UCA に注目しヒントワードを活用して HCF を特定する．ここでは「CA:縦方向制御情報」コントロールアクションに注目したコントロールループで UCA を意識し，発想し定義した．図 5 は「CA:縦方向制御情報」コントロールアクションに注目したコントロールループの図になる．

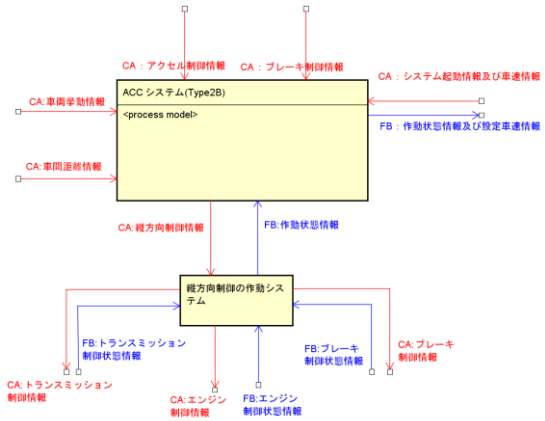


図 5 コントロールループ（CA:縦方向制御情報）

ここでは，表 6 の UCA1-P-1 に注目しヒントワードを活用して導出した HCF を示す.
(UCA1-P-1) は「UCA : 前走車に近づきすぎた時,加速か速度維持の指示を与える」である.

表 7 HCF(UCA1-P-1)

ID	HCF	ヒントワード	シナリオ
HCF1-P-1-1	HCF : 車両挙動情報からACCが正しい縦方向制御情報を作れない	(5) 不適切か欠けているフィードバック、フィードバックの遅れ	車両挙動情報が実際と異なる値のため、ACCは正しい縦方向制御情報を作れない。
HCF1-P-1-2	HCF : 車間距離情報からACCが正しい縦方向制御情報を作れない	(5) 不適切か欠けているフィードバック、フィードバックの遅れ	車間距離情報が実際と異なる値のため、ACCは正しい縦方向制御情報を作れない。
HCF1-P-1-3	HCF : 正しい車間距離情報が伝わってこない	(3) プロセスモデルの矛盾、不完全、不正確	前走車に近づきすぎているにも関わらず、前走車との距離が遠いという車間距離情報がACCに与えられ、ACCは追従しようとする。結果、ACCは加速指示を送り、前走車に近づく。
HCF1-P-1-4	HCF : ACCが正しい縦方向制御情報を作れない	(2) コントロールアルゴリズムの生成の欠陥、プロセス変更、不正確な修正や遅応	ACCに正しい情報が与えられるが、すべての情報を処理できず、正しい縦方向制御情報を作れない。 ACCに正しい情報が与えられるが、ドライバーとセンサーの情報を適切に処理することができず、正しい縦方向制御情報を作れない。

STAMP/STPA の「④損失シナリオの識別」ステップでは,HCF までとして,HCF に対する対策の検討はシステムエンジニアリングプロセスで検討する.

4. STAMP workbench の成果物と規格との連携

4.1 解析目的の定義

① 表 1「前提条件」は規格の「適用範囲」と「要求事項」から「前提条件」と判断できる文章を，できるだけ単一な文として拾い出す.

② 表 3「アクシデントハザード安全制約表」の「安全制約」は規格の「要求事項」から導出する.

4.2 コントロールストラクチャーのモデル化

① 表 5 コンポーネント抽出表の登場人物は, 規格を構成するモノを記載する.

② 表 5 コンポーネント抽出表の責務は, 規格の言葉を使って記載する.

③ 表 5 コンポーネント抽出表の「備考」欄に規格と関連する内容を記載し,トレーサビリティを確保する.

4.3 非安全なコントロールアクションの識別

① 非安全なコントロールアクション(UCA)を導出する. その際，その UCA によって引き起こされることまでは書かないようにする．つまり,非安全なコントロールアクション名とする.

4.4 損失シナリオの識別

① HCF でも規格を意識して状態,状況を意識してシナリオを導出する

② 対策表の対策は規約遵守となるように発想することになるが,本研究ではシステムズエンジニアリングで実施する.

5. 規格からの安全制約の導出とサブハザード

前項「3.2 STEP0 準備 1 「アクシデント，ハザード，安全制約の識別」」で，ACC 規格から安全制約を導出した．これら導出した安全制約の文は具体的な表現（具象）となるので，ハザードも抽象度を下げたサブハザードを考慮することにした.

「(H1) 前方車両に近づき過ぎる」のサブハザードは H1-n,
「(H2)車両コントロールを喪失」のサブハザードは H2-n,
「(H3)自車が予想外の動きになる」のサブハザードは H3-n と分類した.表 8 はサブハザードの抜粋を示す。

表 8 ACC 規格の安全制約とサブハザード

サブハザードID	サブハザード	安全制約ID	安全制約
H1-1	追従制御と速度制御は自動的に行われない	SC1-1	追従制御と速度制御は自動的に行わなければならない（6.2.1 制御モード）
H1-2	当該車両の速度を決定できない	SC1-2	当該車両の速度を決定できなければならない （6.2.2 当該車両の速度）
H1-3	過渡状態においては，車間距離は一時的に最小車間距離未満に接近した場合でも，システムは車間距離が要求車間距離に戻るように調節できない	SC1-3	過渡状態においては，車間距離は一時的に最小車間距離未満に接近しても走し支えない。そのような状況が発生した場合は，システムは車間距離が要求車間距離に戻るように調節しなければならない （6.2.4 追従能力 6.2.4.1）
H1-4	前方車両と当該車両間との車間距離を測定できない	SC1-4	前方車両と当該車両間との車間距離を測定しなければならない （6.2.4 追従能力 6.2.4.2）
H2-1	運転者が希望する設定車速を選定できない	SC2-1	運転者が希望する設定車速を選定できる手段を備えていなければならない。 （6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.1）
H2-2	運転者によって発生されたブレーキカ要求が、ACCシステムが発生したブレーキカより大きいときは、運転者によるブレーキ操作によってACCの機能は作動を休止（ACC待機状態に遷移）できない	SC2-2	運転者によって発生されたブレーキカ要求が、ACCシステムが発生したブレーキカより大きいときは、運転者によるブレーキ操作によってACCの機能は作動を休止（ACC待機状態に遷移）しなければならない （6.3 基本的運転者インタフェース及び運転者による操作介入機能 6.3.1.2）

6. 考察

① ACC システム規格からの安全制約の導出
この作業は「ハザードや安全制約の精密化」になった. ただしハザードから安全制約を導出したのではなく,規格から安全制約の文を導出することができた．しかし規格にはつぎのように具体的すぎるものもあった.
[9]6.2.4.1 一般「1.5 秒～2.2 秒までの範囲内の車間時間γを最低限一つ設定できなければならない」
STAMP/STPA では，具体的表現ではなく，上位概念で捉えるので,「車間時間γを最低限一つ設定できなければならない」と具体的数値を外して安全制約とした方が良いと考える.

② HCF 対策の検討
STEP2 で HCF までは実施するが「対策」の検討は,「システムエンジニアリングプロセス群（SYS)」へフィードバックすることで十分であると考えた。引き続き STAMP/STPA で対策の方針を立てても良いが,システムエンジニアリングプロセスで論理アーキテクチャ,物理アーキテクチャを考慮して HCF の対策を立てた方が確実で効率的であることが分かった.よって,このアプローチでも問題ないと考える.

6.1 当該規格に隣り合う規格や機能と連携する安全性分析

本規格は,「高度道路交通システムーアダプティブ・クルーズコントロールシステム(ＡＣＣ)ー性能要求事項及び試験手順 JIS D 0801：2012（ISO15622：2010)」であった．この規格ができたのが，JIS では 2012 年である．この前後に，この規格に隣り合う規格，つまりシステムとして影響がある規格がある．これらの規格もシステムとして扱い，システムの連携を STAMP/STPA で評価する必要がある．つぎにこれら規格を紹介する.

[10]WG14 走行制御（Vehicle/Roadway Warning and Control Systems）より

・全車速域車間距離制御システム（FSRA） D 0807：2011 (ISO

22179：2009)

ACC の追従機能を，停止制御まで拡張したシステム

・協調型車間距離制御システム（CACC）ISO 20035:2019

車車間通信の技術を用いて前方車両との車間を維持し，更に複数の車両やインフラとの通信も行う

・その他

車線維持支援システム（レーンキープアシスト（LKAS））ISO 22735:2021

7. おわりに

ここでは既存の自動車システムに規格 ACC システムの追加について検証したが，現行システムに新たなシステム（規格）を取り込む際に STAMP/STPA を適用しシステム間のコントロールループと UCA を想定することで，「想定外の想定外の障害」を発想し,AS の「システムエンジニアリングプロセス群（SYS)」のシステム要件分析（SYS.2）へ早期にアクシデント(A)，ハザード(H)，安全制約(SC),HCF をフィードバックすることができることが分かった.

規格からアクシデント，ハザード，安全制約を導出できる．導出した安全制約は具体的な表現（具象）となるので，ハザードだけで分類するだけでなく，チャンクダウン（抽象度を下げ具体化）したサブハザードを考慮して分類することが必要であるということが分かった．しかし，このサブハザードは細かすぎるので「システムエンジニアリングプロセス群（SYS)」では利用せず.「ソフトウェアエンジニアリングプロセス群 (SWE)」で利用することになると考える.

他システムでも規格に基づいた製品開発を行う際に，STAMP/STPA で当該規格の安全性解析を適用することで早期にシステム要件分析に非機能要件としてフィードバックできると考える.

謝辞　本論文の作成にご協力頂いた皆様に，謹んで感謝の意を表する.

参考文献

[1] “STPA HANDBOOK 日本語版 Ver.0.2”. hhttp://psas.scripts.mit.edu/home/get_file2.php?name=STPA_handbook_japanese.pdf, (参照 2018-12-02).

[2] “はじめての STAMP/STPA”. http://www.ipa.go.jp/sec/reports/20160428.html, (参照 2018-12-02).

[3] “はじめての STAMP/STPA（実践編）“. http://www.ipa.go.jp/sec/reports/20170324.html, (参照 2018-12-02).

[4] Extending STPA をベースとしたプロセスモデル抽出の実践 2018 年 12 月　日本ユニシス株式会社　総合技術研究所 福島祐子氏

[5] セキュアな機能の実現を目指す STPA-Sec の試行 ～プロセスモデルを中心とした分析～ 2019 年 12 月 日本ユニシス株式会社 福島祐子氏

[6] STAMP／STPA の理論と実践《入門編》 2016 年 12 月 14 日 HASHIMOTO SOFTWARE CONSULTING INTERNATIONAL Inc.　Takanari HASHIMOTO

[7] MBSE ハンドブック 事例による MBSE＋安全＋システムアシュアランスの実践　2017 年 11 月 10 日　一般社団法人システムズエンジニアリング研究会（SERA）　MBSE ハンドブック作成委員会

[8] MBSE ハンドブック Ver2.0 事例による MBSE＋安全＋システムアシュアランスの実践　2019 年 6 月 14 日　一般社団法人システムズエンジニアリング研究会（SERA）MBSE ハンドブック作成委員会

[9] 高度道路交通システムーアダプティブ・クルーズコントロールシステム(ＡＣＣ)ー性能要求事項及び試験手順　JIS D 0801：2012（ISO15622：2010）

[10] 公益社団法人自動車技術会 ワーキンググループの活動概要 WG14 走行制御 https://www.jsae.or.jp/01info/org/its/tc204_wg14.pdf

著者紹介

林 啓弘
アンリツ株式会社
エンジニアリング本部
業務支援部

SERA 個人会員

吉田 貴信
株式会社豆蔵
エンジニアリングソリューション事業部

SERA 会員

井上 樹
株式会社豆蔵　CTO

一般社団法人システムズエンジニアリング研究会　理事

内田 功志
一般社団法人システムズエンジニアリング研究会
代表理事長