付録1：用語集

■STAMP(Systems Theoretic Accident Model and Processes)
システムの安全性は構成要素の相互作用から創発されるものであり、個々の要素を分割して分析するべきではない、という考えの下、システムの中で安全のための制御を行う要素（コントローラー：Controller）と制御される要素（被コントロールプロセス：Controlled Process）の相互作用が働かないことによってアクシデントは起きるというモデルのこと。

■STPA(System-Theoretic Process Analysis)
STAMPによるアクシデントモデルを基に、システムのハザード分析を行う安全解析手法のこと。

■STRIDE
システムに対するセキュリティ上の脅威として、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つに分類した脅威モデルのこと。

■CA(Control Action)
STAMP分析での、コントローラーから被コントロールプロセスへの必要な制御指示のこと。

■CS(Control Structure)
システムにおいて、安全制約の実現に関係するコンポーネント、および、コンポーネント間の相互作用を分析し作成した、制御構造図のこと。

■UCA(Unsafe Control Action)
CSから、安全制約の実行に必要なコントローラーによるCAを識別し、4種類のガイドワードを適用して抽出された、ハザードにつながる非安全なCAのこと。

■SC(Safety Constraints)
あるアクシデントに対するハザードが発生しないための安全制約のこと。

■HCF(Hazard Causal Factor)
UCA毎に、関係するコントローラーと被コントロールプロセスを識別して、コントロールループ図を作成し、ガイドワードを適用して特定するハザード要因のこと。

■GSN(Goal Structuring Notation)
システムが達成すべき目的や性質について、その達成を導く方法・思考を可視化する際に用いる記法のこと。

付録2：STAMP/STPAの手順

付録3：質問紙

SQiP研究会 2018年度
演習コースⅢ（セーフティ＆セキュリティ開発）

Q1. STAMP/STPAを知っていますか？
※　他者に説明を求められた時に、説明ができる場合に「はい」。
□　はい　□　いいえ

Q2. 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。
□　はい　□　いいえ

Q3. 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のセーフティならびにセキュリティ上のリスクを5つ以上思いつく限り多くあげてください。
※　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。

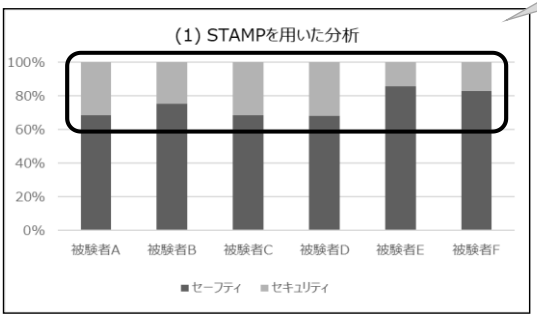
Q4. Q3であげたリスクに対する対策をお答えください。

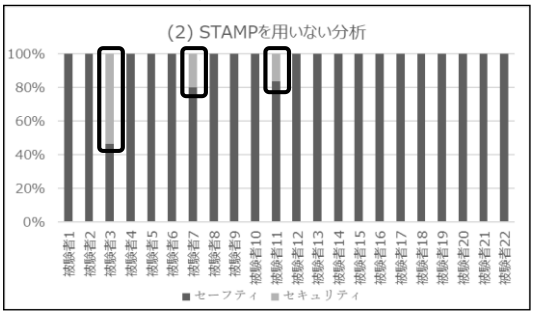
付録4：図3.3-1　実験結果一覧

抽出したリスクのセーフティ/セキュリティの割合

全員がある程度の割合でセキュ

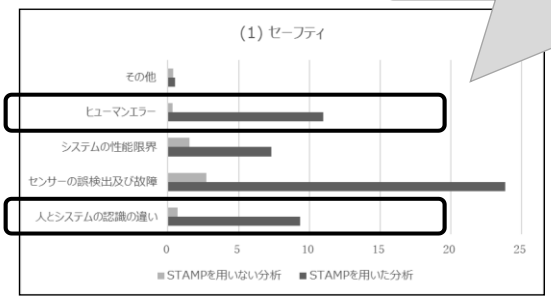
セキュリティ・リスクが抽出しているのは少数

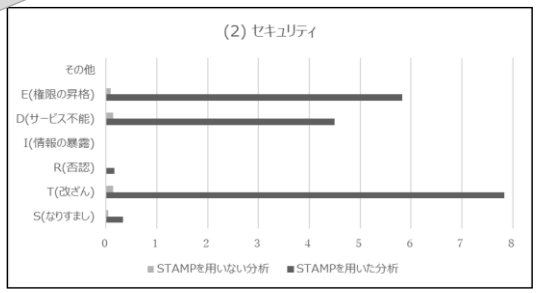




被験者1人当たりのリスク件数の内訳

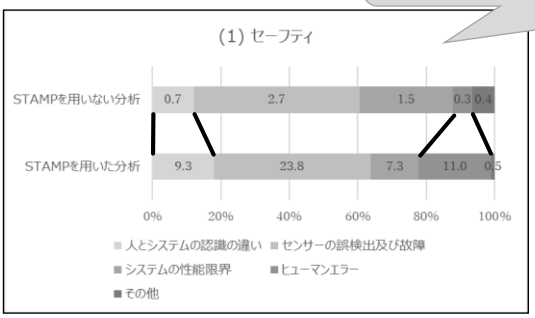
STAMPを用いた分析の方が，その他を除いた全ての項目でリスク抽出数が多く，
特にヒューマンエラーや人とシステムの認識の違いのリスクを非常に多く挙げている

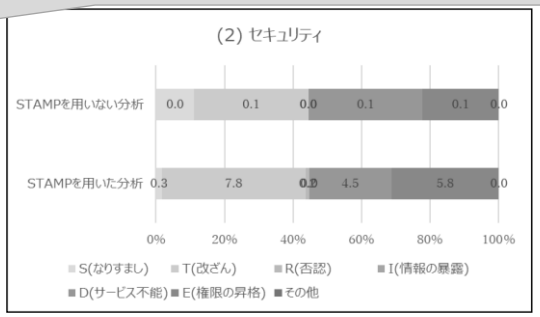




被験者1人当たりのリスクの割合

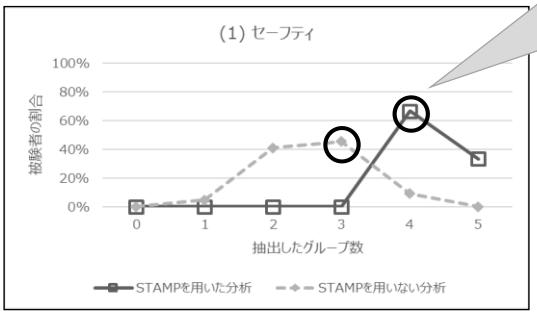
STAMPを用いた分析の方が，ヒューマンエラーや人とシステムの認識の違いの比率が高い．全体的にリスク抽出数が多いので，特にヒューマンエラーや人とシステムの認識の違いのリスクを多く抽出していると言える

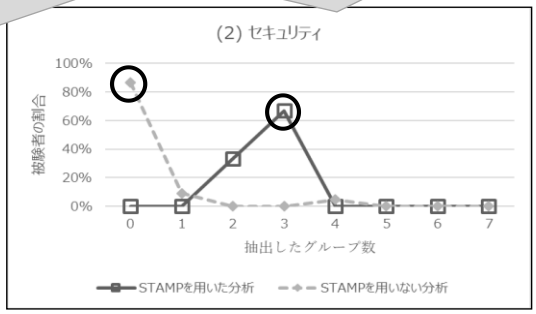




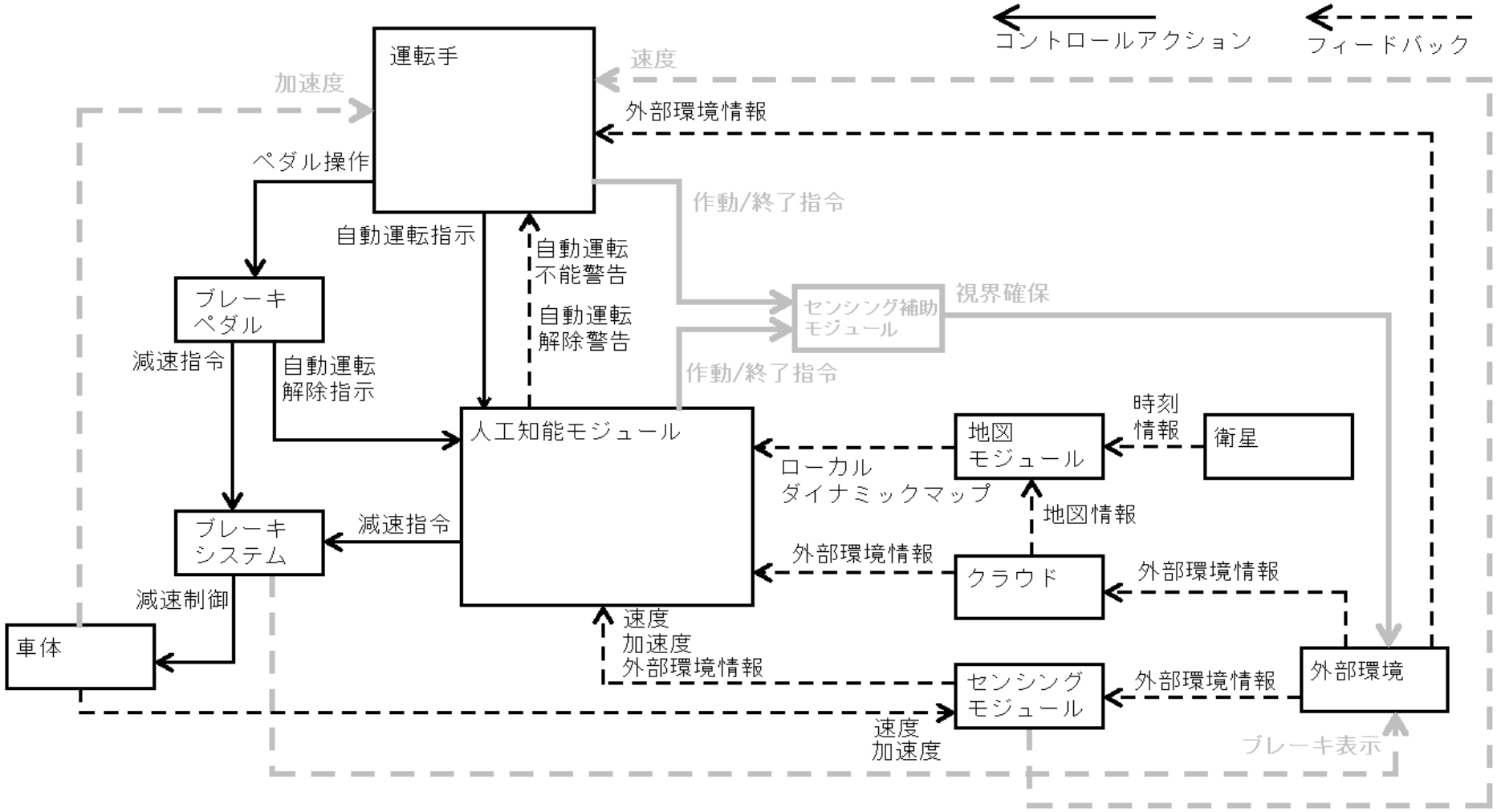
抽出したグループ数ごとの被験者の割合

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，STAMPを用いた分析が，多くのグループでリスクを検出している





付録5：図4-1　CS図


コントロールアクション
フィードバック
運転手
速度
加速度
外部環境情報
ペダル操作
作動/終了指令
自動運転指示
自動運転
不能警告
自動運転
解除警告
ブレーキ
ペダル
センシング補助
モジュール
視界確保
減速指令
自動運転
解除指示
作動/終了指令
時刻
情報
人工知能モジュール
地図
モジュール
衛星
ローカル
ダイナミックマップ
地図情報
ブレーキ
システム
減速指令
外部環境情報
クラウド
外部環境情報
減速制御
速度
加速度
外部環境情報
車体
センシング
モジュール
外部環境情報
外部環境
速度
加速度
ブレーキ表示

付録6：表4-1　UCAの抽出結果

No	CA	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	運転手によるブレーキペダル操作	(UCA1-N) 自動運転不能時に運転手がペダルを踏まないと減速指令が出ず外部環境と衝突する. [SC1][SC2]	(UCA1-P) 自動運転中に意図しないペダル操作が発生し，自動運転が解除されブレーキが作動しなくなり外部環境と衝突する [SC1][SC2]	(UCA1-T) 非自動運転時にペダル操作が遅すぎる場合，減速指令が遅れ，外部環境と衝突する [SC1]	(UCA1-D) 非自動運転時にペダルを踏む時間が不足すると，減速指令が不足して外部環境と衝突する [SC1] ブレーキを踏む時間が長すぎると必要以上に減速し，渋滞の原因となる
2	ブレーキペダル操作によるブレーキシステムへの減速指令	(UCA2-N) 減速指令がないと，そのまま外部環境と衝突する [SC1]	(UCA2-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	(UCA2-T) 運転手のペダル操作に対して減速指令が遅すぎた場合，外部環境との適切な距離が保てず衝突する [SC1]	(UCA2-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1] 必要な減速が完了した後も減速指令を出し続け，加速が困難になる
3	ブレーキシステムによる車体の減速制御	(UCA3-N) 減速制御が行われないと，そのまま走行方向の外部環境と衝突する [SC1][SC2]	減速指令を受けてないのに減速が発生し，交通渋滞となる (UCA3-P) 不必要に強い減速が生じ，後方車両から追突される [SC3]	(UCA3-T-1) 減速指令に対して減速が遅すぎる場合，外部環境との適切な距離が保てず衝突する [SC1] (UCA3-T-2) 外部へのブレーキ表示前に減速を始め，後方の車両から衝突される [SC3]	(UCA3-D) 減速指令が終了する前に減速が終了し，外部環境との適切な距離が保てず衝突する [SC1] 減速指令が終了した後も減速制御を行い，加速が困難になる
4	運転手による人工知能モジュールへの自動運転指示	自動運転指示が行われないと，自動運転が開始されない	意図しない自動運転が開始され，運転手が混乱する	-	-
5	人工知能モジュールによるブレーキシステムへの減速指令	(UCA5-N 自動運転時に人工知能が減速指令を出さないとそのまま外部環境と衝突する. [SC1]	(UCA5-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	(UCA5-T) 減速指令が遅れた場合，前方の外部環境との適切な距離が保てず衝突する [SC1]	(UCA5-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1] 必要な減速が完了した後も減速指令を出し続け，加速が困難になる
6	ブレーキペダル操作による人工知能モジュールへの自動運転解除指示	自動運転の解除指示が行われないと，運転手がブレーキ操作をすることができない	(UCA6-P) 意図せず自動運転が解除され，衝突回避のためのブレーキ指令をだすことができない [SC1][SC2]	-	-
7	人工知能モジュールによるセンシング補助モジュールの作動/終了指令	視界確保無しで人工知能モジュールが外部環境を認識できない場合，作動指令がなされないと人工知能による自動運転が不可能となる	不要な視界確保動作が行われ，部品の寿命が縮む	-	-
8	運転手によるセンシング補助モジュールの作動/終了指令	(UCA8-N) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合に作動指令が出せないと，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1]	不要な視界確保動作が行われ，部品の寿命が縮む (UCA8-P) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合で，運転手の視界確保可能な状況となる前に終了指令が出されると，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1][SC2]	-	-
9	センシング補助モジュールによる外部環境の視界確保	(UCA9-N) 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]	(UCA9-P) 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]	(UCA9-T) 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]	-

付録7：表4-2：HCFの抽出結果 - UCA1に対するHCF

	HCF																				
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA1-D) 非自動運転時にペダルを踏む時間が不足すると，減速指令が不足して外部環境と衝突する [SC1]	-	運転手が雨による路面摩擦の低下を考慮せずにブレーキ操作をする	運転手が前方の車両の減速度が増加していることに気付かない	-	-	-	-	運転手がペダルを踏んではいるが，ブレーキのあそび部分しか踏んでいない	-	-	-	-	-	-	-	-	運転手の意識をそらし，ブレーキから足を離すようにしむける	-	-	-	-
(UCA1-N) 自動運転不能時に運転手がペダルを踏まないと減速指令が出ず外部環境と衝突する. [SC1][SC2]	悪天候など外部環境の情報が鮮明でなく，運転手が危険察知をしない	運転手が十分な操作知識を持っておらず，ペダルを踏む場所を誤って覚えている	運転手が危険を察知したが自動運転を過信して，ブレーキを踏まない	-	スピード表示が実際より低速となっており，危険な速度であることを察知しない	-	-	他のペダルと踏み間違える	-	-	-	-	-	人工知能モジュールが自動運転不能と判断したが，自動運転の解除警告が通知されない	-	外部環境の一部になりすまし，誤った外部環境情報をクラウドへ送信，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告をださせない	・クラウドからの情報を改ざん，自動運転不能な状態であっても人工知能に自動運転可能であると判断させる ・外部環境からセンシングモジュールへの情報を改ざん，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告を出させない ・外部環境からセンシングモジュールへの情報を改ざん，自動運転不能な状態であっても人工知能に自動運転可能であると判断させ，自動運転不能警告を出させない ・自動運転不能警告を改ざん(運転手の気をそらす・警告手段を破壊するなど），運転手への警告を遮断する	-	-	・人工知能モジュールに高負荷(物理的なものを含む)を与え，自動運転不能であることを報知できなくさせる ・運転手に対して大量or致命的な情報を与え，正常な判断をすることが不可能な状態にする	-
(UCA1-P) 自動運転中に意図しないペダル操作が発生し，自動運転が解除されブレーキが作動しなくなり外部環境と衝突する [SC1][SC2]	-	自動運転解除警告以外に気をとられ，自動運転が解除されたことを認識しない	運転手の足が意図せずペダルに触れてしまう	-	-	-	-	-	-	-	-	車の振動などの慣性力でペダルが動作する	-	自動運転解除警告が表示されない	-	-	・運転手以外の何かがペダルに触れる ・自動運転解除警告を表示させない	-	-	-	-
(UCA1-T) 非自動運転時にペダル操作が遅すぎる場合，減速指令が遅れ，外部環境と衝突する [SC1]	外部環境が見え辛く，運転手の判断が遅れる	体調などで運転手の判断能力が低下しており，ペダルを踏むのが遅れる	-	-	実際の速度より低速で速度表示がなされ，運転手が危険回避までの猶予があると勘違いする	-	ペダルのあそびが大きく，運転手の指示より減速指令が遅れる	-	-	-	-	経年劣化でペダルが硬くなり，ブレーキ指示を出すまでに時間がかかる	速度表示をせず，運転手が速度を認識できなくなる	自動運転不能の警告が遅れ，運転手が非自動運転であることの認識が遅れる	-	-	風などで信号と運転手の間に障害物が入るor信号の向きがかわることにより，運転手が危険を察知するのが遅れる	-	-	信号機が破壊し，運転手を迷わせる	-

付録8：表4-3：HCFの抽出結果 - UCA2に対するHCF

	HCF																			
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA2-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1]	-	-	-	-	-	-	-	運転手が濡れた足で操作することによりペダルが滑り，減速指令が解除される	-	-	-	接点不良などの異常が生じ，減速指令が出力されない	-	-	-	-	-	-	-	-
(UCA2-N) 減速指令がないと，そのまま外部環境と衝突する [SC1]	-	-	-	-	-	-	-	-	-	-	-	接点故障などにより，ペダル操作がなされても，減速指令を出力がされない	-	-	-	-	ブレーキシステムへの減速指令出力を改造し，指令がブレーキシステムへ届かないようにされている	-	-	ブレーキペダルが破壊されている	-
(UCA2-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	-	-	-	ブレーキシステムの故障により緩やかな減速が不能となる	-	-	-	・ブレーキペダルの遊びによる減速指令の遅れが生じることによる運転手の焦りにより，ペダルが強く踏み込まれる ・雨により制動距離が長くなったことにより生じた運転手の焦りにより，ペダルが強く踏み込まれる	-	-	-	ペダルの反力が弱く，必要以上に運転手がペダルを踏み込む	-	-	-	-	ブレーキシステムへの指令が改ざんされ，不要な減速指令が出力される	-	-	-	-
(UCA2-T) 運転手のペダル操作に対して減速指令が遅すぎた場合，外部環境との適切な距離が保てず衝突する [SC1]	-	-	-	-	-	-	・ペダルの遊びが大きく，減速指令が遅れる ・雨でペダルが滑り，減速指令が遅れる	-	-	-	-	-	-	-	-	-	-	-	-	-

付録9：表4-4：HCFの抽出結果 - UCA3に対するHCF

	HCF																				
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA3-D) 減速指令が終了する前に減速が終了し，外部環境との適切な距離が保てず衝突する [SC1]	-	-	-	ブレーキシステムの故障により，減速制御が実施されない	-	-	-	-	-	-	-	-	-	-	人工知能とブレーキペダルの減速指令が混在し，減速制御が停止する	-	-	-	-	-	-
(UCA3-N) 減速制御が行われないと，そのまま走行方向の外部環境と衝突する [SC1][SC2]	-	-	-	ブレーキシステムが故障し，減速制御が行われない	-	-	-	-	-	-	-	-	-	-	人工知能とブレーキペダルからの減速指令の突合	-	-	-	-	ブレーキシステムが破壊される	-
(UCA3-P) 不必要に強い減速が生じ，後方車両から追突される [SC3]	-	-	-	ブレーキシステムの故障	-	-	-	-	-	-	-	-	-	-	ブレーキペダルと人工知能モジュールからの減速指令の突合	-	-	-	-	-	-
(UCA3-T) 減速指令に対して減速が遅すぎる場合，外部環境との適切な距離が保てず衝突する [SC1] (UCA13-T-2) 外部へのブレーキ表示前に減速を始め，後方の車両から衝突される [SC3]	-	-	-	ブレーキシステムの故障	-	-	-	-	-	-	-	-	-	-	ブレーキペダル及び人工知能モジュールからの減速指令の突合	-	-	-	-	-	-

付録10：表4-5：HCFの抽出結果 - UCA5に対するHCF

	HCF																			
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA5-D) 十分な減速が行われる前に減速指令が終了し，外部環境との適切な距離が保てず衝突する [SC1]	減速中に運転手から意図しない自動運転解除指示が入力される	-	人工知能の学習データに存在しない状況が発生した	-	・速度が実際よりも遅く計測された ・悪天候により外部環境が認識できなかった	-	-	-	-	-	-	-	-	-	運転手が危険を察知し急ブレーキ操作を行う場合に，人工知能の判断が優先される	-	自動運転解除指示が改ざんされ，減速中に自動運転が終了される	-	-	DOS攻撃によりローカルダイナミックマップが攻撃され，地図参照ができなくなる	-
(UCA5-N) 自動運転時に人工知能が減速指令を出さないとそのまま外部環境と衝突する. [SC1]	運転手から意図しない自動運転解除指示が入力される	-	-	-	-	-	-	-	-	-	-	-	-	自動運転不能時に，運転手への通知が出力されない	-	ダミーの信号機を設置し，赤信号の交差点へ侵入させる	・自動運転解除指示を改ざんし，運転手が気付かない中で自動運転が解除される ・外部環境から車への情報が改ざんされ，障害物が存在しないように見せかけられる	-	-	-	-
(UCA5-P) 不必要に強い減速指令が出され，後方車両から追突される [SC3]	外部環境との距離が短くなってから自動運転指令が出され，急ブレーキとなる	-	人工知能が誤った学習をしている	ブレーキシステムの劣化により減速指令に対する減速度が小さくなり，その修正により過剰な減速指令が出力される	外部環境を御認識する	-	-	-	-	-	-	-	-	-	-	-	歩行者が飛び出すふりをする	-	-	-	-
(UCA5-T) 減速指令が遅れた場合，前方の外部環境との適切な距離が保てず衝突する [SC1]	外部環境との衝突が迫ってから，自動運転指示が出される	-	人工知能の教師データが不足している	-	雨や電磁波などのノイズにより外部環境の認識が遅れる	-	-	-	-	-	-	-	-	-	-	-	レーダーがジャミングされ，外部環境の認識が遅れる	-	-	-	-

付録11：表4-6：HCFの抽出結果 - UCA6に対するHCF

	HCF																				
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA6-D) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
(UCA6-N) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
(UCA6-P) 意図せず自動運転が解除され，衝突回避のためのブレーキ指令をだすことができない [SC1][SC2]	-	-	-	-	-	-	-	運転手が意図せずペダル操作をする	-	-	-	振動などでペダルが動いてしまう	-	-	運転手がブレーキペダルを踏みながら自動指示を出す	-	-	-	-	-	-
(UCA6-T) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

付録12：表4-7：HCFの抽出結果 - UCA8に対するHCF

	HCF																			
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA8-D) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
(UCA8-N) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合に作動指令が出せないと，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1]	-	薄暗い程度であるため，運転可能であると運転手が誤った判断をする	・運転手が視界確保の作動指令を出力する方法を知らない ・運転手が人工知能モジュールを過信し，自ら作動指示を行わない	-	センシング補助モジュールが作動していないにも関わらず，運転手に対して作動中の表示がされる	-	運転手のレバーなどの操作に対して接点不良などにより作動指令の出力が遅れる	運転手がレバーなどの操作を誤る	-	-	-	-	-	-	人工知能よりセンシングモジュールの終了指令が出力されている	-	-	-	-	-	-
(UCA18-P) 非自動運転かつ運転手が視界の確保無しで運転ができない状況となった場合で，運転手の視界確保可能な状況となる前に終了指令が出されると，運転手が外部環境を認識できず，ブレーキをかけずに外部環境と衝突する [SC1][SC2]	-	-	運転手がセンシング補助モジュール無しで視界確保可能であると誤って判断する	-	-	-	-	-	-	-	対向車両を気遣って運転手がセンシング補助モジュールに終了指令を与える	-	-	-	人工知能モジュールから終了指令が出力される	-	-	-	-	-	-
(UCA6-T) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

付録13：表4-8：HCFの抽出結果 - UCA9に対するHCF

	HCF																				
UCAx	(1) コントロールの入力か外部情報が欠けているか間違っている	(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、不正確な修正や適応	(3) プロセスモデルの矛盾、不完全、不正確	(4) コンポーネント故障、経時変化	(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	(6) 情報が与えられないか間違っている。測定が不正確。フィードバックの遅れ	(7) 遅れたアクション	(8) 不適切、有効でない欠けたコントロールアクション	(9) プロセスへの入力が欠けているか間違っている	(10) 識別されないか範囲外の妨害	(11) プロセスの出力がシステムハザードの一因に	(12) アクチュエーターの不適切なオペレーション	(13) センサーの不適切なオペレーション	(14) 他のコントローラーとの通信が欠けているか間違っている	(15) 矛盾するコントロールアクション	Spoofing（なりすまし）	Tampering（改ざん）	Repudiation（否認）	Information Disclosure（情報漏えい）	Denial of Service（サービス拒否）	Elevation of Privilege（特権の昇格）
(UCA9-D) N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
(UCA9-N) 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]	-	-	-	センシング補助モジュールの故障	外部環境が不明瞭であることを運転手/人工知能が認識でず，作動指令が入力されない	-	-	-	-	-	-	-	-	-	運転手と人工知能で異なる指示を与える	-	センシング補助モジュールの出力，方向が変更される	-	-	センシング補助モジュールを破壊する	-
(UCA9-P) 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]	-	-	-	センシング補助モジュールの故障	-	-	-	-	-	-	光が乱反射する	-	-	-	-	-	-	-	-	-	-
(UCA9-T) 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]	-	-	-	センシング補助モジュールの故障	-	-	雨が突然振り出し，運転手/人工知能からの作動指令の入力が遅れる	-	-	-	-	-	-	-	-	-	-	-	-	-	-

付録14：図4-2　UCAを基にしたGSN図