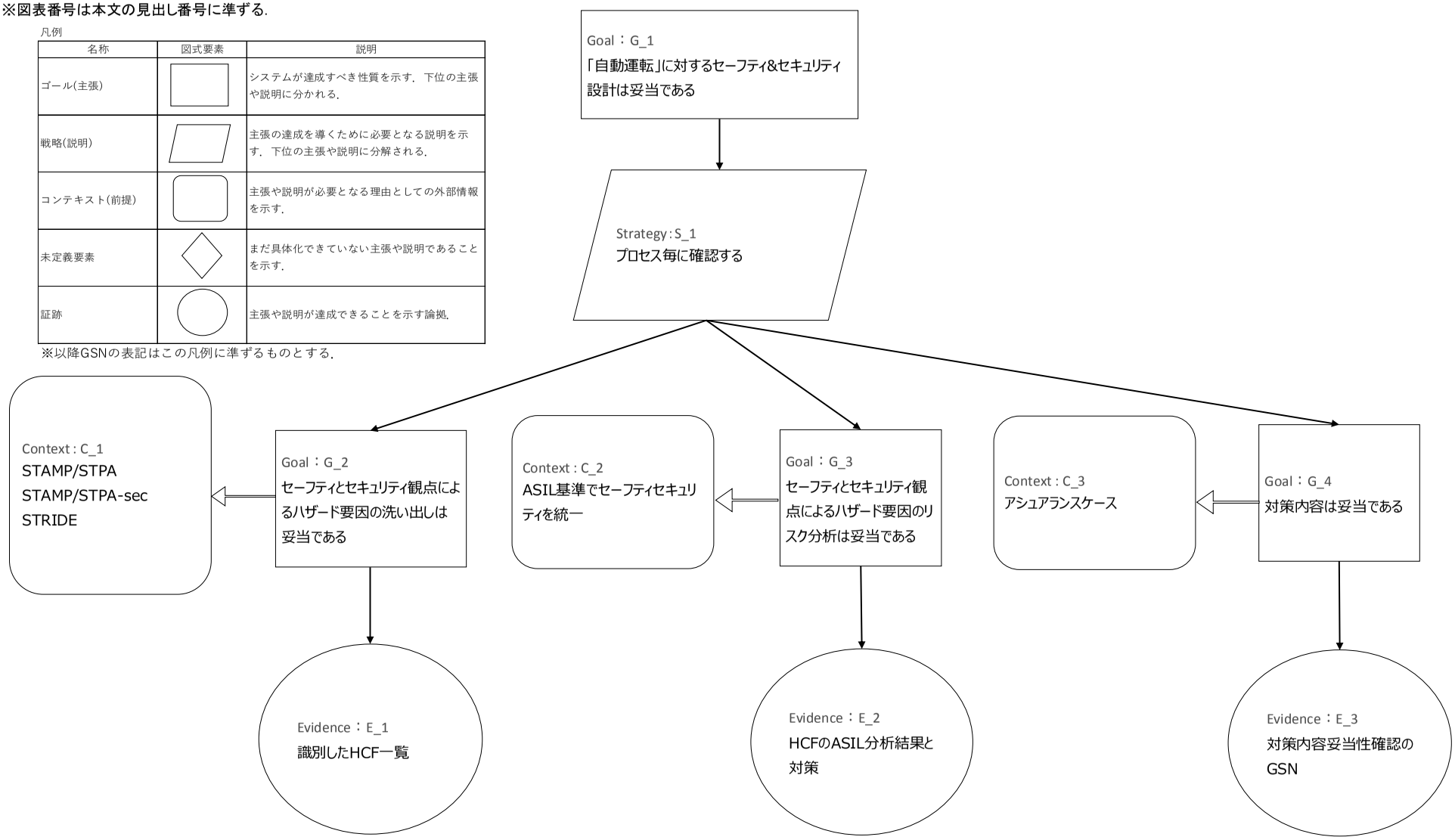
付録1：図3.2-1　保証全体像

※図表番号は本文の見出し番号に準ずる.

凡例

名称	図式要素	説明
ゴール(主張)		システムが達成すべき性質を示す．下位の主張や説明に分かれる.
戦略(説明)		主張の達成を導くために必要となる説明を示す．下位の主張や説明に分解される.
コンテキスト(前提)		主張や説明が必要となる理由としての外部情報を示す.
未定義要素		まだ具体化できていない主張や説明であることを示す.
証跡		主張や説明が達成できることを示す論拠.

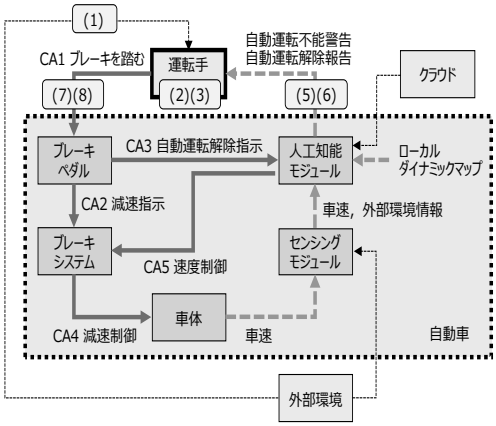
※以降GSNの表記はこの凡例に準ずるものとする.



付録2：図3.2-2　コントロールストラクチャに対するCAごとのガイドワードの割り当て

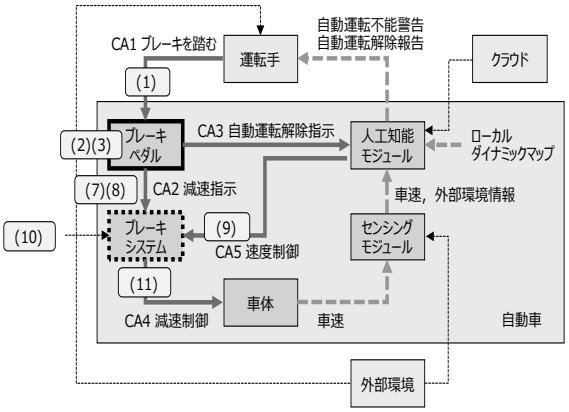
コントローラと制御対象プロセスを示したコントロールループ図と，割り当てたガイドワードを示す．
(1)～(11)がHCF導出のためのガイドワードを示す．（内容はHCFの表を参照）
ここでは部品の劣化を対象外として，「(4)コンポーネントの不具合．経年による変化」の割り当ては省略している．
STRIDEは該当箇所が多いため，コントロールループ図には記載していない．

CA1のガイドワードの割り当て



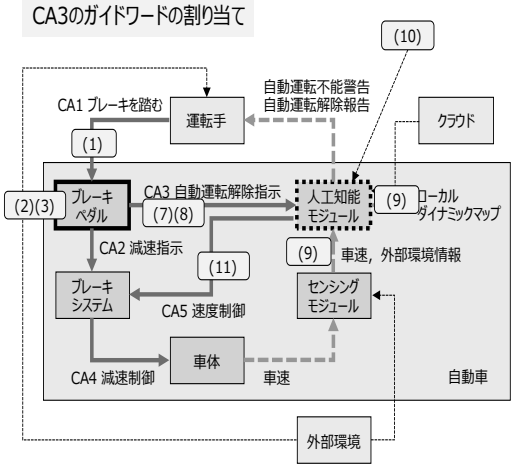
(9),(10),(11)は他のCAで確認するため，ここでは省略

CA2のガイドワードの割り当て



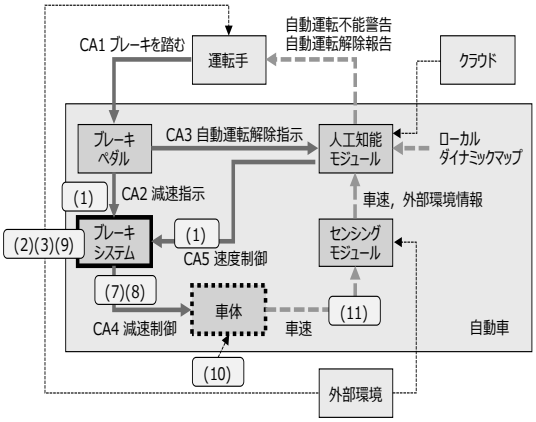
ブレーキペダルへのフィードバックがないため，(5),(6)はなし

CA3のガイドワードの割り当て



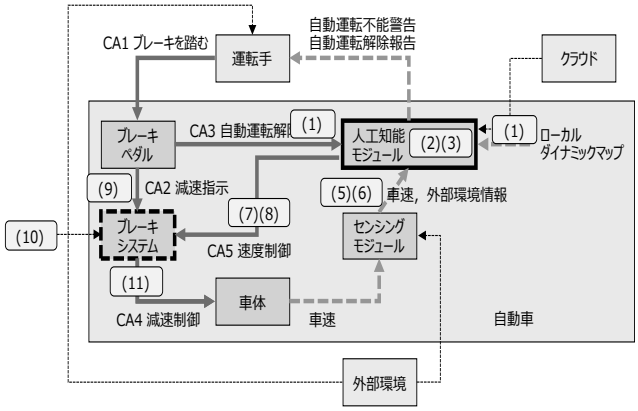
ブレーキペダルへのフィードバックがないため，(5),(6)はなし

CA4のガイドワードの割り当て



ブレーキシステムへのフィードバックがないため，(5),(6)はなし

CA5のガイドワードの割り当て



付録3：表3.2-1　UCAの抽出結果

コントロールアクション	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
CA1 運転手がブレーキを踏む	(UCA1-N) 運転手がブレーキを踏まないと危険回避ができず，外部環境と衝突する (SC1-2)違反	(UCA1-P) 運転手が誤った力加減でブレーキ操作を行うと，減速が弱く外部環境と衝突する (SC1-1)違反	(UCA1-T) 運転手のブレーキが遅すぎる場合，危険回避ができず，外部環境と衝突する (SC1-1)違反 運転手のブレーキが早すぎる場合，特に問題なし	(UCA1-S) 運転手がブレーキを踏む時間が短すぎる場合，危険回避ができず外部環境と衝突する (SC1-1)違反 運転手のブレーキを踏む時間が長すぎる場合，特に問題なし
CA2 減速指示	(UCA2-N) 運転手がブレーキペダルを踏んでいるのに減速指示を出さないと，外部環境と衝突する (SC1-2)違反	(UCA2-P) 運転手がブレーキペダルを強く踏んでいるのに減速指示が小さいと，外部環境と衝突する (SC1-1)違反 ブレーキペダルが弱く踏まれているのに減速指示が大きい場合およびブレーキペダルが踏まれていないのに減速指示を出す場合，特に問題なし	(UCA2-T) 運転手がブレーキペダルを踏んだタイミングに対し減速指示が遅すぎる場合，外部環境と衝突する (SC1-1)違反 ブレーキペダルが踏まれたタイミングに対し減速指示が早すぎる場合，特に問題なし	(UCA2-S) 運転手がブレーキペダルを踏み続けているのに減速指示の解除が早すぎる場合，外部環境と衝突する (SC1-1)違反 ブレーキペダルが離されたのに減速指示が長すぎる場合，特に問題なし
CA3 自動運転解除指示	(UCA3-N) 運転手が手動運転に切り替えたにもかかわらず自動運転が継続し，指示が競合して外部環境と衝突する (SC1-1)違反	(UCA3-P) 運転手が自動運転を解除していないにもかかわらず，自動運転が解除され，外部環境と衝突する (SC1-2)違反	(UCA3-T) 運転手が手動運転に切り替えたにもかかわらず，自動運転の解除が遅れ，自動運転が継続し，指示が競合して外部環境と衝突する (SC1-1)違反 自動運転の早すぎる解除はProviding causes hazardに該当する	(UCA3-S) N/A 自動運転停止命令はあるか無いかの物なので，長すぎる/短すぎる適用はなし
CA4 減速制御	(UCA4-N) ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けたのに，車体へ減速制御を行わないと，外部環境と衝突する (SC1-1)違反	(UCA4-P) ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に，車体への減速制御が想定よりも弱いと外部環境と衝突する (SC1-1)違反 減速制御が想定よりも強い場合は問題なし	(UCA4-T) ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に， 車体へ減速制御が遅れた場合，外部環境と衝突する (SC1-1)違反 減速制御が早すぎる場合，特に問題なし	(UCA4-S) ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に， 車体へ減速制御の適用が想定よりも短い場合，外部環境と衝突する (SC1-1)違反 減速制御の適用が長過ぎる場合，特に問題なし
CA5 速度制御	(UCA5-N) 障害物を検知した際に人工知能モジュールから速度制御（減速）が与えられない場合，外部環境と衝突する (SC1-1)違反	(UCA5-P) 障害物を検知した際に人工知能モジュールから誤った速度制御(小さすぎる減速)がある場合，外部環境と衝突する (SC1-1)違反	(UCA5-T) 障害物を検知した際に人工知能モジュールからの速度制御(減速)が遅すぎる場合，外部環境と衝突する (SC1-1)違反 速度制御(減速)が早すぎる場合，特に問題なし	(UCA4-S) 障害物を検知した際に人工知能モジュールからの速度制御(減速)が短すぎる場合，外部環境と衝突する (SC1-1)違反 速度制御(減速)が長すぎる場合，特に問題なし

付録4：表3.2-2：HCFの抽出結果 - UCA1に対するHCF

	HCF															
UCAx	(1)コントロール入力や外部情報の誤りや喪失	(2)不適切なコントロールアルゴリズム	(3)不整合，不完全，または不正確なプロセスモデル，不適切な操作	(5)悪い形状・不適切なフィードバック，あるいはフィードバックの喪失，フィードバックの遅れ	(6)部分的な情報・不正確な情報の供給，または情報の欠如，測定の不正確性，フィードバックの遅れ	(7)操作の遅れ **部分的・悪い形状のオペレーション**	(8)悪い形状・不適切または無効なコントロールアクション，コントロールアクションの喪失	(9)コントロールアクションの衝突，プロセス入力の喪失または誤り	(10)未確認，または範囲外の障害	(11)システムにハザードを引き起こすプロセス入力	(S) Spoofing identity なりすまし	(T) Tampering 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の暴露	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA1-N 運転手がブレーキを踏まないと危険回避ができず，外部環境と衝突する (SC1-2)違反	・悪天候など外部環境が悪く，運転手が危険察知しない	-	・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	-	・人工知能モジュールで異常を検知したが内部判定ロジックの誤りで自動運転不能警告が報知されない	-	・ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	-	-	-	-	・クラウドからの情報を改ざんし人工知能モジュールに自動運転継続可能であると誤認識させる	-	-	・人工知能モジュールに高負荷を与え自動運転不能警告を報知できない	-
UCA1-P 運転手が誤った力加減でブレーキ操作を行うと，減速が弱く外部環境と衝突する (SC1-1)違反	-	・運転手がブレーキを弱く踏む	-	-	-	-	・ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキが弱い	-	-	-	-	-	-	-	-	-
UCA1-T 運転手のブレーキが遅すぎる場合，危険回避ができず，外部環境と衝突する (SC1-1)違反	・悪天候など外部環境が悪く，運転手の危険察知が遅れる	-	-	・自動運転不能警告と自動運転解除報告が同時に鳴る	・人工知能モジュールに処理が集中して高負荷状態になり自動運転不能警告が遅れて鳴る	・運転手のブレーキ操作が遅れる	-	-	-	-	-	-	-	-	・人工知能モジュールに高負荷を与え自動運転不能警告を遅らせる	-
UCA1-S 運転手がブレーキを踏む時間が短すぎる場合，危険回避ができず外部環境と衝突する (SC1-1)違反	-	-	・運転手がブレーキを踏む時間が短すぎる	・自動運転解除報告がブレーキを踏んだが，人工知能モジュールへの他の割り込み処理が優先され直ぐに鳴り止む	-	-	-	-	-	-	-	-	-	-	-	-

(5)～(8)で太字で示したガイドワードはSTPA-Secのもの

コンポーネント間相互作用に注目したいため，故障や経年変化は対象外とし，以下を表から除外している
(4)コンポーネントの不具合．経年による変化，(12)アクチュエータの動作が不十分，(13)センサの動作が不十分

付録5：表3.2-3：HCFの抽出結果 - UCA2に対するHCF

	HCF															
UCAx	(1)コントロール入力や外部情報の誤りや喪失	(2)不適切なコントロールアルゴリズム	(3)不整合，不完全，または不正確なプロセスモデル，不適切な操作	(5)悪い形状・不適切なフィードバック，あるいはフィードバックの喪失，フィードバックの遅れ	(6)部分的な情報・不正確な情報の供給，または情報の欠如，測定の不正確性，フィードバックの遅れ	(7)操作の遅れ **部分的・悪い形状のオペレーション**	(8)悪い形状・不適切または無効なコントロールアクション，コントロールアクションの喪失	(9)コントロールアクションの衝突，プロセス入力の喪失または誤り	(10)未確認，または範囲外の障害	(11)システムにハザードを引き起こすプロセス入力	(S) Spoofing identity なりすまし	(T) Tampering 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の暴露	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA2-N 運転手がブレーキペダルを踏んでいるのに減速指示を出さないと，外部環境と衝突する (SC1-2)違反	-	・ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	-	-	-	-	-	・人工知能モジュールの速度制御と衝突し，ブレーキペダルの減速指示がブレーキシステムに適用されない	-	-	-	-	-	-	-	・ブレーキシステムを機能停止されると，ブレーキペダルの減速指示が受け付けられない ・掌握された人工知能モジュールによりブレーキシステムにDoS攻撃がしかけられていると，減速指示が受け付けられない ・人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ指示無しにされる
UCA2-P 運転手がブレーキペダルを強く踏んでいるのに減速指示が小さいと，外部環境と衝突する (SC1-1)違反	-	・ブレーキペダルの踏込具合と減速指示の強弱が感覚的に一致しない	-	-	-	-	-	・人工知能モジュールの速度制御と合算されてしまい，中途半端な減速制御となる	-	-	-	-	-	-	-	・人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ異なる指示にされる
UCA2-T 運転手がブレーキペダルを踏んだタイミングに対し減速指示が遅すぎる場合，外部環境と衝突する (SC1-1)違反	-	・ブレーキペダルの欠陥により減速指示が遅い	・ブレーキペダルの踏込を減速指示に変換する処理が遅い	-	-	-	-	・人工知能モジュールの速度制御とブレーキペダルの減速指示の優先順位判断が遅れ，ブレーキペダルの減速指示適用が遅くなる	-	-	-	-	-	-	-	・掌握された人工知能モジュールによりブレーキシステムにDoS攻撃がしかけられていると，減速指示の適応が遅延する ・人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ一時停止等の不要な処理を組み込まれる
UCA2-S 運転手がブレーキペダルを踏み続けているのに減速指示の解除が早すぎる場合，外部環境と衝突する (SC1-1)違反	-	・ブレーキペダルの欠陥により減速指示の解除が早すぎる		-	-	-	-	・ブレーキペダルの減速指示による減速中に人工知能モジュールの速度制御が衝突し，ブレーキペダルの減速指示が解除される	-	-	-	-	-	-	-	・人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ減速指示の継続限界時間が設定される

(5)～(8)で太字で示したガイドワードはSTPA-Secのもの

コンポーネント間相互作用に注目したいため，故障や経年変化は対象外とし，以下を表から除外している
(4)コンポーネントの不具合．経年による変化，(12)アクチュエータの動作が不十分，(13)センサの動作が不十分

付録6：表3.2-4：HCFの抽出結果 - UCA3に対するHCF

	HCF															
UCAx	(1)コントロール入力や外部情報の誤りや喪失	(2)不適切なコントロールアルゴリズム	(3)不整合，不完全，または不正確なプロセスモデル，不適切な操作	(5)悪い形状・不適切なフィードバック，あるいはフィードバックの喪失，フィードバックの遅れ	(6)部分的な情報・不正確な情報の供給，または情報の欠如，測定の不正確性，フィードバックの遅れ	(7)操作の遅れ **部分的・悪い形状のオペレーション**	(8)悪い形状・不適切または無効なコントロールアクション，コントロールアクションの喪失	(9)コントロールアクションの衝突，プロセス入力の喪失または誤り	(10)未確認，または範囲外の障害	(11)システムにハザードを引き起こすプロセス入力	(S) Spoofing identity なりすまし	(T) Tampering 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の暴露	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA3-N 運転手が手動運転に切り替えたにもかかわらず自動運転が継続し，指示が競合して外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの誤った入力情報で，自動運転解除指示が喪失する	・ブレーキシステムの欠陥により，ブレーキペダル踏み込み時に自動運転解除を指示しない ・ブレーキが踏まれているのにブレーキの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	-	-	-	-	-	-	-	-	-	-	-	-	・自動運転解除指示をしようとしたときに，人工知能モジュールにDoS攻撃を仕掛け，自動運転停止命令の受信ができない	・ブレーキペダルを掌握して，手動運転に切り替える際にも，自動運転解除指示を送出しない ・人工知能モジュールを掌握して，ブレーキペダルから送信された自動運転解除指示を受け付けない
UCA3-P 運転手が自動運転を解除していないにもかかわらず，自動運転が解除され，外部環境と衝突する (SC1-2)違反	・ブレーキペダルからの誤った入力情報で，意図しない自動運転解除指示がある	・ブレーキシステムの欠陥により，ブレーキペダル踏み込みが無くても自動運転解除指示がある	-	-	-	-	-	-	-	-	-	-	-	-	-	・ブレーキペダルを掌握して，自動運転中に，故意に自動運転停止命令を送出する ・人工知能モジュールを掌握して，指示がなくても勝手に自動運転解除指示を受け付ける
UCA3-T 運転手が手動運転に切り替えたにもかかわらず，自動運転の解除が遅れ，自動運転が継続し，指示が競合して外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの誤った入力情報で，自動運転解除指示が遅れる	・ブレーキシステムの欠陥により，ブレーキペダル踏み込み時の自動運転解除指示が遅れる	・ブレーキペダルの踏み込みを自動運転解除指示に変換する処理が遅い	-	-	**・人工知能モジュールに大量の入力情報(DoS攻撃)がある中で，自動運転解除指示が送出される**	-	-	-	-	-	-	-	-	・自動運転解除をしようとしたときに，人工知能モジュールにDoS攻撃を仕掛け，自動運転停止命令の受信が遅れる	・ブレーキペダルを掌握して，手動運転に切り替える際に，自動運転解除の指示を故意に遅らせる ・人工知能モジュールを掌握して，ブレーキペダルから送信された自動運転解除指示の受付を遅らす
UCA3-S N/A	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

(5)～(8)で太字で示したガイドワードはSTPA-Secのもの
UCA3-Tの(7)のHCFはSTPA-Secから導出したもの

コンポーネント間相互作用に注目したいため，故障や経年変化は対象外とし，以下を表から除外している
(4)コンポーネントの不具合．経年による変化，(12)アクチュエータの動作が不十分，(13)センサの動作が不十分

付録7：表3.2-5：HCFの抽出結果 - UCA4に対するHCF

	HCF																
UCAx	(1)コントロール入力や外部情報の誤りや喪失	(2)不適切なコントロールアルゴリズム	(3)不整合，不完全，または不正確なプロセスモデル，不適切な操作	(5)悪い形状・不適切なフィードバック，あるいはフィードバックの喪失，フィードバックの遅れ	(6)部分的な情報・不正確な情報の供給，または情報の欠如，測定の不正確性，フィードバックの遅れ	(7)操作の遅れ **部分的・悪い形状のオペレーション**	(8)悪い形状・不適切または無効なコントロールアクション，コントロールアクションの喪失	(9)コントロールアクションの衝突，プロセス入力の喪失または誤り	(10)未確認，または範囲外の障害	(11)システムにハザードを引き起こすプロセス入力	(S) Spoofing identity なりすまし	(T) Tampering 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の暴露	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA4-N ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けたのに，車体へ減速制御を行わないと，外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの誤った入力情報で，減速指示が喪失する ・人工知能モジュールからの誤った入力情報で，速度制御が喪失する	・ブレーキシステムの欠陥により，ブレーキペダルからの減速指示を車体への減速制御に変換できない ・ブレーキシステムの欠陥により，人工知能モジュールからの速度制御を車体への減速制御に変換できない	-	-	-	-	・ブレーキシステムから車体への減速制御が欠陥により伝わらず，車体の減速制御が失われる	・ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御が与えられない	-	-	-	-	-	-	・（人工知能掌握により）人工知能からブレーキシステムへDoS攻撃を行い，ブレーキシステムをダウンさせる	・ブレーキシステム掌握することで，車体への減速制御を行わない
UCA4-P ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に，車体への減速制御が想定よりも弱いと外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの誤った入力情報により，想定よりも弱い値で車体への減速制御となる ・人工知能モジュールからの誤った入力情報により，想定よりも弱い値で車体への減速制御となる	・ブレーキペダルからの減速指示を車体への減速制御に変換する際に，ブレーキシステムの欠陥により，想定よりも弱い値となる ・人工知能モジュールからの減速指示を車体への減速制御に変換する際に，ブレーキシステムの欠陥により，想定よりも弱い値となる	-	-	-	-	-	・ブレーキペダルと人工知能モジュールから同時に減速指示を受けた際に，人工知能の速度制御を優先してしまい，ブレーキペダルの想定よりも車体への減速制御が弱くなる	-	-	-	-	-	-	-	・ブレーキシステム掌握することで，車体への減速制御を想定よりも弱く行う
UCA4-T ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に，車体へ減速制御が遅れた場合，外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの減速指示が遅く，車体へ減速制御が遅れる ・人工知能モジュールからの速度制御が遅く，車体へ減速制御が遅れる	・ブレーキペダルからの減速指示を，車体への減速制御に変換する際に，ブレーキシステムの欠陥により，車体への通知が遅くなる ・人工知能モジュールからの減速指示を，車体への減速制御に変換する際に，ブレーキシステムの欠陥により，車体への通知が遅くなる	-	-	-	-	-	・ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御が遅れる	-	-	-	-	-	-	-	・ブレーキシステム掌握することで，車体への減速制御を遅れて行う
UCA4-S ブレーキペダルからの減速指示，または人工知能モジュールからの速度制御を受けた際に，車体へ減速制御の適用が想定よりも短い場合，外部環境と衝突する (SC1-1)違反	・ブレーキペダルからの誤った入力情報により，想定よりも早く減速制御を解除する ・人工知能モジュールからの誤った入力情報により，想定よりも早く減速制御を解除する	・ブレーキペダルからの減速指示により，車体への減速制御を行っている際に，ブレーキシステムの欠陥により，想定よりも早く減速制御を解除する ・人工知能モジュールからの減速指示により，車体への減速制御を行っている際に，ブレーキシステムの欠陥により，想定よりも早く減速制御を解除する	-	-	-	-	-	・ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御を想定外に解除する	-	-	-	-	-	-	-	・ブレーキシステム掌握することで，車体への減速制御解除を早めに行う

(5)～(8)で太字で示したガイドワードはSTPA-Secのもの

コンポーネント間相互作用に注目したいため，故障や経年変化は対象外とし，以下を表から除外している
(4)コンポーネントの不具合．経年による変化，(12)アクチュエータの動作が不十分，(13)センサの動作が不十分

付録8：表3.2-6：HCFの抽出結果 - UCA5に対するHCF

	HCF															
UCAx	(1)コントロール入力や外部情報の誤りや喪失	(2)不適切なコントロールアルゴリズム	(3)不整合，不完全，または不正確なプロセスモデル，不適切な操作	(5)悪い形状・不適切なフィードバック，あるいはフィードバックの喪失，フィードバックの遅れ	(6)部分的な情報・不正確な情報の供給，または情報の欠如，測定の不正確性，フィードバックの遅れ	(7)操作の遅れ **部分的・悪い形状のオペレーション**	(8)悪い形状・不適切または無効なコントロールアクション，コントロールアクションの喪失	(9)コントロールアクションの衝突，プロセス入力の喪失または誤り	(10)未確認，または範囲外の障害	(11)システムにハザードを引き起こすプロセス入力	(S) Spoofing identity なりすまし	(T) Tampering 改ざん	(R) Repudiation 否認	(I) Information Disclosure 情報の暴露	(D) Denial of Service サービス不能	(E) Elevation of Privilege 権限の昇格
UCA5-N 障害物を検知した際に人工知能モジュールから速度制御（減速）が与えられない場合，外部環境と衝突する (SC1-1)違反	・自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が与えられない	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールから速度制御が与えられない	-	・センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御ができなかった	・ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御ができなかった	-	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールから速度制御が与えられない	・自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が与えられない	-	-		・悪意のある第三者がクラウドの情報を改ざんし，外部環境を誤検知した結果，速度制御が与えられない	-	-	・悪意のある第三者がDoS攻撃などによって人工知能を不能としたため，速度制御が与えられない	・悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速制御を実施させない
UCA5-P 障害物を検知した際に人工知能モジュールから誤った速度制御(小さすぎる減速)がある場合，外部環境と衝突する (SC1-1)違反	-	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールから誤った速度制御となる	-	・センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，誤った速度制御となる	・ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，誤った速度制御となる	-	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールから誤った速度制御となる	-	-	-		・悪意のある第三者がクラウドの情報を改ざんし，外部環境を誤検知した結果，誤った速度制御となる	-	-	-	・悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速制御を小さくする
UCA5-T 障害物を検知した際に人工知能モジュールからの速度制御(減速)が遅すぎる場合，外部環境と衝突する (SC1-1)違反	・自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が遅い	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールからの速度制御が遅い	-	・センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が遅い	・ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が遅い	-	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールからの速度制御が遅い	-	-	-		・悪意のある第三者がクラウドからの情報を改ざんし，外部環境を誤検知した結果，速度制御が遅い	-	-	-	・悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速指示を遅くする
UCA5-S 障害物を検知した際に人工知能モジュールからの速度制御(減速)が短すぎる場合，外部環境と衝突する (SC1-1)違反	・自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が短い	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールからの速度制御が短すぎる	-	・センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が短すぎる	・ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が短すぎる	-	・人工知能の欠陥（＝プログラムバグ）があり，人工知能モジュールからの速度制御が短すぎる	-	-	-		・悪意のある第三者がクラウドからの情報を改ざんし，外部環境を誤検知した結果，速度制御が短すぎる	-	-	・悪意のある第三者がDoS攻撃などによって人工知能を不能としたため，速度制御が短すぎる	・悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速指示を短くする

(5)～(8)で太字で示したガイドワードはSTPA-Secのもの

コンポーネント間相互作用に注目したいため，故障や経年変化は対象外とし，以下を表から除外している
(4)コンポーネントの不具合．経年による変化，(12)アクチュエータの動作が不十分，(13)センサの動作が不十分

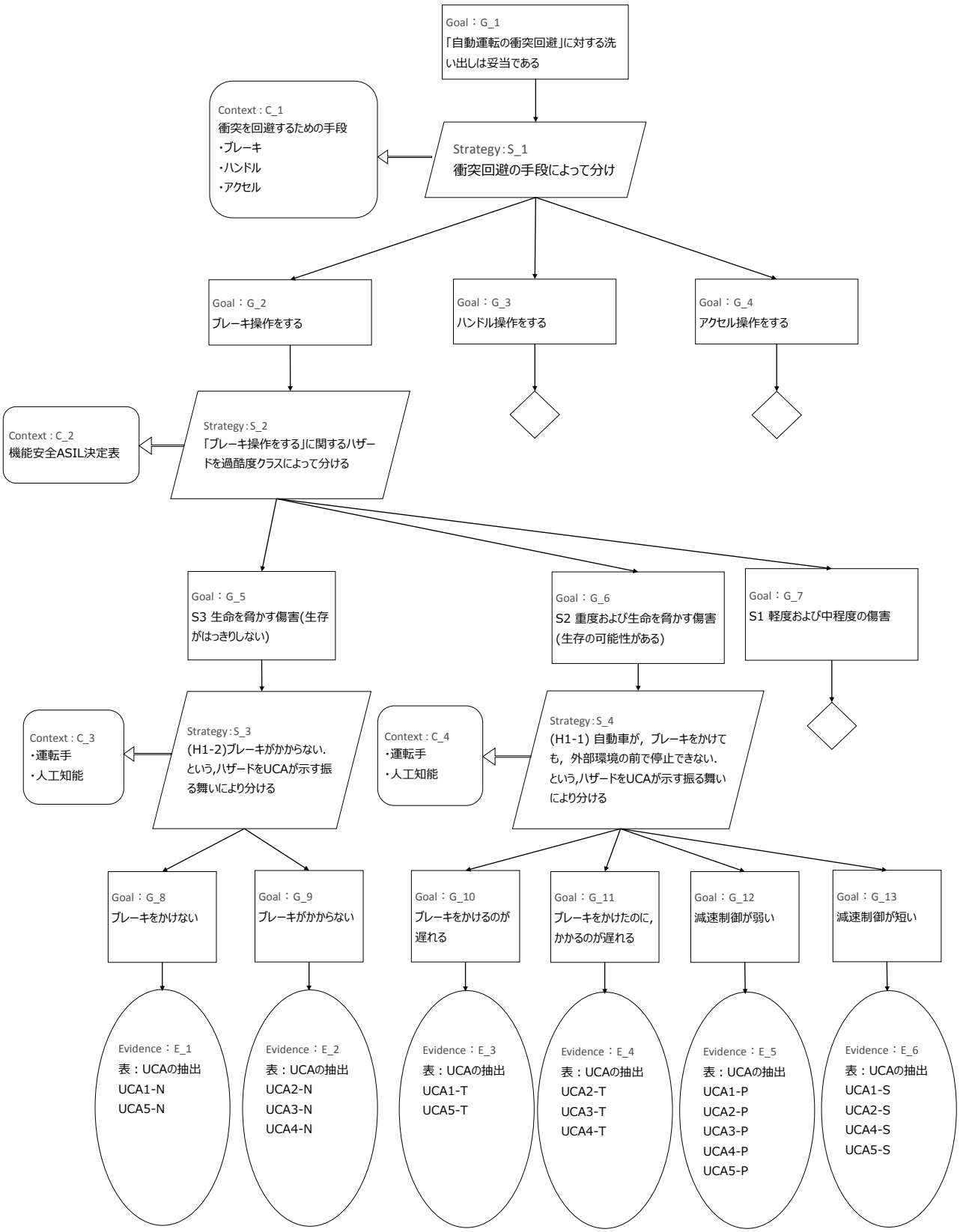
付録9：表3.2-7：ハザードに至るシナリオ（抜粋）

#	ハザードシナリオ
UCA1-Nに至るハザードシナリオ	
1-N1	悪天候など外部環境が悪く運転手が危険察知をできず，ブレーキを踏まない
1-N2	運転手が外部環境から危険を察知したが，自動運転を過信してブレーキを踏まない
1-N3	人工知能モジュールで異常を検知したが，内部ロジックの誤りで自動運転不能警告が鳴らず，運転手が自らブレーキを踏まない
1-N4	運転手がブレーキを踏んだがブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない
1-N5	クラウドからの情報を改ざんし，人工知能モジュールに自動運転の継続が可能であると誤認識させると，自動運転不能警告が鳴らず，運転手が自らブレーキを踏まない
1-N6	人工知能モジュールに高負荷を与えると，自動運転不能警告が鳴らず，運転手が自らブレーキを踏まない
UCA1-Pに至るハザードシナリオ	
1-P1	運転手が危険を察知した際，自動運転を過信してブレーキを踏む力が弱くなった
1-P2	運転手がブレーキを踏んだがブレーキペダルの遊びと認知する値が大きすぎて，ブレーキが弱く伝わった
UCA1-Tに至るハザードシナリオ	
1-T1	悪天候など外部環境が悪く，運転手が危険を察知するのが遅れブレーキを踏むのが遅れた
1-T2	人工知能モジュールからの警告と報告が同時に鳴り，運転手が一瞬戸惑い，ブレーキを踏むのが遅れた
1-T3	人工知能モジュールに異常が発生したが，処理が集中して高負荷になり自動運転不能警告が遅れて鳴ったため，ブレーキを踏むのが遅れた
1-T4	運転手が外部環境から危険を察知したが，自動運転を過信してブレーキを踏むのが遅れた
1-T5	悪意のある第三者が人工知能モジュールに高負荷を与え自動運転不能警告が遅れたため，ブレーキを踏むのが遅れた
UCA1-Sに至るハザードシナリオ	
1-S1	運転手が外部環境の危険を察知してブレーキを踏んだが，自動車を過信してブレーキを踏む時間が短すぎた
1-S2	運転手が外部環境からの危険察知や自動運転解除報告を受けてブレーキを踏んだ際，自動運転解除報告が鳴ったが，人工知能モジュールへの他の割り込み処理が優先され直ぐに鳴りやんだため，ブレーキを踏む時間が短くなった

#	ハザードシナリオ
UCA2-Nに至るハザードシナリオ	
2-N1	ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識せず，ブレーキペダルから減速指示が出ない
2-N2	人工知能モジュールの速度制御と衝突し，ブレーキペダルの減速指示がブレーキシステムに伝わらない
2-N3	ブレーキペダルからの指示アルゴリズムを改ざんされ減速指示を無しにされる
2-N4	ブレーキシステムにDoS攻撃がしかけられていると，減速指示が受け付けられない
2-N5	ブレーキシステムを機能停止されると，ブレーキペダルの減速指示が受け付けられない
UCA2-Pに至るハザードシナリオ	
2-P1	ブレーキペダルの踏込具合と減速指示の強弱が感覚的に不一致で，ブレーキペダルの減速指示が小さくなる
2-P2	人工知能モジュールの速度制御と合算されてしまい，ブレーキシステムが受ける減速指示が中途半端な値となる
2-P3	ブレーキペダルからの指示アルゴリズムを改ざんされ意図しない減速指示となる
UCA2-Tに至るハザードシナリオ	
2-T1	ブレーキペダルの欠陥により減速指示の伝達が遅れる
2-T2	ブレーキペダルの踏込を減速指示に変換する処理が遅く，減速指示が遅れる
2-T3	人工知能モジュールの速度制御とブレーキペダルの減速指示の優先順位判断が遅れ，ブレーキペダルの減速指示が遅くなる
2-T4	ブレーキペダルからの指示アルゴリズムの改ざんにより一時停止等の不要な処理を組み込まれ，減速指示が遅れる
2-T5	ブレーキシステムにDoS攻撃がしかけられていると，減速指示の適応が遅延する
UCA2-Sに至るハザードシナリオ	
2-S1	ブレーキペダルの欠陥により減速指示の継続が解除される
2-S2	ブレーキペダルの減速指示による減速中に人工知能モジュールの速度制御が衝突し，ブレーキペダルの減速指示が解除される
2-S3	ブレーキペダルからの指示アルゴリズムの改ざんにより減速指示の継続限界時間が設定され，減速指示が短くなる

※UCA3～UCA5のハザードシナリオは省略

付録10：図3.2−3：GSNによるUCAの整理結果



付録11：表3.2-8：ASIL 評価指標と決定値ルール

評価指標		
過酷度クラス	S0（低）	傷害なし
	S1	軽度および中程度の障害
	S2	重度および生命を脅かす障害（生存の可能性がある）
	S3（高）	生命を脅かす傷害（生存がはっきりしない）
発生頻度クラス	E0（低）	可能性なし
	E1	可能性が非常に低い
	E2	可能性が低い
	E3	可能性が中程度
	E4（高）	可能性が高い
回避可能性クラス	C0（可能）	一般的に回避可能
	C1	容易に回避可能
	C2	通常は回避可能
	C3（不可能）	回避困難または回避不可

※ＡＳＩＬ決定値のルール

過酷度クラス，発生頻度クラス，回避可能性クラスの数字部分を

点数（例：S2であれば2点）とし，各クラスの合計により

以下のようにASIL決定値を定める

ASIL決定値ルール	
6点以下	QM（Quality Management）
7点	ASIL_A
8点	ASIL_B
9点	ASIL_C
10点	ASIL_D

付録12：表3.2-9：ASIL 分析結果と対策（セーフティ）-1

※表サイズの関係で2ページに分割して記載．(1/2)

項番	アクシデント	対象	該当する UCA	HCF	評価指標				対策内容	残存リスク
					過酷度クラス	発生頻度クラス	回避可能性クラス	ASIL 決定値		
1	自動車が外部環境(歩行者/他の車/周辺物)と衝突/接触する	運転手－ブレーキペダル間	UCA1-N	悪天候など外部環境が悪く，運転手が危険察知しない	S3	E2	C2	ASIL_A	運転手の注意レベルを監視する	－
2				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	S3	E4	C2	ASIL_C	運転手の注意レベルを監視する 定期的に音声による注意喚起	－
3				人工知能モジュールで異常を検知したが内部判定ロジックの誤りで自動運転不能警告が報知されない	S3	E1	C2	QM		○
4				ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	S3	E2	C2	ASIL_A	ユーザビリティ評価を実施し，適切な遊び量に調整する	－
5			UCA1-P	運転手がブレーキを弱く踏む	S3	E2	C1	QM		○
6				ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキが弱い	S2	E1	C2	QM		○
7			UCA1-T	悪天候など外部環境が悪く，運転手の危険察知が遅れる	S2	E2	C2	QM		○
8				自動運転不能警告と自動運転解除報告が同時に鳴る	S2	E2	C2	QM		○
9				人工知能モジュールに処理が集中して高負荷状態になり自動運転不能警告が遅れて鳴る	S2	E1	C2	QM		○
10				運転手のブレーキ操作が遅れる	S2	E2	C2	QM		○
11			UCA1-S	運転手がブレーキを踏む時間が短すぎる	S2	E2	C2	QM		○
12				自動運転解除報告がブレーキを踏んだが，人工知能モジュールへの他の割り込み処理が優先され直ぐに鳴り止む	S2	E1	C2	QM		○
13		ブレーキペダル－ブレーキシステム間	UCA2-N	ブレーキペダルの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	S3	E2	C2	ASIL_A	ユーザビリティ評価を実施し，適切な遊び量に調整する	－
14				人工知能モジュールの速度制御と衝突し，ブレーキペダルの減速指示がブレーキシステムに適用されない	S2	E1	C3	QM		○
15			UCA2-P	ブレーキペダルの踏込具合と減速指示の強弱が感覚的に一致しない	S3	E2	C1	QM		○
16				人工知能モジュールの速度制御と合算されてしまい，中途半端な減速制御となる	S2	E1	C2	QM		○
17			UCA2-T	ブレーキペダルの欠陥により減速指示が遅い	S2	E2	C2	QM		○
18				ブレーキペダルの踏込を減速指示に変換する処理が遅い	S2	E2	C2	QM		○
19				人工知能モジュールの速度制御とブレーキペダルの減速指示の優先順位判断が遅れ，ブレーキペダルの減速指示適用が遅くなる	S2	E1	C2	QM		○
20			UCA2-S	ブレーキペダルの欠陥により減速指示の解除が早すぎる	S2	E2	C2	QM		○
21				ブレーキペダルの減速指示による減速中に人工知能モジュールの速度制御が衝突し，ブレーキペダルの減速指示が解除される	S2	E1	C2	QM		○
22		ブレーキペダル－人工知能モジュール間	UCA3-N	ブレーキペダルからの誤った入力情報で，自動運転解除指示が喪失する	S3	E1	C2	QM		○
23				ブレーキシステムの欠陥により，ブレーキペダル踏み込み時に自動運転解除を指示しない	S2	E1	C2	QM		○
24				ブレーキが踏まれているのにブレーキの遊びと認知する値が大きすぎて，ブレーキを踏んだと認識しない	S3	E2	C2	ASIL_A	ユーザビリティ評価を実施し，適切な遊び量に調整する	－
25			UCA3-P	ブレーキペダルからの誤った入力情報で，意図しない自動運転解除指示がある	S2	E2	C2	QM		○
26				ブレーキシステムの欠陥により，ブレーキペダル踏み込みが無くても自動運転解除指示がある	S2	E2	C1	QM		○
27			UCA3-T	ブレーキペダルからの誤った入力情報で，自動運転解除指示が遅れる	S2	E2	C2	QM		○
28				ブレーキシステムの欠陥により，ブレーキペダル踏み込み時の自動運転解除指示が遅れる	S2	E2	C2	QM		○
29				ブレーキペダルの踏み込みを自動運転解除指示に変換する処理が遅い	S2	E2	C2	QM		○
30		ブレーキシステム－車体間	UCA4-N	ブレーキペダルからの誤った入力情報で，減速指示が喪失する	S3	E2	C2	ASIL_A	サイドブレーキを使用した緊急停止機能を追加する	－
31				人工知能モジュールからの誤った入力情報で，速度制御が喪失する	S3	E2	C2	ASIL_A	サイドブレーキを使用した緊急停止機能を追加する	－
32				ブレーキシステムの欠陥により，ブレーキペダルからの減速指示を車体への減速制御に変換できない	S3	E1	C2	QM		○
33				ブレーキシステムの欠陥により，人工知能モジュールからの速度制御を車体への減速制御に変換できない	S3	E1	C2	QM		○
34				ブレーキシステムから車体への減速制御が欠陥により伝わらず，車体の減速制御が失われる	S3	E1	C2	QM		○
35				ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御が与えられない	S3	E1	C2	QM		○

付録12：表3.2-9：ASIL 分析結果と対策（セーフティ）-2

※表サイズの関係で2ページに分割して記載．(2/2)

項番	アクシデント	対象	該当するUCA	HCF	評価指標				対策内容	残存リスク
					過酷度クラス	発生頻度クラス	回避可能性クラス	ASIL決定値		
36	自動車が外部環境(歩行者/他の車/周辺物)と衝突/接触する	ブレーキシステム－車体間	UCA4-P	ブレーキペダルからの誤った入力情報により，想定よりも弱い値で車体への減速制御となる	S2	E2	C2	QM		○
37				人工知能モジュールからの誤った入力情報により，想定よりも弱い値で車体への減速制御となる	S2	E2	C2	QM		○
38				ブレーキペダルからの減速指示を車体への減速制御に変換する際に，ブレーキシステムの欠陥により，想定よりも弱い値となる	S2	E1	C2	QM		○
39				人工知能モジュールからの減速指示を車体への減速制御に変換する際に，ブレーキシステムの欠陥により，想定よりも弱い値となる	S2	E1	C2	QM		○
40				ブレーキペダルと人工知能モジュールから同時に減速指示を受けた際に，人工知能の速度制御を優先してしまい，ブレーキペダルの想定よりも車体への減速制御が弱くなる	S2	E1	C2	QM		○
41			UCA4-T	ブレーキペダルからの減速指示が遅く，車体へ減速制御が遅れる	S2	E1	C2	QM		○
42				人工知能モジュールからの速度制御が遅く，車体へ減速制御が遅れる	S2	E1	C2	QM		○
43				ブレーキペダルからの減速指示を，車体への減速制御に変換する際に，ブレーキシステムの欠陥により，車体への通知が遅くなる	S2	E1	C2	QM		○
44				人工知能モジュールからの減速指示を，車体への減速制御に変換する際に，ブレーキシステムの欠陥により，車体への通知が遅くなる	S2	E1	C2	QM		○
45				ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御が遅れる	S2	E1	C2	QM		○
46			UCA4-S	ブレーキペダルからの誤った入力情報により，想定よりも早く減速制御を解除する	S2	E1	C2	QM		○
47				人工知能モジュールからの誤った入力情報により，想定よりも早く減速制御を解除する	S2	E1	C2	QM		○
48				ブレーキペダルからの減速指示により，車体への減速制御を行っている際に，ブレーキシステムの欠陥により，想定よりも早く減速制御を解除する	S2	E1	C2	QM		○
49				人工知能モジュールからの減速指示により，車体への減速制御を行っている際に，ブレーキシステムの欠陥により，想定よりも早く減速制御を解除する	S2	E1	C2	QM		○
50				ブレーキペダルからの減速指示と，人工知能からの速度制御の衝突により，車体の減速制御を想定外に解除する	S2	E1	C2	QM		○
51		人工知能モジュール－ブレーキシステム間	UCA5-N	自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が与えられない	S2	E1	C2	QM		○
52				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールから速度制御が与えられない	S2	E2	C2	QM		○
53				センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御ができなかった	S2	E2	C2	QM		○
54				ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御ができなかった	S2	E2	C2	QM		○
55				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールから速度制御が与えられない	S2	E2	C2	QM		○
56				すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が与えられない	S2	E1	C2	QM		○
57			UCA5-P	人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールから誤った速度制御となる	S2	E1	C2	QM		○
58				センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，誤った速度制御となる	S2	E1	C2	QM		○
59				ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，誤った速度制御となる	S2	E1	C2	QM		○
60				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールから誤った速度制御となる	S2	E1	C2	QM		○
61			UCA5-T	自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が遅い	S2	E1	C2	QM		○
62				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールからの速度制御が遅い	S2	E1	C2	QM		○
63				センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が遅い	S2	E1	C2	QM		○
64				ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が遅い	S2	E1	C2	QM		○
65				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールからの速度制御が遅い	S2	E1	C2	QM		○
66			UCA5-S	自動運転解除の指示誤り（解除すべきでないときに解除の指示がきた）があり，人工知能の指示と衝突した結果，速度制御が短い	S2	E1	C2	QM		○
67				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールからの速度制御が短すぎる	S2	E1	C2	QM		○
68				センシングモジュールの誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が短すぎる	S2	E1	C2	QM		○
69				ローカルダイナミックマップに誤りがあり，人工知能モジュールが正しい計算ができず，速度制御が短すぎる	S2	E1	C2	QM		○
70				人工知能の欠陥（=プログラムバグ）があり，人工知能モジュールからの速度制御が短すぎる	S2	E1	C2	QM		○

付録13：表3.2-10：ASIL 分析結果と対策（セキュリティ）

項番	アクシデント	対象	該当するUCA	HCF	評価指標				対策内容	残存リスク
					過酷度クラス	発生頻度クラス	回避可能性クラス	ASIL決定値		
1	自動車が外部環境(歩行者/他の車/周辺物)と衝突/接触する	運転手ーブレーキペダル間	UCA1-N	クラウドからの情報を改ざんし人工知能モジュールに自動運転継続可能であると誤認識させる	S2	E1	C2	QM		○
2				人工知能モジュールに高負荷を与え自動運転不能警告を報知できない	S3	E2	C2	ASIL_A	DoS対策を実施する	－
3			UCA1-T	人工知能モジュールに高負荷を与え自動運転不能警告を遅らせる	S2	E2	C2	QM		○
4		ブレーキペダルーブレーキシステム間	UCA2-N	ブレーキシステムを機能停止されると，ブレーキペダルの減速指示が受け付けられない	S3	E1	C2	QM		○
5				掌握された人工知能モジュールによりブレーキシステムにDoS攻撃がしかけられていると，減速指示が受け付けられない	S3	E1	C2	QM		○
6				人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ指示無しにされる	S3	E1	C2	QM		○
7			UCA2-P	人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ異なる指示にされる	S3	E1	C2	QM		○
8			UCA2-T	掌握された人工知能モジュールによりブレーキシステムにDoS攻撃がしかけられていると，減速指示の適応が遅延する	S2	E1	C2	QM		○
9				人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ一時停止等の不要な処理を組み込まれる	S2	E1	C2	QM		○
10			UCA2-S	人工知能経由で侵入された攻撃者によりブレーキペダルからの指示アルゴリズムを改ざんされ減速指示の継続限界時間が設定される	S2	E1	C2	QM		○
11		ブレーキペダルー人工知能モジュール間	CA3-N	自動運転解除指示をしようとしたときに，人工知能モジュールにDoS攻撃を仕掛け，自動運転停止命令の受信ができない	S3	E2	C1	QM		○
12				ブレーキペダルを掌握して，手動運転に切り替える際にも，自動運転解除指示を送出しない	S3	E1	C2	QM		○
13				人工知能モジュールを掌握して，ブレーキペダルから送信された自動運転解除指示を受け付けない	S3	E1	C2	QM		○
14			UCA3-P	ブレーキペダルを掌握して，自動運転中に，故意に自動運転停止命令を送出する	S3	E1	C2	QM		○
15				人工知能モジュールを掌握して，指示がなくても勝手に自動運転解除指示を受け付ける	S3	E1	C2	QM		○
16			UCA3-T	自動運転解除をしようとしたときに，人工知能モジュールにDoS攻撃を仕掛け，自動運転停止命令の受信が遅れる	S2	E1	C2	QM		○
17				ブレーキペダルを掌握して，手動運転に切り替える際に，自動運転解除の指示を故意に遅らせる	S2	E1	C2	QM		○
18				人工知能モジュールを掌握して，ブレーキペダルから送信された自動運転解除指示の受付を遅らす	S2	E1	C2	QM		○
19				人工知能モジュールに大量の入力情報(DoS攻撃)がある中で，自動運転解除指示が送出される	S2	E2	C3	ASIL_A	DoS対策を実施する	－
20		ブレーキシステムー車体間	UCA4-N	（人工知能掌握により）人工知能からブレーキシステムへDoS攻撃を行い，ブレーキシステムをダウンさせる	S3	E1	C2	QM		○
21				ブレーキシステム掌握することで，車体への減速制御を行わない	S3	E1	C2	QM		○
22			UCA4-P	ブレーキシステム掌握することで，車体への減速制御を想定よりも弱く行う	S3	E1	C2	QM		○
23			UCA4-T	レーキシステム掌握することで，車体への減速制御を遅れて行う	S3	E1	C2	QM		○
24			UCA4-S	ブレーキシステム掌握することで，車体への減速制御解除を早めに行う	S3	E1	C2	QM		○
25		人工知能モジュールーブレーキシステム間	UCA5-N	悪意のある第三者がクラウドの情報を改ざんし，外部環境を誤検知した結果，速度制御が与えられない	S3	E1	C2	QM		○
26				悪意のある第三者がDoS攻撃などによって人工知能を不能としたため，速度制御が与えられない	S3	E1	C2	QM		○
27				悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速制御を実施させない	S3	E1	C2	QM		○
28			UCA5-P	悪意のある第三者がクラウドの情報を改ざんし，外部環境を誤検知した結果，誤った速度制御となる	S2	E1	C2	QM		○
29				悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速制御を小さくする	S2	E1	C2	QM		○
30			UCA5-T	悪意のある第三者がクラウドからの情報を改ざんし，外部環境を誤検知した結果，速度制御が遅い	S2	E1	C2	QM		○
31				悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速指示を遅くする	S2	E1	C2	QM		○
32			UCA5-S	悪意のある第三者がクラウドからの情報を改ざんし，外部環境を誤検知した結果，速度制御が短すぎる	S2	E1	C2	QM		○
33				悪意のある第三者がDoS攻撃などによって人工知能を不能としたため，速度制御が短すぎる	S2	E1	C2	QM		○
34				悪意のある第三者が人工知能の制御を掌握（権限の昇格）し，ブレーキシステムへの減速指示を短くする	S2	E1	C2	QM		○

付録14：図3.2−4：ブレーキをかけないハザードのGSN