

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。

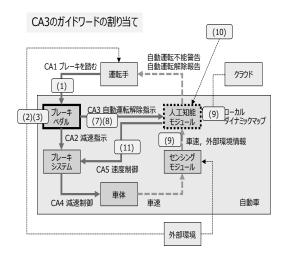
- (1)~(11)がHCF導出のためのガイドワードを示す. (内容はHCFの表を参照)
- ここでは部品の劣化を対象外として、「(4)コンポーネントの不具合.経年による変化」の割り当ては省略している.
- STRIDEは該当箇所が多いため、コントロールループ図には記載していない.

CA1のガイドワードの割り当て (1) 自動運転不能警告 CA1 ブレーキを踏む 自動運転解除報告 運転手 クラウド (7)(8) (5)(6) (2)(3) 人工知能 CA3 自動運転解除指示 ダイナミックマッフ ペダル モジュール CA2 減速指示 車速,外部環境情報 センシング ブレーキ システム モジュール CA5 速度制御 車体 白動車 CA4 減速制御 車谏 外部環境

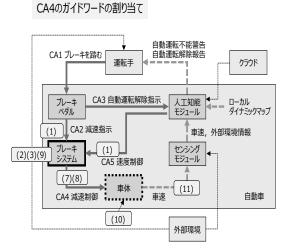
(9),(10),(11)は他のCAで確認するため、ここでは省略

CA2のガイドワードの割り当て 白動運転不能警告 CA1 ブレーキを踏む 運転手 クラウド (1) (2)(3) ブレーキ ペダル CA3 自動運転解除指示 ローカル ダイナミックマップ モジュール (7)(8) CA2 減速指示 車速,外部環境情報 ブレーキ システム (9) CA5 センシング モジュール (10) CA5 速度制御 (11) 車体 自動車 CA4 減速制御 車速 外部環境

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

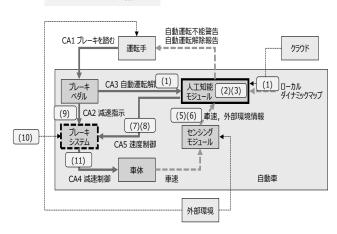


ブレーキペダルへのフィードバックがないため,(5),(6)はなし



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 NCAの抽出結果

く トラールアクション	Not Providina	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
#	近手がブレーキを踏まないと危険回避が 境と衝突する	が誤った力加減でブレーキ操作を行 限環境と衝突する	運転手のブレーキが遅すぎる場合, 危険回外部環境と衝突する	(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
		2764	運転手のブレーキが早すぎる場合,特に問題なし	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) 運転手がプ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 (SL) (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 5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 3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 (SC1-1)違反 プ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 (がわらず, 自動運転が解除され, 外部環境と衝突する (SC1-2)違反 (SC1-2)違反 (SC1-2) (SC1-2) (((UCA3-T) 運転手が手動運転に切り替えたにもかかり 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,事体へ 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) プ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 (SC1-1)違反 特に問題なし 特に問題なし	(UCA4-S) プレーキペグルからの減速指示,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 (いかにいた)でいた。 から誤った速度制御(小さすぎる減速)がある場合, 外 が部環境と衝突する (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,外部環境と値 突する (SC1-1)違反 進度制御(減速)が早すぎる場合,特に問題なし 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

	(E) Elevation of Privilege 権限の昇 格				
	(1) (D) (D) (Informat Denial of E ion Service o Disclosur サービス不能 P e 情報の暴	・人工知能モー 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		・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	N .
	(R) (I) Repudiat Informat ion	1	1	1	· 公公?**
	(R) Repudiat ion 容認	1	1	1	H
	(T) Tampering 改ざん	・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			
	(S) Spoofing identity なりすまし				
	(11)システ ムにハザー ドを引き起 こすプロセ ス入力 ス入力				±
	(10)未確 認, または 範囲外の 障害	1	1	1	· · · · · · · · · · · · · · · · · · ·
5	(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	1			- 間 拓 万 佐 店
•	(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	・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	・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		4
	(7)操作の遅 れ 都分的・悪い 形状のオペ レーション			・運転手のブ レー 士操作が 遅れる	
		・人工知能モージュールで異常 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		・人工知能モ ジュールに処理 が集中して高 負荷状態にな 負荷状態にな 的自動運転不 能警告が遅れ で鳴る	+
	(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			·自動運転不能警告と自動運転所運転解除報告	 ・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
	(3)不整合, 不完全, 非た は不正確なブ ロセスモデル, 不適切な操作	・運転手が待 険を察知したが 自動運転を過 信して, プレー キを踏まない	1		- ・運転手がブ ・自動運転解 - レーキを踏む時 除報告がプレー 間が短すぎる 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
	(2)不適切なコ ントロールアルゴ リズム	1	・運転手がブ レーキを弱く踏 む	1	む+火(0) (3)
	(1)コントロール 入力や外部情 報の誤りや喪 失	・悪天候など外部環境が悪く、運転手が危険察知しない	1	・悪天候など外 部環境が悪 く、運転手の 危険察知が遅 れる	1
	UCAX	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 力が成でプレーキ 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 運転手のプレーキ 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	UCA1-S 運転手がプレーキ 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

付録5:表3.2-3: HCFの抽出結果 - UCA2に対するHCF

UCAx	√∠Ľ(1)	(2)不適切なコン	(3)不整合,不 ((5)悪い形状・不適 ((6)部分的な情報・	(7)操作の (8)	(8)悪い形状・不適	HCF (9)コントロールア (1	(10)未確 (11	(11)システ (S)	(<u>L</u>)	(R)	(I)	(D)	(E)	
	(エノスカ ロール入力 や外部情 報の誤りや 喪失	トロールアルゴリズ ム				に	がないたが、これまたは無効なコント ・ルアクション、コン 「ールアクションの喪					ri Repudiat ion <u>杏酸</u>	No. 1 Information ion Disclosure 古認 情報の暴露	nial of vice ビス不	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 出されいと、AMT環接と編:		・プレーキペダルの 遊びと認知する値 が大きすぎて, ブ	-	1		1		・人工知能モ ジュールの速度制 御と衝突し,ブ	1	1	1	1	1	1	・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。 い・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
並Gavic, 77m/来死に割 実する (SC1-2)違反		認識しない						レーキ・グアレンJav 速指示がブレーキ システムに適用さ れない							・手座された人工が開きた。 レーキシストにDoS攻撃が、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プレーキペグルからの指示アルゴリズムを改さがよけれた。 さ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 強べ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		・ブレーキペグルの 踏込具合と減速 指示の強弱が感 覚的に一致しな い				1		・人工知能モ シュールの速度制 御に合真されてし まい、中途半端 な減速制御となる	1		1	1	1	1	・人工知能経由で侵入された攻撃者によりフル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 連転手がプレーキペダルを 踏んだタイミングに対し滅速 指示が遅すぎる場合,外 指示が遅すぎる場合,外 は関境は衝突する (SC1-1)違反		・ブレーキペダルの 久稲により減速 指示が驚い	・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		,	1		・人工知能モ ジュールの速度制 御ピカレーキペダ 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	1	1	1	1		1	・掌握された人工知能モジュールによりプレーキシステムにDoS攻撃がしかけられていると、減速指示の適応が墜延する・人工知能経田で侵入された攻撃者によりプレーキペグいからの指示アルコリズムを改ざんされ一時停止等の不要な処理を組みさえまれる	
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 久略により減速 指示の解除が早 すぎる				1		・ブレーキペグルの - 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	1	1		1		1	・人工知能経由で侵入された攻撃者によりプレーキペダルからの指示アルゴリズムを改さ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-	(5)~(8)で太字で示したガイドワードはSTPA-Secのもの	5.0			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	相互作用に注	目したいため	、故障や経年	=変化は対象ク	↑とし,以下を表	から除外し	タい2	_

付録6:表3.2-4:HCFの抽出結果 - UCA3に対するHCF

(5)~(8)で太子でホレだガイトソートはSTPA-Secのもの UCA3-Tの(7)のHCFはSTPA-Secから導出したもの

コノホーイントE和五作用に注目したいてめ,吹陣で粧牛変化は対象がとし,以下で衣がら除かしている(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 -

	(E) Elevation of Privilege 橋限の昇格	・プレーキシステム撃艦することで、事体への減速影響を行わない	・ブレーキシステム雑題すること。 で、事体への減速期節を想定 よりも既く行う	・プレーキシステム維護すること で、事体への減速解測を遅れ で行う	・プレーキシステル雑雑すること で、車体への減速制御解除を 早めに行う	2
	(D) Denial of Service サービス不能	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・				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
	(I) io Informatio n Disclosure 情報の暴露				,	象外とし, 以
	(R) Repudiatio n 否認		1			変化は対
	(T) Tampering 改定が	1	1			対障 や経年
	(S) Spoofing Spoofing はない	,				いため, お
	(11)システム 範 (こ)ザードを 引き起 <i>さ</i> す了 ロセス入力					注目した
	(10)未確 は認,または範 国外の障害		~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	 - 	· = -	互作用に
חכר	(9)コントロールアクションの衝突 突、プロセス入力の限失または 誤り	・ブレーキベダルからの高速指示 と、人工部的からの速度制御 の確実により、事体の高速制 他が与えられない	・プレーキペダルと人工知能を ジェーから同時に減難指示を 製工・別が、人工知能の速度 制能を確先してよい、プレー 中ペジルの想定よびも単体への 減速制御が弱くなる	・プレーキベダルからの減速指示 と、人工知能から改度制御 の衝突におり、事体の減速制 御が遅れる	・プレーキベダルからの減速指示 と、人工知能からの速度制御 の衝突にお、事体の減速制 御を想定外に解除する	コンポーネント間相互作用に注目したいため,
	(6)悪い形状・不適切または無 効なコントロールアジョンの喪失 トロールアグションの喪失 1	・ブレーキシズチムから単体への 減速制御が欠陥により近わら ず、単体の減速制御が失れれ る	7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7			
	7.7.1操作の運 n m	1 25 Pa 10				
	(6)部分的な (情報・不正確 対情報の供 計 約, または情 約, または情 熱 級の欠如, 別定の不正 確性, フィードツの遅れ					@ 1 @ 0;
	(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 の授失, フィードバック					≴STPA-Se
	(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					44-64
		・ブレーキンズトムの欠陥により、ブレーキ・イタリルシの流速制 イタリルシの流速制を単体への流速制 関心変換でまない。 ・ブレーキシステムの交陥により、人工知 能モジュールからの速度制御を単体への減 透開網に変換できない	- ブレーキペダルからの減速指示を車体へ の減速制制に変換する際に、プレーキシ スプムの欠陥により、想定よりも弱い値と なる ・ 人工有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、プレー キンズムの欠陥により、想定よりも弱い 値となる	- ブレーキペグルからの減速指示を、事体 - への減速制御に変換する際に、ブレーキングラムの欠陥により、事体への適知的登組が登る。 - 「工知能ドンニー」がらの減速指示を、事体への減速制御に変換する際に、ブーキンス上の欠陥により、事体への適知が加速を表している。	-プレーキペタルからの最らたスカイ情 - プレーキペタルからの減速指示により、車・軽により、表定よりも早く減速制御 体への減速制御を行っている際に、プレーを解する。 キンプルの公園により、想定よりも早く減・人工知能を持った。 選手がを解除する は、人工知能を対しかの減速指示により、車体への減速制御を行っている際に、プレーキシズムの公園により、程定よりを呼ば速制御を解除する に、プレーキシズムの公園により、復定よりた早く減速制御を解除する。 よりち早く減速制御を解除する	(5)~(8)で太字で示したガイドワードはSTPA-Secのもの
	(1)コントロール人力や外部階級の (2)不適切なコントロールアルゴリズム 誤りで喪失	- ナイグルからの際った入力情報で、流送を対象でである。 - 大工機能をラールから原わて - 大力情報で、速度制御が提供す。 - 5	- ブレーキベタルからの誤った入力情・ 機により、地差にも弱い値で車 体へが返出側ではな 大人工組能をジェールからの誤った 大力情報により、想定よりも弱い、 値で車体への減速制御になる 信で車体への減速制御になる	・ブレーキベダルからの減速指示が・ 選次、事体へ減速制御が膨れる・ 人工知能モジュールかの速度制 部が選次、事体へ減速制御が照れ。 る 音が選次、事体へ減速制御が配れ。	-ブレーキベタJ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 と解除する - 工工組能モジュールからの誤った 法制御を解除する に に	
	NCA×	UCA4-N プレーオイタリからの減 運転売、またし人工列 能モジュールから返還度 開催をジェールから返還度 体へ減速制御を行わな いた、外部環境を行わな でした。外部環境を行わな でした。外部環境を行わな でした。外部環境を行わな でした。外部環境を行わな でした。 でして、1)違反	UCA4P プレーキペタルからの減 電場下が、または人工知 能モジュールからの速度 別価を受けた際に、車 体への減速制御が提定 はたらがいと外部環境と 衝突する (SCL-1)違反	UCA4-T プレーキペリルトの減 選指示、または人工知 選指で、または人工知 無効を受けた際に、車 体へ減速制御が違れた する。 かのは環境を衝突 する。 (SCI-1)違反	UCA4-S プレーキペダルからの流 遠程市、または人工知 海モジュールからの運度 制御を受けた際に、車 体へ減速制御の適用が 規定よりた街の場合、 外部環境を衝突する (SCL-1)違反	

付録8:表3.2-6:HCFの抽出結果 - UCA5に対するHCF

								HCF]	ì	
UCAx	(1)コントロールスカや (2)不適切な 外部情報の誤りや喪失 ルアルゴリズム	- - -	(3)不整合, (不完全, ま こ たは不正確なこ プロセスモデ こ 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)操作の選(たれた 間分的・腸の ア 形状のオペ アーション	(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、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 (10)未確 の衝突, プロセス入力の 認。非には範 喪失または誤り 田外の障害	(10)未確 (10)未確 (10)	(11)システム (C)ぜードを 引き起こすプ ロセス入力	(S) Spoofing identity なりずまし	(T) Tampering 改さん	(R) (J) Repudiatio Ir n n n n n n n n n n n n n n n n n n	(I) (I) Informatio D D D D D D D D D D D D D D D D D D D	(R) (D) (D) (D) Repudiation Information Denial of Service n P-LX不能 Disclosure 情報の暴露	(E) Elevation of Privilege 権限の昇格
UCA5-N 層書物を検知した際に 人工が能をジュールが 送度制御(減速)が 与えられない場合、外 部環境と衝突する (SC1-1)違反	- 信動連転解除の指示 問り (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 の指示を衝突し、結 果、速度制御が与えら れない	- 人工知能の女腦(= 1- プログラムパグ)があり、 人工知能モジュールから 逸度制御が与えられな い		・センシンガモジュールの 誤りがあり、人工知能モ ジュールが正し、引導が できず、速度制御がで きなかった	・ローカルダイチミッカマップに誤りがあり、人工知能を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。		-人工知能のな階 (= プログラムパグ) があり、 人工知能モジュールがら 逸度制御が与えられない	・自動運転解除の指示・ に関係するでないととに解除の指示がきた があり、人工知能の指示がをの指示を要した結果、速度制御が与えられない	1 2			・悪慮のある第三者がク・ランドの情報を改さんし、外部環境を課後がし、外部環境を課後知りて結集、速度制御が与えられない			・ 動画のある第三者が 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	・悪悪のある第三者が 人工知能の制御を掌握 (権限の契格) し, ブ レーキシズムへの減速 制御を実施させない
UCA5-P 障害物を検知した際に 大工知能をジュールが 誤った速度制御(小さす きる減速)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 (= プログラル(ダ) 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 調りがあり、人工知能モ ジュールが正し、4件算が できず、誤った速度制 値となる	・ローカルダイナミッグマップに誤りがあり、人工知能をジュールが正しい計算ができず、誤った速度制能になる。	- 1 3 3 mmu	・人工知能の次陥 (= プログラムパグ) があり、人工知能モジュールがら 人工知能モジュールがら 誤った速度制御となる		1			・悪意のある第三者がワ・ランドの情報を改さん し、外部環境を課後知 した結果、誤うた速度 制御心なる				・悪意のある第三者が 人工知能の制御を掌握 (権限の契格) し, ブ し、十等のテムへの減速 制御を小さでする
UCA5-T 障害がを検知した際に 人工知能をジュールから 人工動をきる場合、外部環境 と衝突する (SC1-1)違反	・自動運転解除の指示 語り(解除すべきでない ときに解除の指示がき たりがあり、人工知能 の指示・衝突し、結 果, 速度制御が運い	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		・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、信拝が できず、速度制御が遅 い	・ローカルダイナミッグマップに誤りがあり、人工知能を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 (= プログラムパグ) があり、 人工知能モジュールがら の速度制御が遅い		1			・悪意のある第三者がクラウドかの情報を改さ んし、外部環境を課後 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 ドーキメテムへの減速 指示を運ぐする
UCA5-S 障害物を検知した際に 人工知能をジュールから の速度削削(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 語り(解除すべきでない ときに関係の指示がき 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			- センシンガモジュールの - ローカルダイナミッグマッ 場の方をり、人工知能子 プに誤りがあり、人工知 ジュールが正しい計算が 能モジュールが正しい計 できず、速度制御が短、算ができず、速度制御 すぎる	-ローカルダイチミッグマップに誤りがあり、人工知能をジュールが正しい計算ができず、速度制御ができず、速度制御が関すぎる。		- 人工知能の次陥 (= プログラムパグ) があり、人工知能モジュールがらの速度制御が短すぎる。					・悪魔のある第三者がク - ラウドからの情報を改さ んし、外部環境を誤検 知した結果、速度制御 が知すぎる			・悪魔のある第三者が DoS攻撃などによって人 工知能を不能としたた め、速度制御が残すぎ る	- 悪意のある第三者が 人工知能の制御を掌握 (権限の契格) し, ブ 指示を短ぐする 指示を短ぐする

(5)~(8)で太字で示したガイドワードはSTPA-Secのもの

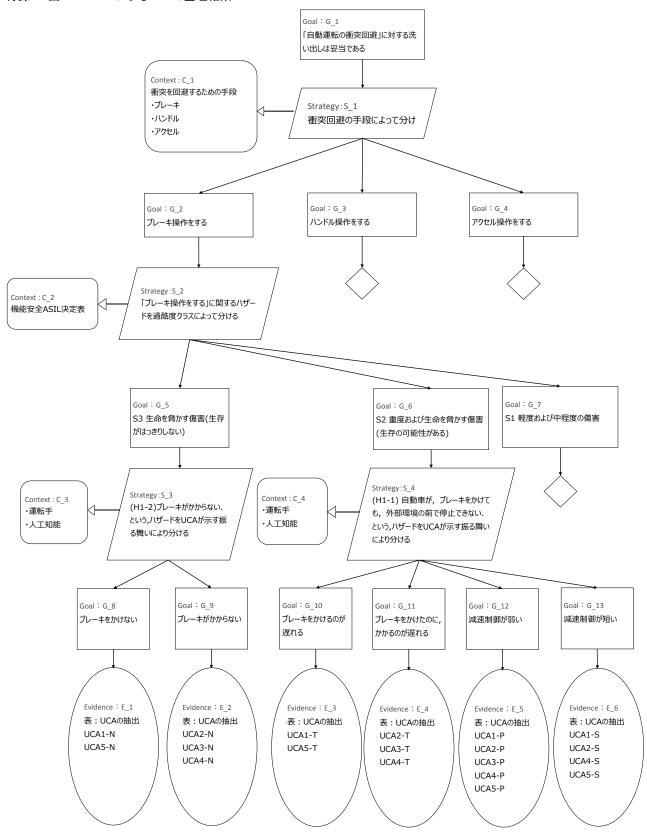
コンポーネント間相互作用に注目したいため、故障や経年変化は対象外とし、以下を表から除外している(4)コンポーネントの不具合、経年による変化,(12)アクチュエータの動作が不十分,(13)センサの動作が不十分

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	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-F	たである。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

11	
#	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

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										
	S0(低)	傷害なし								
過酷度クラス	S1	軽度および中程度の障害								
週間及ノノハ	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)								
	E0(低)	可能性なし								
	E1	可能性が非常に低い								
発生頻度クラス	E2	可能性が低い								
	E3	可能性が中程度								
	E4(高)	可能性が高い								
	C0(可能)	一般的に回避可能								
回避可能性クラス	C1	容易に回避可能								
四世り比圧ノノヘ	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)

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
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
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
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
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
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
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
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
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

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)

残存	U25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
公 第4次																																				
	ASIL 決定値	QM	ΜØ	Ø	ΜQ	ΜQ	MQ	ΜØ	Ø	Ø	MQ	ΜØ	ΜØ	ΜØ	ΜQ	ΜØ	ΜØ	ΜØ	ΜØ	ΜØ	ΜØ	QM	ΜØ	ΜØ	ΦM	ΜØ	ΜØ	ΜQ	ΜØ	ΜØ	ΜØ	Ø	ΜQ	ΜØ	ΜØ	ΜØ
1標	回避可能性 クラス	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2
評価指標	発生頻度 クラス	E2	E2	EI	E1	E1	E1	E1	EI	E1	E1	E1	E1	E1	Б	E1	E1	E2	E2	E2	E2	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E	EI	E1	E1	E1
	過酷度 クラス	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2	S2
HOH		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、プレーキシステムの欠陥により、想定よりも弱い値となる 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「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滅法指示を、車体への滅法制御に変換する際に、プレーキシステムの次陥により、車体への通知が選くなる	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、プ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	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(=プログラムパグ)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(=プログラムパグ)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	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 (=プログラムパグ) があり、人工知能モジュールから誤った速度制御となる	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 (=プログラムパグ) 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 (=プログラムパグ) があり、人工知能モジュールからの速度制御が遅い	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 (=プログラムパグ) があり, 人工知能モジュールからの速度制御が短すぎる
該当する	UCA	UCA4-P					UCA4-T					UCA4-S					UCA5-N						UCA5-P				UCA5-T					UCA5-S				
6 14		プレーキシステム	- 車体間										_				人工知能モジューループレーキシュ	ン	1	_		_	_	_		_				_			_		_	
アカシデット		自動車が外部環境 (歩矢巻 / 歩の車/国	辺物)と衝突/接触す	29																																
光	I C	36	37	88	39	40	41	42	43	44	45	46	47	48	49	20	51	52	53	54	22	26	22	28	59	09	19	62	63	64	65	99	67	89	69	70

付録13:表3.2-10:ASIL 分析結果と対策(セキュリティ)

残存	りスク	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
对策内容			DoS対策を実施する																	DoS対策を実施する															
	ASIL 決定値	ΜØ	ASIL_A	ΜØ	ΜØ	Ø	MQ	QM	Ø	MQ	MQ	MQ	ΜÖ	ΜØ	QM	ΜØ	ΜØ	ΜØ	ΜØ	ASIL_A	ΜØ	ΜØ	ΜØ	ΜØ	ΜØ	QM	QM	ΜØ	ΜØ	ΜØ	QM	ΜØ	ΜØ	ΜØ	Ø
計画 計画 計画 計画 計画 計画 計画 計画	回避可能性 クラス	C2	C2	C2	C2	C2	C2	C2	C2	0.2	C2	C1	C2	C2	C2	C2	C2	C2	C2	C3	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2	C2
	発生頻度 クラス	E1	E2	E2	E1	EI	EI	E1	E1	П	E1	E2	E1	E1	E1	E1	E1	E1	E1	E2	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1	E1
	過酷度 クラス	S2	S3	S2	S3	S	S3	S3	S2	SS	SS	SS	SS	S3	S3	S3	S2	S2	S2	S2	S3	S3	S3	S3	S3	S3	S3	S3	S2	S2	S2	S2	S2	S2	S2
LVII	nor	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	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	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	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	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プ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	人工知能経由で侵入された攻撃者によりプ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	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	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	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	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	(人工知能掌握により)人工知能からプレーキシステムへDoS攻撃を行い、プ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、車体への滅速制御を行わない	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	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	ブレーキシステム掌握することで、車体への滅速制御解除を早めに行う	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ひら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	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	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、プレーキシステムへの滅速指示を遅くする	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、プレーキシステムへの減速指示を短くする
該当する		UCA1-N		UCA1-T	UCA2-N			UCA2-P	UCA2-T		UCA2-S	CA3-N			UCA3-P		UCA3-T				UCA4-N		UCA4-P	UCA4-T	UCA4-S	UCA5-N			UCA5-P		UCA5-T		UCA5-S		
8	₩ Z	連転キーフレーキへ ダル間 フレーキペダルーフ レーキシステム間									エ知能モジュール間を表えていません。								ブレーキシステムー車体間					人工始能モジュールー・プレーキンステム間											
11	17777		(ダ1) 4/1607 年/16 辺物)と衝突/接触す				1			T	Τ		ı										- 1	1					ı				1	1	
班和	Ķ	1	2	3	4	2	9	7	8	6	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	58	30	31	32	33	34

付録14:図3.2-4:ブレーキをかけないハザードのGSN

