

自動運転システムにおける 運転指示ソフトウェアの システムアシュアランス

2017/03/27

奈良先端科学技術大学院大学
知能コミュニケーション研究室
博士前期課程1年 長村 佳歩

論証したテーマ

- 自動運転に対応した
運転指示ソフトウェア



音声認識機能:http://panasonic.jp/car/guide/voice_recognition/

タッチ操作:<http://pioneer.jp/carrozzeria/cybernavi/08cybernavi/function/design/touchpanel.html>

前提

- 危機回避は自動運転システムが行う
 - 危険の判断：システムと法令に基づく
- 安全：ドライバに不安を与えない
 - システムへの信頼性を損なわないため
- ドライバはシステムより優先される
- システムはstand aloneで動き，外部との通信はない

自動運転の段階

分類		概要	注(責任関係等)	左記を実現するシステム	
情報提供型		ドライバーへの注意喚起等	ドライバー責任	「安全運転支援システム」	
自動制御活用型	レベル1: 単独型	加速・操舵・制動のいずれかの操作をシステムが行う状態	ドライバー責任		
	レベル2: システムの複合化	加速・操舵・制動のうち複数の操作を一度にシステムが行う状態	ドライバー責任 ※監視義務及びいつでも安全運転できる態勢		
	レベル3: システムの高度化	加速・操舵・制動を全てシステムが行い、システムが要請したときのみドライバーが対応する状態	システム責任 (自動走行モード中) ※特定の交通環境下での自動走行 (自動走行モード) ※監視義務なし (自動走行モード:システム要請前)	「準自動走行システム」	「自動走行システム」
	レベル4: 完全自動走行	加速・操舵・制動を全てシステムが行い、ドライバーが全く関与しない状態	システム責任 ※全ての行程での自動走行	「完全自動走行システム」	

論証

システムが担当する部分

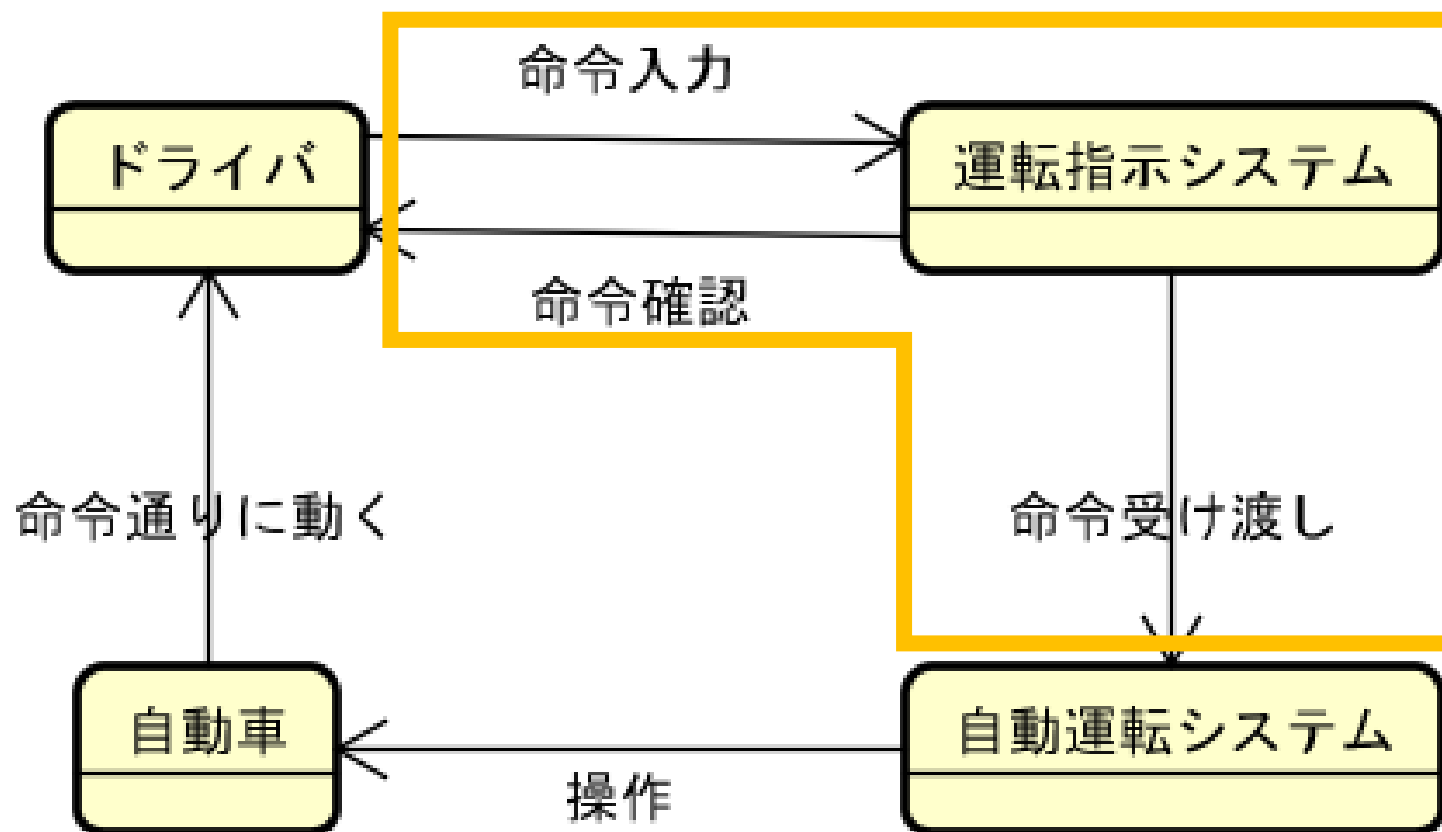
- 運転操作のUI
- 複雑な操作については，停車し再度設定させる

システム担当	操作	命令例
○	出車，出庫	
○	目的地設定	
×	走行中サービス	店の予約
	stand aloneのシステムであるので，考慮しない	駐車場検索
		電話，メール
○	操作	止まれ，速度を上げろ
×	危機回避	停止，避けろ，下がれ，進め
	自動運転の安全システムが対処	
○	駐車	

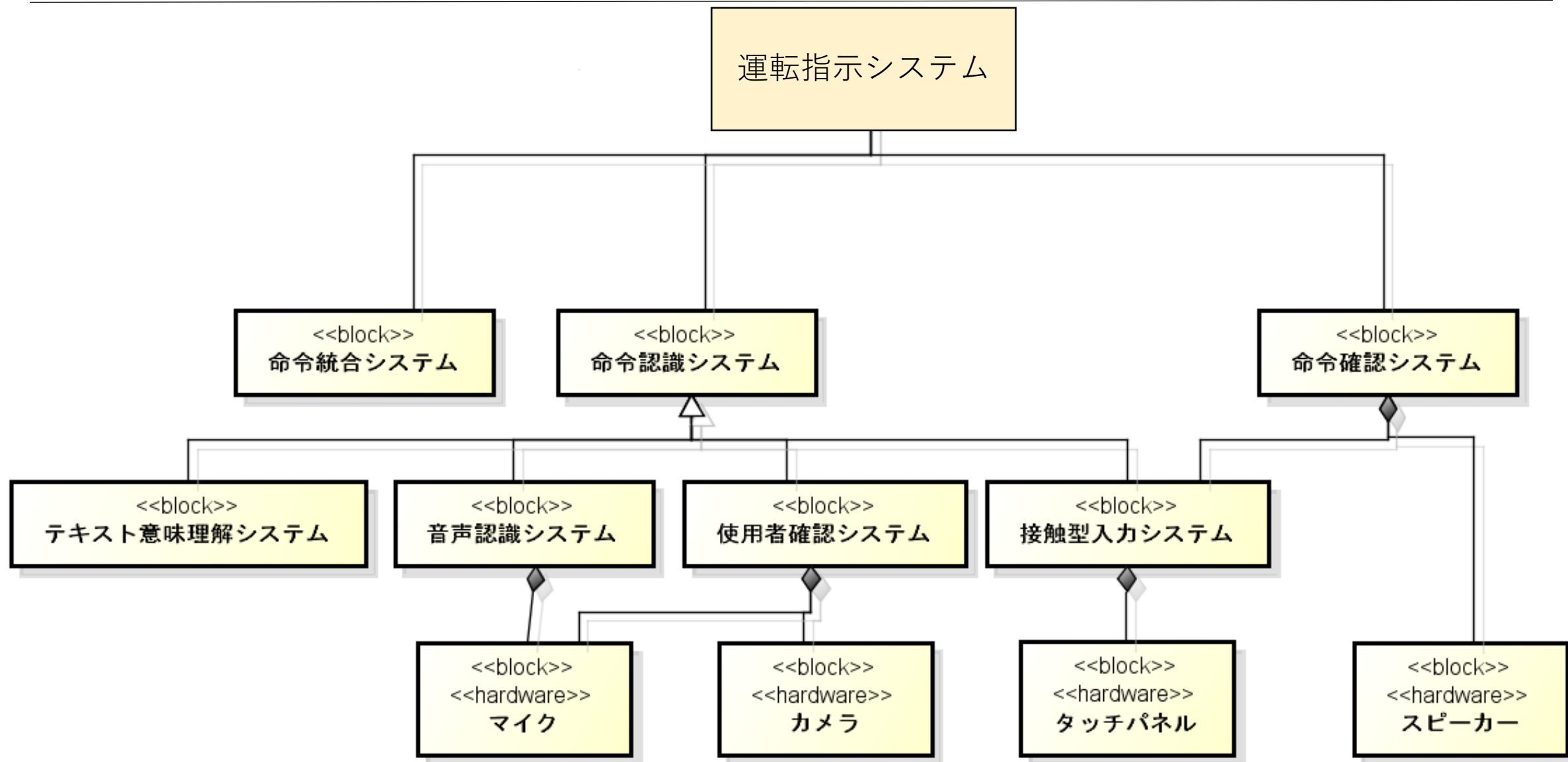
システム構成

- 自動運転システムを操作するためのUI

論証を行ったシステム



ブロック定義図



ステークホルダー

ステークホルダー一覧	ロール
ドライバ	命令を入力し、自動運転システムに命令を行う
	自動運転システムからの命令に対応する
自動運転システム	命令を運転に反映させる
└ 危機回避システム	危険時に事故回避を行う
運転操作システム	ドライバからの命令を受けとり、自動運転システムに実行させる
└ 命令統合システム	ドライバの命令を統合する
└ テキスト意味理解システム	テキストより意図を読み取る
└ 命令確認システム	命令が正しいか確認
└ 命令認識システム	ドライバからの命令を認識
	入力機器が壊れていないかテストする
└ 音声認識システム	音声をテキスト化する
└ 使用者確認システム	ドライバの声紋を判断する
	ドライバの顔を認識する
└ 接触型入力システム	タッチパネルのどこに触れているか確認

メリット

- 音声/タッチ入力によるコマンド/カーソル入力の煩雑さ除去
 - 使い慣れている人にはスムーズな移行
 - 慣れていない人には操作修得の容易性がある
- 現在のインターフェースを利用できる



デメリット

- 安全性への不安
 - 危険な動きをする
 - 意図しない動きをする

「安全の定義：ドライバに不安を与えない」

→以上についてSTAMP/STPAを用いて論証

STAMP/STPA(step0)

No.	アクシデント	No.	ハザード	No.	安全制約
A1	意図した目的地にたどり着かない	H1-1	命令の認識を誤り，システムが認識した目的地は意図したものではない	SC1-1	命令実行前にドライバに確認を取らなければならない
		H1-2	目的地が書き換えられない	SC1-2	命令変更できなければならない
		H1-3	命令が実行されない	SC1-3	命令は実行されなければならない
A2	運転する資格がないものが運転する	H2-1	ドライバ以外(車内の人物や音楽，子ども)の命令を識別してしまう	SC2-1	システムは声と顔で操作者の確認をせねばならない
		H2-2	ドライバの会話を命令と識別してしまう	SC2-2	システムはトリガーがあったときのみ命令を受け付ける (「OK,google」のように)
		H2-3	ドライバでないものをドライバと識別する	SC2-3	声紋，顔認証によってドライバを判別しなければならない
A3	運転者が不安になる	H3-1	入力機器の故障により操作に反応しなくなる	SC3-1	システムは定期的な自己検査を行わねばならない
		H3-2	近い道があるにもかかわらず理由なく遠回りをする	SC3-2	システムは経路選択の理由を伝えなければならない
		H3-3	命令を受け付けたかどうかのフィードバックがないため，実際に受け付けられたのか分からない	SC3-3	システムは受領した命令を確認できるようにしなければならない

STAMP/STPA(step1)

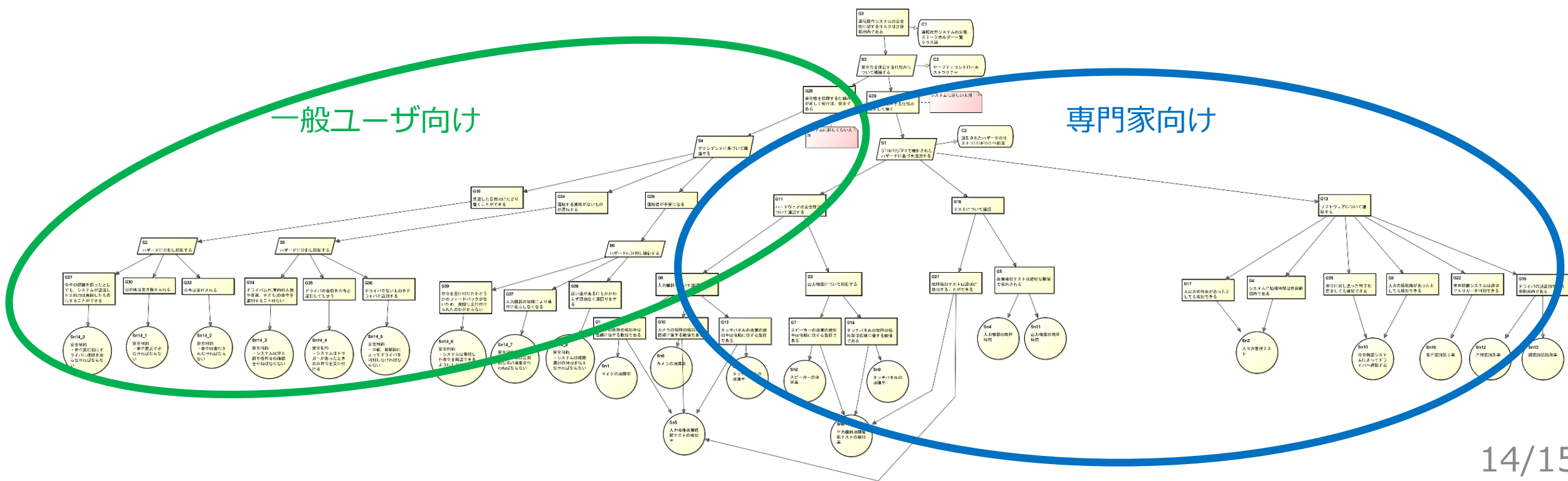
システム	コントロールアクション	行われない	誤った条件下で正しい制御情報	早過ぎる/遅過ぎる	終了が早過ぎる/長時間行われる
命令確認システム	・ 命令の認識結果をドライバに確認する	命令が実行されない(SC1-1違反)	命令がないので確認できない	/時間をがとられる(SC3-4違反)	承認前に終了する/承認しても終了しない(SC3-4違反)
	・ ドライバからの修正に対応する	命令が修正されない(SC1-2違反)	修正がない状況なので動かない	修正入力途中に対応してしまう/修正入力が終わったにも関わらず対応しない (SC3-4違反)	修正入力中に終了してしまう/修正入力が終わったにも関わらず対応しない(SC3-4違反)
	・ 経路選択理由をドライバに伝える	ドライバに選択理由が伝わらない(SC3-2違反)	伝える情報がないので動かない	問題ない/時間を食う (SC3-2違反)	ドライバに伝わらない(SC3-2違反)
	・ 自動運転システムに命令を受け渡す	運転されない(SC1-3違反)	受け渡す命令がないので動かない	入力途中に受け渡される/ (SC3-1違反)	命令が途中までしか伝わらない (SC1-3違反)/命令がすべて伝わったにもかかわらず受け渡し中になる(SC3-4違反)
	・ 出力機器に異常がないか自己テストをする	故障しても検知できない (SC3-1違反)	異常があるにもかかわらず正常と判別する(SC3-1違反)	/異常に気づくのが遅れる(SC3-1違反)	/メモリを食う
命令統合システム	・ 認識した命令を統合する	命令を統合しない(SC3-1違反)	入力がないにも関わらず動くためメモリを食う	認識した入力の一部が使えない/いつまでたっても統合しない (SC3-1違反)	認識した入力の一部が使えない (SC3-1違反)/いつまでたっても統合しない(SC3-4違反)
命令認識システム	・ 入力機器に異常がないか自己テストをする	故障しても検知できない (SC3-1違反)	異常があるにもかかわらず正常と判別する(SC3-1違反)	/異常に気づくのが遅れる(SC3-1違反)	/メモリを食う

STAMP/STPA(step2)

UCA No	UCA	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	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	システムにハザードを引き起こすプロセス出力	コンポーネントの不具合
UCA1	命令が実行されない(SC1-1違反)		入力の喪失		
UCA2	/時間を食う(SC3-4違反)	処理の遅れ			
UCA3	承認前に終了する/承認しても終了しない(SC3-4違反)		入力の喪失		入力機器の故障による誤認識
UCA4	命令が修正されない(SC1-2違反)		入力の喪失		入力機器の故障による認識不可
UCA5	修正入力途中に対応してしまう(SC3-4違反)/	終了判定をしてしまう	入力があると誤認識		入力機器の故障による誤認識
UCA6	/修正入力が終わったにも関わらず対応しない(SC3-4違反)	終了判定ができない	入力の喪失		
UCA7	ドライバに選択理由が伝わらない(SC3-2違反)	出力しない	出力の喪失		出力機器の故障
UCA8	問題ない/時間を食う(SC3-2違反)	処理の遅れ			
UCA9	ドライバに伝わらない(SC3-2違反)	処理の遅れ	出力の喪失		
UCA10	運転されない(SC1-3違反)		出力の喪失		

GSN

- 一般ユーザ向けの論証と専門家向けに分け論証を行う
- 一般ユーザに対して、アクシデントとハザードから事故の防止までを説明できる
- 専門家に対してはコントロールストラクチャが正しく働くことを説明して安全を示すことができる



STAMP/STPAとGSN

- STAMP/STPAは複雑なシステムの分析に適している
 - Step**0**で判別したアクシデントとハザードをGSNに用いる
→ **一般ユーザ**向けの論証
 - Step**2**で判別したアクシデントとハザードをGSNに用いる
→ **専門家** 向けの論証
- GSNは議論構造を明確にし，視覚的に理解しやすい

 STAMP/STPA
GSNは自動運転システムに関わる論証に適している

おわり

ありがとうございました