第14回
総合演習1
STAMP/STPAによる
自動運転システムの信頼性分析

総合演習
自動運転車の事例：L4 自動車駐車誘導（L4 Car Park Pilot, L4 CPP）

想定：自動運転車サービスを提供する会社。

要求分析の結果、以下のような要求仕様が固まってきた。

なんらかの認証がなされた駐車場又は駐車エリア内において、無人での移動を行う。最大速度は0km/h。

危険を検知したときのアクション：

1. 車速を徐行速度まで落とす。ただし、交差地点や合流箇所には進入しない。
   このとき目指す安全状態：車両は徐行速度で運転され、衝突を回避している。
2. 安全地帯で停止し、（もしいれば）遠隔オペレーター、又は、ドライバーに通知する
   このとき目指す安全状態：安全な場所で停止し、セキュアな状態にある。遠隔オペレーター又はドライバは情報を通知され、今後の対処について決定している。

題材: Safety First for Automated Driving (SaFAD)

2019年7月2日、ミュンヘン（ドイツ）

自動車および自動運転技術業界をリードする企業11社は2019年7月2日、自動運転車のセーフティバイデザインを浸透させるべく、ガイドラインとしてSafety First for Automated Driving (SaFAD)白書を発行しました。これは、安全な自動運転を可能にする乗用車の開発、ならびに検証および妥当性確認に向けた独自の統一フレームワークです。

この度、インフィニオン テクノロジーズ（FSE：IFX／OTCQX：IFNNY）をはじめ、Aptiv、Audi、Baidu、BMW、Continental、Daimler、FCA US LLC、HERE、Intel、Volkswagenの11社は、広範な業界を代表し、安全な自動運転車の製造、テスト、実用などに関する現時点において最も詳細なガイドラインを発行しました。

業界内では現在、自動運転車に関連する標準規格の策定が進められており、SaFAD白書は、セーフティバイデザイン、ならびに検証および妥当性確認の浸透を目的として作成されました。

SaFAD白書は、自動運転車が「通常のドライバーによる運転よりも安全」であることをカメラやステアリングシステムといったコンポーネントを介して実証できる明確なトレーサビリティをメーカーおよびオペレーターに初めて提供するものです。

また、SAE (J3016)が定義する自動運転レベル3およびレベル4の一般的なセーフティバイデザイン、ならびに検証および妥当性確認の手法も初めて概説しています。

SaFAD白書は、12の基本指針で構成され、さらに各基本指針は、自動運転車の各機能ごとに細分化されています。そして、各機能に対応するセーフティバイデザインを踏襲することで、基本指針の実践が可能になります。

「安全第一の自動運転」を掲げるSaFAD白書は、主要自動車メーカーおよびサプライヤー、ならびに関連技術業界が有する専門技能を結集させ、安全な自動運転車の開発を指南するものです。

過去数年間、自動運転技術への関心やその開発は自動車事故に関連する死亡者数の低減、交通渋滞の解消、新しいモビリティコンセプトの導入といった目標と相まって急速に成長しています。このような成長は、大企業だけでなく、成長を続ける多数の新興企業からも広範な開発手法がもたらされると期待されています。

SaFAD白書を発行したことで、同グループに参画している各パートナー企業の執筆者および専門家は、今後数か月にわたって国際的な業界および技術会議において、その取り組みを報告する予定です。

（出典）

ありうるシステム要素（1）

- Localization（位置推定のためのセンシングシステム）駐車場内の駐車場所を特定するのに十分な精度を持つ。実装方法は、例えば、駐車場の地図情報と、人工的なランドマークを配置するなどの方法が考えられる。
- Environmental Perception Sensor（物標検知のためのセンシングシステム）前方などの障害物や他車両、歩行者、駐車場構造物、路上の標識やラインなどを検知する。
  - 駐車場との通信なども必要であれば可能性あり
- Interpretation and Prediction（解釈と予測システム）他車両や歩行者、その他障害物などの動きの意味を解釈し、未来の動きを予測する。意味には、直進する、や、停止する、駐車する、右左折する、などがある。
- Driving Planning（運転計画システム）走行経路を計画し、計画された走行経路に対し、走行路の条件や自車の幅、他の物標などの制限を考慮し、車両の縦方向及び横方向の運動に変換する。危険を検知した場合、安全な場所に停止し、（もしあれば）遠隔オペレーター又はドライバーに通知する。

ありうるシステム要素（2）

- ADS Mode Manager(自動運転モード管理システム）自動運転モードの起動条件を入力情報に基づきチェックする。これは、車両が車室（1台分の駐車枠）にあり、センサーからの入力値が正常であり、ドライバーが不在の時である。自動運転モードの解除条件もチェックする。これは、フェールセーフ状態になったり、ドライバーが安全に車両の運転を引き継いだときである。ADS Mode Managerは、縮退モードへの遷移も担う。
- User State Determination（ユーザー状態決定システム）ユーザー（任意の搭乗者）が運転機能の委譲を要求しているか検出する。遠隔オペレーターについては、十分に訓練を積んだエキスパートであると仮定できるため、検出機能は必要ない。
- Human-Machine Interaction(HMI、人との相互作用システム）自動運転中はドライバーがいないため、必要ない。
- Monitors（監視システム）長時間のオペレーションになる場合、電源又は燃料を監視する必要性はあるかもしれない。

SaFADを読んでみよう: 2.2.2.1 Environmental Perception Sensors

The environment perception sensors cluster should capture all relevant external information to create a world model. Entities to detect are, but are not limited to, infrastructure defining the allowed area of driving, (vulnerable) road users, obstacles, traffic signs and acoustic signals.

Sensor types: As of today, a single sensor is not capable of simultaneously providing reliable and precise detection, classifications, measurements, and robustness to adverse conditions. Therefore, a multimodal approach is required to cover the detectability of relevant entities. In more detail, a combination of the following technologies shall provide suitable coverage for the given specific product:

環境知覚センサークラスタは、関連するすべての外部情報を捕捉して、世界モデルを作成する必要がある。検知するエンティティは、走行許可エリア、(脆弱な)道路利用者、障害物、交通標識、音響信号を定義するインフラであるが、これらに限定されない。

センサーの種類：現在現在、単一のセンサーでは、信頼性が高く正確な検出、分類、測定、および悪条件に対する堅牢性を同時に提供できない。したがって、関連するエンティティの検出可能性をカバーするために、マルチモーダルなアプローチが必要である。より詳細には、以下の技術の組み合わせにより、指定された特定の製品に適したカバー率を提供するものとする。

L4 CAR PARK PILOT (CPP)

名目ファンクションの定義 	L4 自動車顧客およびフリート運転における選択肢としての駐車場パイロット(CPP):認定駐車場構造物またはエリア内でのドライバーレス移動(警戒ドライバーなし、ドライバーの免許不要)、最大時速10km、ODDはオフストリート駐車場およびロジスティックエリアに重点を置く、インフラのスケーラブルな使用(インフラは必須ではないが遠隔操作まで可能)。
DEGRADED MODE/ MINIMAL RISK CONDITIONS	**CPP_MRC_2.1** 車両は這う速度で走行しており、衝突を回避している。
	CPP_MRC_3.1 車両は安全な場所で停止され、固定される。(遠隔)オペレーターは、さらなる行動の経過を知らされ、決定される(例.g.牽引車)。
MINIMAL RISK MANEUVER	**CPP_MRM_2.1** 速度を這う速度に下げる。交差点やランプには入らないようにする。
	CPP_MRM_3.1 安全な場所で立ち止まり、遠隔操作者(可能な場合)または車両ユーザーに通知する。

L4 CAR PARK PILOT (CPP)

NOMINAL FUNCTION DEFINITION 	L4 Car Park Pilot (CPP) as an option for vehicle customers and in fleet operation: Driverless movement within certified parking structures or areas (no vigilant driver, no driver's license necessary), max. 10 km/h, ODD focus on off-street parking and logistic areas, scalable use of infrastructure (infrastructure not mandatory but possible up to teleoperation)
DEGRADED MODE/ MINIMAL RISK CONDITIONS	**CPP_MRC_2.1** Vehicle is driving at crawling speed and avoids collisions.
	CPP_MRC_3.1 Vehicle is stopped in a safe location and secured; the (remote) operator is informed and decides on the course of further actions (e. g. towing vehicle).
MINIMAL RISK MANEUVER	**CPP_MRM_2.1** Reduce speed to crawling speed. Do not enter intersections or ramps.
	CPP_MRM_3.1 Stop in a safe location and inform the remote operator (if available) or vehicle user.

運転自動化のSAEレベル［J3016参照］

SAE J3016™ Levels of Driving Automation

	SAE Level 0	SAE Level 1	SAE Level 2	SAE Level 3	SAE Level 4	SAE Level 5
What does the human in the driver's seat have to do?	あなたは、これらのドライバーサポート機能が作動しているときはいつでも運転しています – たとえ足がペダルから外れていて、ステアリングがしていないとしても			このような自動運転機能が作動しているときは運転しない – "運転席"に座っていても		
	これらのサポート機能を常に監督しなければならない。安全性を維持するために、必要に応じてステアリング、ブレーキ、または加速しなければならない。			機能要求の際には、駆動してください。	このような自動運転機能では、運転を引き継ぐ必要はないでしょう	
	これらはドライバーサポート機能			これらは自動運転機能です		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	これらの特徴は、限られた条件下で車両を運転することができ、要求されるすべての条件を満たさない限り動作しない。		この機能は、あらゆる条件下で車両を駆動することができる
Example features	• Automatic emergency braking • Blind spot warning • Lane departure warning	• Lane centering OR 巡航の適応制御	• Lane centering AND 巡航の適応制御を同時に行う	• Traffic jam chauffeur	• Local driverless taxi • Pedals/steering wheel may or may not be installed	• Same as Level 4, but feature can drive everywhere in all conditions

SAFE STATE

安全状態とは、不合理なレベルのリスクを伴わない運転モードである。

SAFE(TY)

これは、危険による不合理なリスクがないことを意味する。

意図した機能の安全性(Sotif)

"The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF)."
[HTTPS://WWW.ISO.ORG/STANDARD/70939.HTML]

SCENARIO

シナリオはシーンの時間的シーケンスであり、ある時間スパンをカバーする。

SCENE

シーンは、すべてのアクターとオブザーバーの風景、動的要素、自己表現、およびそれらのつながりを記述する環境のスナップショットを記述する。シミュレートされたシーンだけがオールエンブラッシング(つまり客観的、別名グランドトゥルース)になり得るが、実世界のシーンは不完全で、欠陥や不確実性に悩まされ、主観的な観点から観察される。

SCENERY

The scenery includes all spatial stationary elements: The lane network (lanes, lane markings, etc.), stationary elements (obstacles, curbs, traffic signs, traffic lights, etc.), vertical elevation, and environmental conditions.

SECURITY

セキュリティとは、意図的な破壊や強制的な失敗を防ぐことである。

SAE LEVELS OF DRIVING AUTOMATION [SAE J3016]

SAE J3016™ Levels of Driving Automation

	SAE Level 0	SAE Level 1	SAE Level 2	SAE Level 3	SAE Level 4	SAE Level 5
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals, and you are not steering			You are not driving when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to uphold safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/acceleration support to the driver	These features provide steering AND brake/acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example features	• Automatic emergency braking • Blind spot warning • Lane departure warning	• Lane centering OR • Adaptive cruise control	• Lane centering AND • Adaptive cruise control at the same time	• Traffic jam chauffeur	• Local driverless taxi • Pedals/steering wheel may or may not be installed	• Same as Level 4, but feature can drive everywhere in all conditions

SAFE STATE

Safe state is an operating mode without an unreasonable level of risk.

SAFE(TY)

This refers to the absence of unreasonable risk due to hazards.

SAFETY OF THE INTENDED FUNCTIONALITY (SOTIF)

"The absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or by reasonably foreseeable misuse by persons is referred to as the Safety Of The Intended Functionality (SOTIF)."
[HTTPS://WWW.ISO.ORG/STANDARD/70939.HTML]

SCENARIO

A scenario is a temporal sequence of scenes and covers a certain time span.

SCENE

A scene describes a snapshot of an environment that describes the scenery, dynamic elements, and the self-representation of all actors and observers as well as their connection. Only a simulated scene can be all-embracing (i.e. objective, otherwise known as ground truth), whereas a real-world scene is incomplete, afflicted with faults and uncertainties, and observed from a subjective perspective.

SCENERY

The scenery includes all spatial stationary elements: The lane network (lanes, lane markings, etc.), stationary elements (obstacles, curbs, traffic signs, traffic lights, etc.), vertical elevation, and environmental conditions.

SECURITY

Security is the protection against intentional subversion or forced failure.

STAMP/STPAによる安全分析

- 分析目的の定義
  - ロス、アクシデント、ハザード、安全制約の識別
- 制御構造図のモデル化
  - 岡本先生の図を参考にして描いてみよう
- 非安全制御動作の識別
- ロスシナリオの識別

ロス(アクシデント)・ハザードの例

ロスID	ロス	ハザードID	ハザード	安全制約ID	安全制約
L1	道路利用者の死亡または負傷	H1	自車両と道路利用者との距離が規定値未満である状態(CPP_MRC_2.1)		
L1	道路利用者の死亡または負傷	H2	H1_CPP1 自車両の速度が10km/hを超えている状態(CPP_MRC_2.1)		
L2	自車両または自車両外の物体の損壊(自車両の盗難を含む)	H3	自車両が安全でない場所に停車している状態(CPP_MRC_3.1)		
L2	自車両または自車両外の物体の損壊(自車両の盗難を含む)	H4	自車両が安全な場所に停車した後、(遠隔)オペレーターに通知されない状態(CPP_MRC_3.1)		

制御構造のモデル化の例

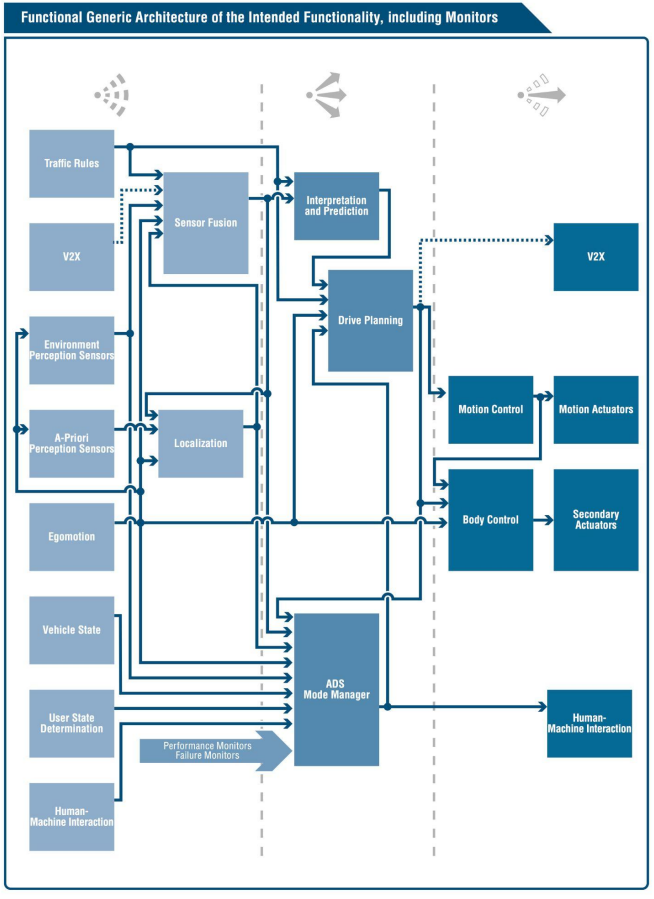


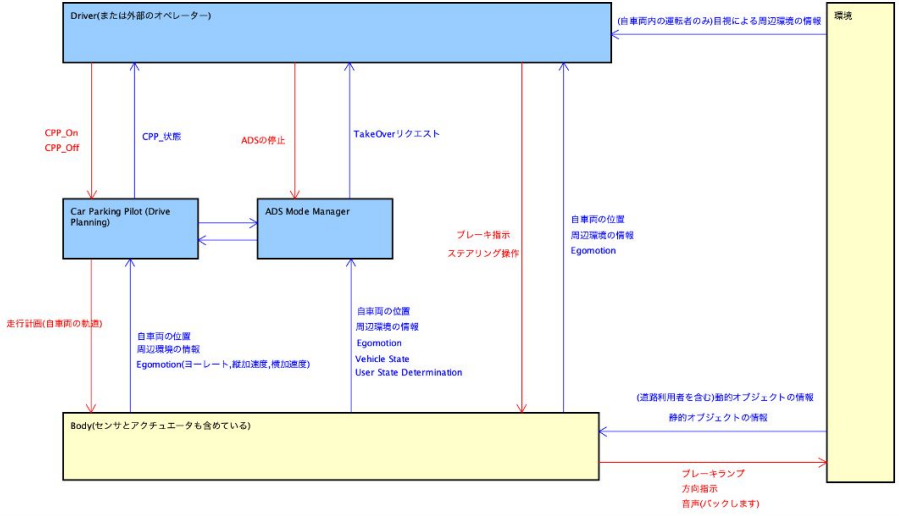
Figure 27: Functional Generic Architecture of the Intended Functionality, including Monitors

pp.106
名目上の機能定義
L4 Car Park Pilot (CPP) 車両の顧客およびフリート運用のオプションとして： 認定された駐車場構造またはエリア内でのドライバーレス移動（警戒運転手なし、運転免許不要）、最大時速10km、時速10km、路外駐車場と物流エリアに重点を置いたODD、インフラのスケーラブルな利用（インフラは必須ではないが、遠隔操作までは可能）。

劣化モード／最小リスク条件
CPP_MRC_2.1 クロール速度で走行し、衝突を回避する。
CPP_MRC_3.1 車両が安全な場所に停車し、固定される。（遠隔）オペレータに通知され、今後の対応（車両の牽引など）が決定される。

ミニマムリスクマヌーバ
CPP_MRM_2.1 クロール速度まで速度を落とす。交差点やランプに進入しない。
CPP_MRM_3.1 安全な場所に停止し、遠隔操作者（いる場合）または車両使用者に知らせる。

pp.105のFig.33から、CPPに関係しそうなエレメントを選択する？



UCA表の例

No	CA	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	ブレーキ指示	Driver(または外部のオペレーター)	Body(センサとアクチュエータも含めている)					
2	ステアリング操作	Driver(または外部のオペレーター)	Body(センサとアクチュエータも含めている)					
3	CPP_On	Driver(または外部のオペレーター)	Car Parking Pilot (Drive Planning)					
4	CPP_Off	Driver(または外部のオペレーター)	Car Parking Pilot (Drive Planning)					
5	走行計画(自車両の軌道)	Car Parking Pilot (Drive Planning)	Body(センサとアクチュエータも含めている)			(UCA5-P-1) 駐車スペースに道路利用者がいるにもかかわらず、駐車スペースへ移動する走行計画を指示した。(H1)		
6	ブレーキランプ	Body(センサとアクチュエータも含めている)	環境					
7	方向指示	Body(センサとアクチュエータも含めている)	環境					
8	音声(バックします)	Body(センサとアクチュエータも含めている)	環境					
9	ADSの停止	Driver(または外部のオペレーター)	ADS Mode Manager					

ロスシナリオの例

ID	HCF	ヒントワード	シナリオ
HCF5-P-1-1	センサの性能限界(カメラの死角)		カメラ(センサの１つ)の死角に道路利用者が居たため、(interpretation and Predictionが)駐車スペースに道路利用者が居ないと判断してしまい、(CPPが)非安全な走行計画を指示してしまった。