

MaaS システム安全コンセプト

SAMPLE

版	作成日	変更内容	発行
1.0.0	2020/2/29	新規作成	WITZ
1.1.0	2020/6/9	関連文書更新、図の差し替え、誤記修正	WITZ
1.2.0	2020/9/3	図の差し替え、誤記修正	WITZ
1.3.0	2020/10/15	コントロールストラクチャ図の差し替え、システム全体のコントロールアクション/フィードバック修正、UCA 追加	WITZ
1.4.0	2020/10/19	図の差し替え、誤記修正、関連文書更新	WITZ

目次

1	本文書の概要	1
1.1	目的	1
1.2	用語定義	1
1.3	準拠する規格	1
1.4	関連文書	2
2	対象システム定義	3
2.1	MaaS システム概要	3
2.2	システムの登場人物	4
2.3	システム全体の機能	5
2.4	システム全体構成	7
2.5	前提条件	8
2.5.1	自動運転車両	8
2.5.2	走行環境	10
2.5.3	利用環境	12
2.5.4	管制	12
2.5.5	駅	12
2.5.6	インフラセンサ	13
2.5.7	運行前点検	13
2.6	ユースケース	14
2.6.1	車両の走行	15
2.6.2	車両の専有路逸脱停車	16
2.6.3	車両の衝突回避停車	17
2.6.4	車両の乗客操作での非常停車	18
2.6.5	車両の駅での通常停車	19
2.6.6	車両のその他の非常停車	20
2.6.7	駅での車両乗降	21
2.6.8	駅以外での車両乗降	23
2.6.9	車両の駅での通常発車	24
2.6.10	車両の走行復帰	26
2.6.11	障害物対応	27
2.6.12	非常停車対応	28
2.6.13	想定環境逸脱監視	29
3	システムの全体設計	30
3.1	各構成要素の詳細	30
3.1.1	管制	30

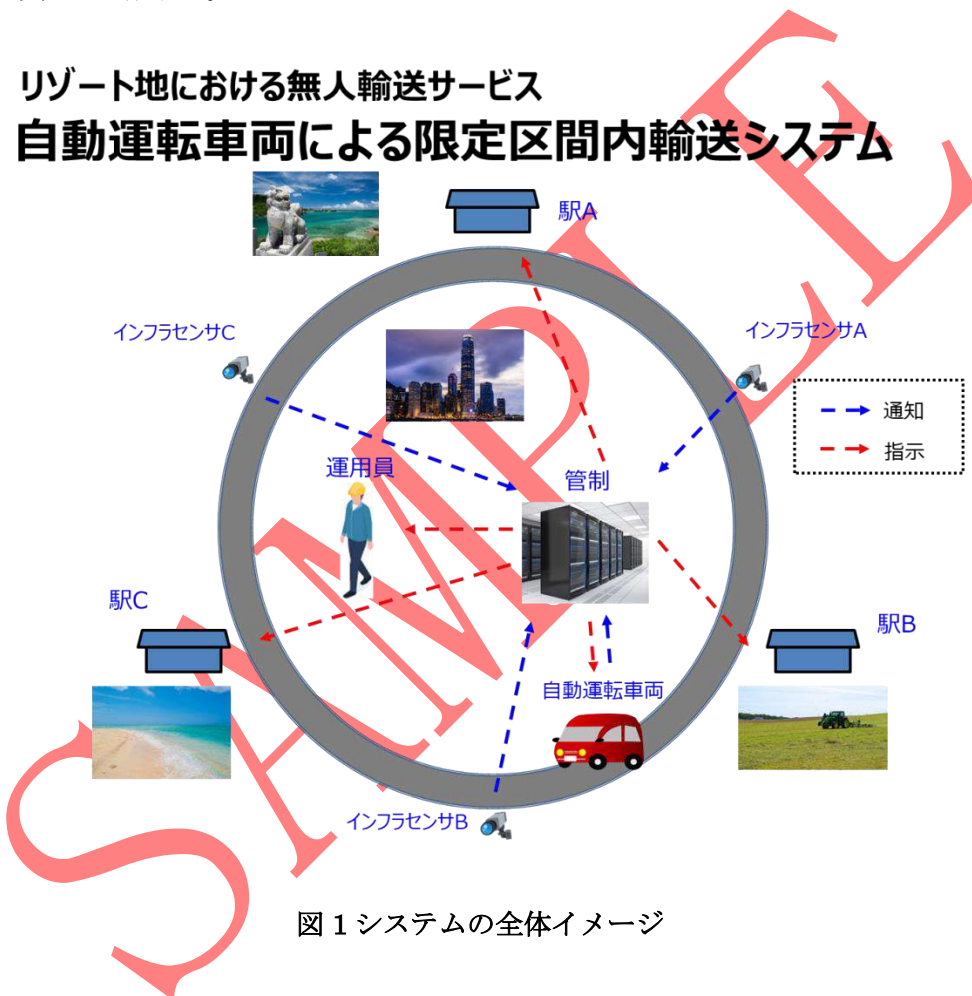
3.1.2 車両	31
3.1.3 インフラセンサ	33
3.1.4 駅.....	34
3.1.5 運用員	34
3.1.6 利用客	35
3.1.7 乗客	35
3.1.8 環境(専有路).....	36
3.1.9 環境(障害物).....	37
3.1.10 環境(その他).....	37
4 ハザード分析及びリスクアセスメント	38
4.1 目的.....	38
4.2 ハザード分析対象	38
4.3 ハザード分析手法	38
4.3.1 アクシデント・ハザード・安全制約の決定.....	38
4.3.2 非安全動作 (UCA) の抽出.....	39
4.3.3 非安全動作 (UCA) を含めたユースケースでのシナリオ導出.....	39
4.4 ハザード分析結果	39
4.4.1 アクシデント・ハザード・安全制約表.....	39
4.4.2 非安全動作 (UCA) の抽出.....	40
4.4.3 非安全動作 (UCA) を含めたユースケースでのシナリオ導出.....	43
4.5 リスクアセスメント	46
5 安全方策を追加したシステムの再評価.....	49
5.1 安全要求の割り当て.....	49
5.2 システムの再評価	49

2 対象システム定義

本章では今回の安全コンセプト定義対象である、MaaS システムについて記載する。

2.1 MaaSシステム概要

本システムは、リゾート地における利用を想定した自動運転車両による限定区間内輸送システムであり、下図のように自動運転車専用路（以降、専用路と記載）、自動運転車両（以降、車両と記載）、駅 A、B、C、車両を待つ利用客、乗車中の乗客、管制、障害物、インフラセンサ及び運用員にて構成する。



車両は専用路上を駅 A→駅 B→駅 C→駅 A の順に移動し、利用客の有無に関わらず各駅停車する。

もし駅での乗降目的以外に停車を要する事象が発生した場合、車両又は管制の判断により車両は停車し、運用員による対応が完了次第再発車する。停車を要する事象として、以下の四つが考えられる。一つ目はシステムの不具合で入ってしまった利用客や運用員、動物、及び故意の侵入者や落下物を含めた障害物の検出、二つ目は車両の専用路からの逸脱、三つ目は乗客による非常停車操作の実行、四つ目はシステムの想定する利用環境からの逸脱である。これらの場合は検出、停車ののち適宜対応とする。

2.6.7 駅での車両乗降

概要	車両が移動中に専有路上を走行する	
アクター	駅、乗客、利用客、インフラセンサ、車両、環境（専有路）	
事前条件	① 車両状態が「通常停車」	
	② 車両の検出位置が「駅」	
	③ 車両ドアの状態が「閉じている」	
	④ 乗客、利用客へフィードバックする車両の位置が「駅」	
	⑤ 乗客、利用客へフィードバックする車両の状態が「止まっている」	
	⑥ ホームドアの状態が「閉じている」	
事後条件	① 車両状態が「通常停車」	
	② 車両の検出位置が「駅」	
	③ 車両ドアの状態が「閉じている」	
	④ 乗客、利用客へフィードバックする車両の位置が「駅」	
	⑤ 乗客、利用客へフィードバックする車両の状態が「止まっている」	
	⑥ ホームドアの状態が「開いている」	
基本フロー	① 車両から管制に「車両状態通知（通常停車）」が行われる	VE-CO-FB-03
	② 管制から駅に「ホームドア制御指示（開放）」が行われる	CO-ST-CA-01
	③ ホームドアの状態が「閉じている」から「開いている」になる	ST-CO-FB-01
	④ 駅から乗客、利用客へのホームドアの状態が「開いている」になる	PA-ST-CA-01 ST-PA-FB-01 CU-ST-CA-01 ST-CU-FB-01
	⑤ 客も利用客もない場合、以降のフローを全てスキップする	—
	⑥ 利用客は駅から専有路に出て車両まで移動する 利用客がいない場合、本フローをスキップする	—
	⑦ 乗客または利用客は車両が停車していることを確認する	RO-PA-FB-02 RO-CU-FB-02
	⑧ 乗客または利用客から車両へ「車両のドアを開ける」を行う	PA-VE-CA-03 CU-VE-CA-01
	⑨ 車両ドアの状態が「閉じている」から「開いている」	—

3 システムの全体設計

3.1 各構成要素の詳細

「2.4 システム全体構成」に記載した各構成要素の役割・詳細を以下に示す。

3.1.1 管制

管制はインフラセンサから入力されたカメラ映像から人工知能による画像認識結果と、各機能との通信で入力された通知内容から運行状態を判定し、各機能への制御指示を行う。

基本動作は以下の通り。

・ 車両制御指示

車両へ移動、停車、非常停車、走行復帰の車両制御指示を行う。

管制の指示後、車両の状態通知が 2 秒以内に得られない場合には指示を再送する。

各指示を行う条件を下記に示す。

1. 移動

車両が走行可能状態であり、専有路上に障害物が無い事とホームドアが閉じた事を確認したら移動指示を行う。

2. 停車

車両が移動中状態であり、車両が駅に接近した事を検出したら駅から 90m の地点で車両が減速を開始できるように停車指示を行う。

車両が移動中、または走行可能状態であり、管制とインフラセンサの間に通信障害が発生した場合、車両に停車指示を出す。

車両が移動中、または走行可能状態であり、管制と車両の周期通信に障害が発生した場合、発生前の指示内容に関わらず停車指示を出す。

3. 非常停車

インフラセンサ経由で受けたカメラ映像内から障害物が検出された場合、または車両が検出できなくなった場合、運用員から環境逸脱報告を受けた場合のいずれかが発生したら非常停車指示を行う。

4. 走行復帰

運用員から走行復帰報告、または障害物除去報告を受けたら走行復帰指示を行う。

・ 運用員対応指示

運用員へ障害物除去、車両確認の指示を行う。

各指示を行う条件を下記に示す。

1. 障害物除去

インフラセンサ経由で受けたカメラ映像内から障害物が検出された場合、または車両から障害物検出通知を受けた場合のいずれかが発生したら指示を行う。

AEBS 安全コンセプト

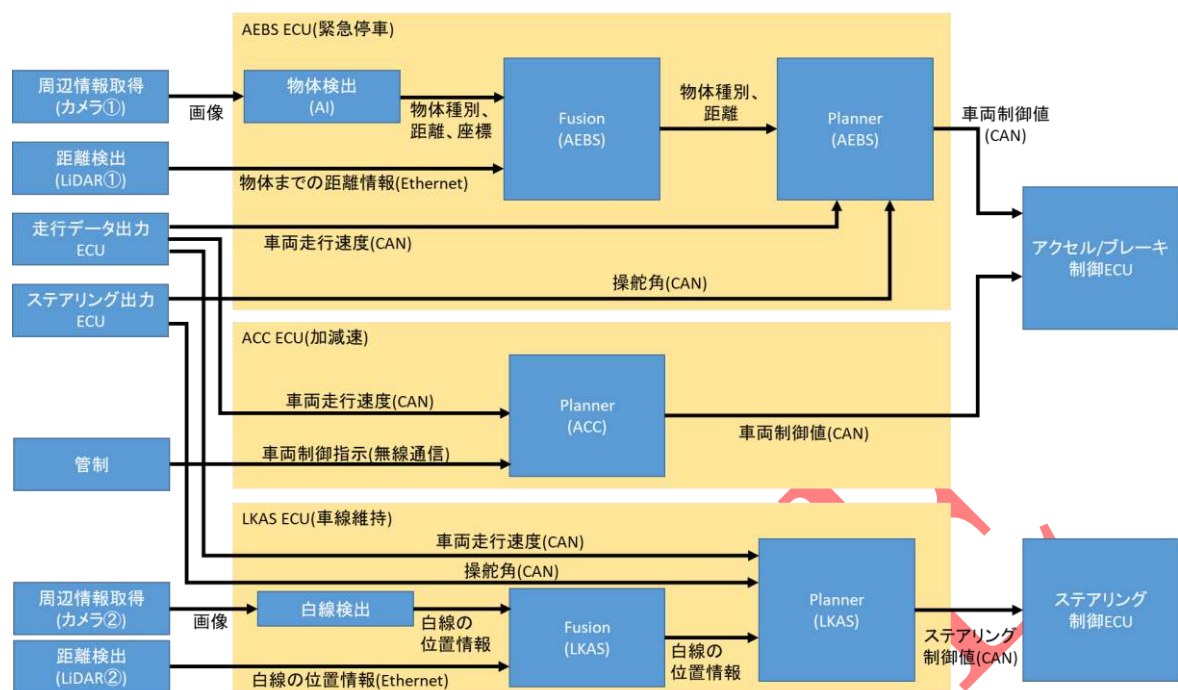
SAMPLE

版	作成日	変更内容	発行
1.0.0	2020/2/29	新規作成	WITZ
1.1.0	2020/6/9	関連文書更新、図の差し替え、誤記修正	WITZ
1.1.1	2020/10/15	関連文書更新（内容の更新はなし）	WITZ
1.1.2	2020/10/19	関連文書更新（内容の更新はなし）	WITZ

SAMPLE

目次

1	概要	1
1.1	目的	1
1.2	用語定義	1
1.3	準拠する規格	1
1.4	関連文書	1
2	自動運転車両の機能	2
2.1	各機能の概要	2
2.1.1	AEBS	2
2.1.2	ACC	2
2.1.3	LKAS	2
2.2	利用環境	2
2.3	システム構成	2
2.4	車両レベルでの共通原因故障	6
2.5	自動運転車両に割り当てる安全要求	7
3	AEBS 安全要求	8
3.1	安全目標の詳細化	8
3.2	機能安全要求	10
3.3	安全分析結果	13
4	システマティック故障対策	14
4.1	開発フェーズ全体像	14
4.2	①初期 AI コンポーネント開発	14
4.3	②コンセプトフェーズ	14
4.4	③システム設計	14
4.5	④ハードウェア・ソフトウェア開発	15
4.6	⑤AI 学習フェーズ	15
4.7	⑥統合試験	16



各機能ブロックの役割について以下に示す。

機能ブロック	役割
周辺情報取得(カメラ①)	自車両前方の状況を画像として取得し、出力する。
距離検出(LiDAR①)	自車両から周辺障害物までの距離を点群データとして出力する。
走行データ出力 ECU	車両走行速度を取得し、出力する。
ステアリング出力 ECU	操舵角を取得し、出力する。
管制	車両制御指示(移動、停車、非常停車)を出力する
周辺情報取得(カメラ②)	自車両前方の状況を画像として取得し、出力する。
距離検出(LiDAR②)	自車両から白線までの距離を点群データとして出力する。
物体検出(AI)	AI による画像認識を用いて物体検出を実施し、検出した物体の種別、画像上での座標位置、および車両から物体までの距離を出力する。
Fusion(AEBS)	距離検出の結果と物体検出の結果を統合し、障害物の確認結果として物体種別および距離を出力する。
Planner(AEBS)	Fusion の直前の 5 回の結果及び現在の車両走行速度、操舵角に応じて緊急停車の要否を決定し、必要な際に緊急停車命令を出力する。故障を検出した場合は非常停車命令を出力する。
Planner(ACC)	現在の車両走行速度及び管制の命令に応じて、目標速度または停車命令を出力する。
白線検出	画像処理による白線検出を実施し、白線の位置情報を出力する。

3 AEBS 安全要求

2.5 自動運転車両に割り当てる安全目標より、AEBS に割り当たる要求を詳細化する。

3.1 安全目標の詳細化

SG1：前方 30m に高さ 10cm 以上の障害物、人間、動物を検出した場合、3.5 秒以内に緊急停車する(ASIL B)

を、以下のサブ SG(以下 SSG)として詳細化する。

- SSG1：前方 30m にある高さ 10cm 以上の物体を検出する
- SSG2：物体の検出から 3.5 秒以内に緊急停車する
- SSG3：各機能ブロックにおいて算出した情報の信頼性を担保する
- SSG4：各機能ブロックの故障を検出した場合は非常停車する ※

※復帰処理は運用員によって行われるため、ここでは考えないものとする。

SG2：走行データ出力 ECU の故障を検出した場合は非常停車する

SG3：ステアリング出力 ECU の故障を検出した場合は非常停車する

SG4：アクセル/ブレーキ制御 ECU の故障を検出した場合は非常停車する

については、SSG4にまとめるものとする。

SSG1：前方 30m にある高さ 10cm 以上の物体を検出する

を詳細化する。

- SSG1-01：前方 30m にある高さ 10cm 以上の物体を検出すること。
- SSG1-02：LiDAR の距離情報と AI の距離情報が不一致の場合、LiDAR の情報を優先すること。

SSG2：物体の検出から 3.5 秒以内に緊急停車する

を詳細化する。

- SSG2-01：障害物が検出範囲に入ってから 300ms 以内に障害物検出を行うこと。
(障害物検出)
- SSG2-02：障害物検出を行ってから、100ms 以内に緊急停車の実行を判断すること。
(緊急停車判断)
- SSG2-03：緊急停車判断を行ってから、100ms 以内に命令を送信すること。
(緊急停車命令)
- SSG2-04：緊急停車を開始してから 3000ms 以内に停車すること。(緊急停車処理)

