D-Case モデリング環境連携

デモンストレーション

クルーズコントロールシステム仕様書

目次

1　概要 4
1.1　目的 4
1.2　用語定義 4
2　システム構成 4
2.1　システム構成の概要 4
2.2　システムを構成する主たる要素 4
3　機能概要 5
4　制約条件 5
4.1　開発プロセスの制約 5
4.2　システムの構成と制約 5
4.3　周辺システム、利用するハードウェアおよびソフトウェア 5
5　ユースケース 6
6　機能詳細 7
6.1　機能に関する要求 7
6.2　性能・品質に関する要求 7
6.3　機能安全に関する要求 8
7　ハザード分析 8
7.1　HAZOPによるハザード分析 8
7.2　FTAによるハザード分析 8
7.3　FMEAによる影響分析 9
8　機能ブロック概要 10
8.1　ブロック定義図 10
8.2　システムを構成する機能ブロック 10
8.3　ユースケースと機能ブロックの対応 12
8.4　制約との対応 13
8.5　ステートマシン図 16

変更履歴

変更日	変更内容
2014/01/27	作成

1　概要

1.1　目的

本ドキュメントでは、D-Case – SysML 連携のデモンストレーションに使用するクルーズコントロール開発の仕様について記載する。

1.2　用語定義

ID	用語・略号	正式表記	意味
1	CC	クルーズコントロール	アクセルペダルを踏み続けることなくセットした速度を維持する機能
2	PCS	プリ・クラッシュ・セーフティ	障害物との衝突回避を支援する機能

2　システム構成

2.1　システム構成の概要

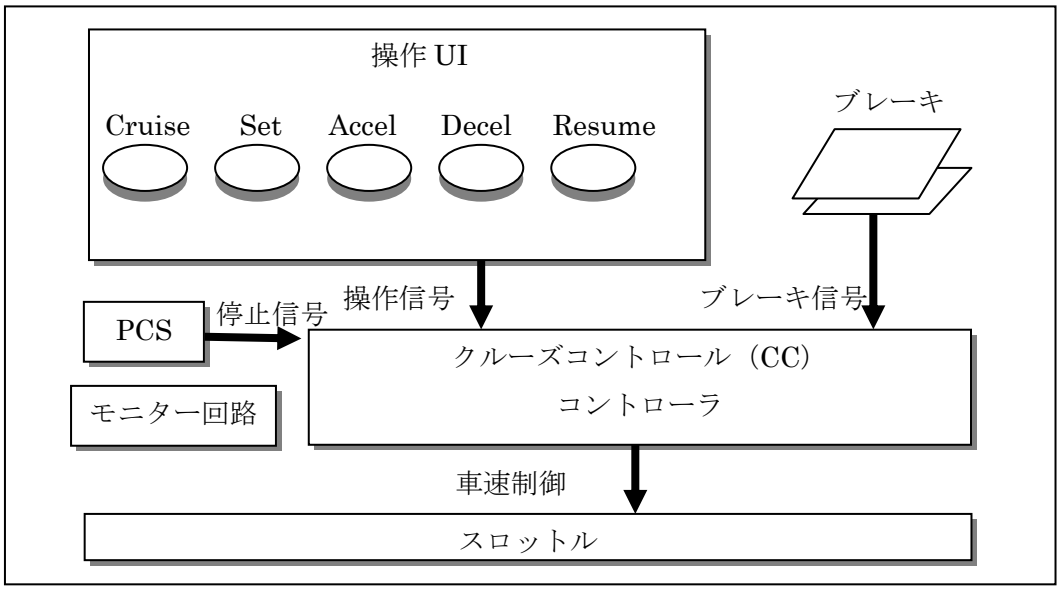

Figure 1　システム全体構成図

2.2　システムを構成する主たる要素

構成要素 ID	構成要素	概要
C_01	操作 UI	ドライバがクルーズコントロールを指示するためのボタンを配列した UI
C_02	ブレーキ	ドライバが車を減速または停止するための制動装置
C_03	CC コントロー	クルーズコントロールの制御方式を判断するため

	ラ	のコントローラ
C_04	スロットル	車速を制御するためのアクチュエータ
C_05	モニター回路	CC がドライバの操作通りに動作し、加速度が適正範囲内であることを監視する回路

3　機能概要

クルーズコントロール CC は、ドライバの指示を受け、走行制御を行うことで、走行の支援を実現する。

4　制約条件

4.1　開発プロセスの制約

- [CY_01] 前機種からの派生開発（差分開発）を行う。次機種では ISO 26262 準拠のため、機能安全の機能を追加する。
- [CY_02] クルーズコントロール（CC）は安全である。

4.2　システムの構成と制約

- [CY_11] クルーズコントロール CC は、操作 UI にクルーズの起動または停止を行うボタン、クルーズ復帰と加速開始と加速停止を指示するボタンで構成される。
- [CY_12] ドライバは、この操作 UI とブレーキから CC に指示を送る。
- [CY_13] ドライバは運転中、クルーズコントロールをいつでも指示できる。

4.3　周辺システム、利用するハードウェアおよびソフトウェア

種類	名称	バージョン
利用する OS	xxx	1.23

5　ユースケース

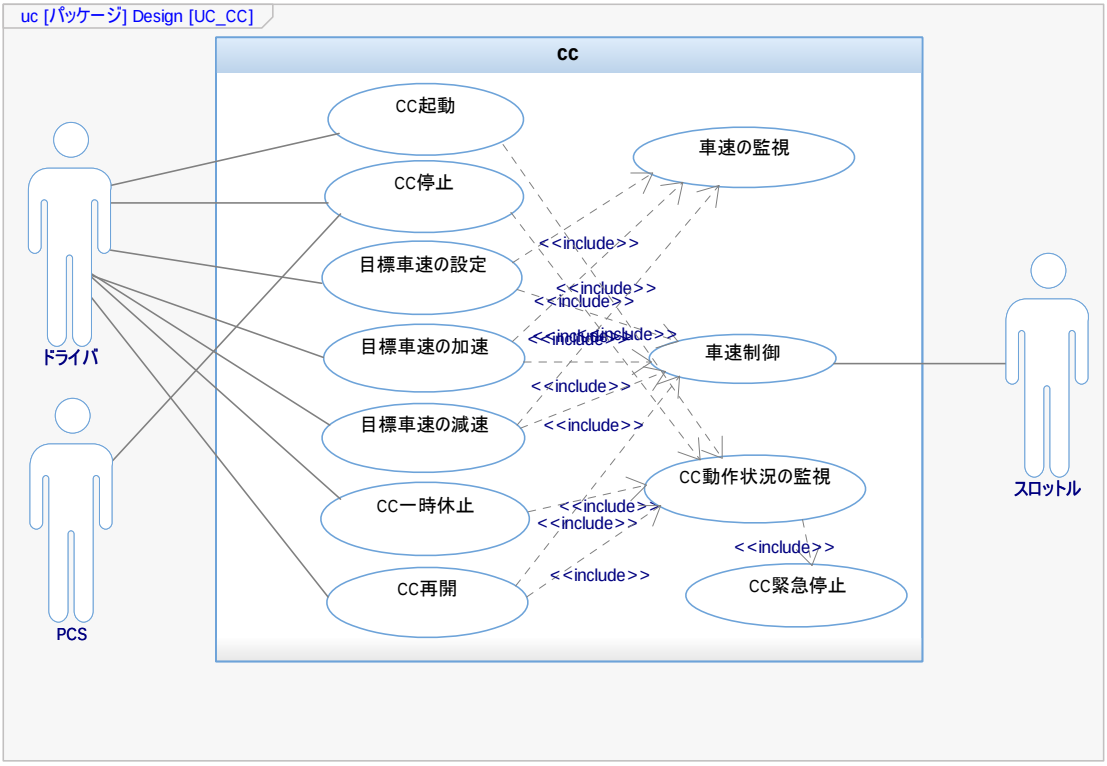

Figure 2　ユースケース図

ユースケース ID	ユースケース名	概要
UC_01	CC 起動	CC を起動する
UC_02	CC 停止	ドライバに制御を戻す
UC_03	目標車速の設定	目標車速を設定する
UC_04	目標車速の加速	目標車速の設定値を上げる
UC_05	目標車速の減速	目標車速の設定値を下げる
UC_06	CC 一時休止	一時的にドライバに制御を戻す
UC_08	CC 再開	一時休止していた CC を再開する
UC_09	車速制御	車速を制御する
UC_10	CC 動作状況の監視	CC の動作状況を監視する
UC_11	CC 緊急停止	異常を検知すると CC を緊急停止する
UC_12	車速の監視	車速を監視する

6　機能詳細

開発対象である CC プログラムによって、クルーズコントロール CC が以下の機能を実現することが要求される。

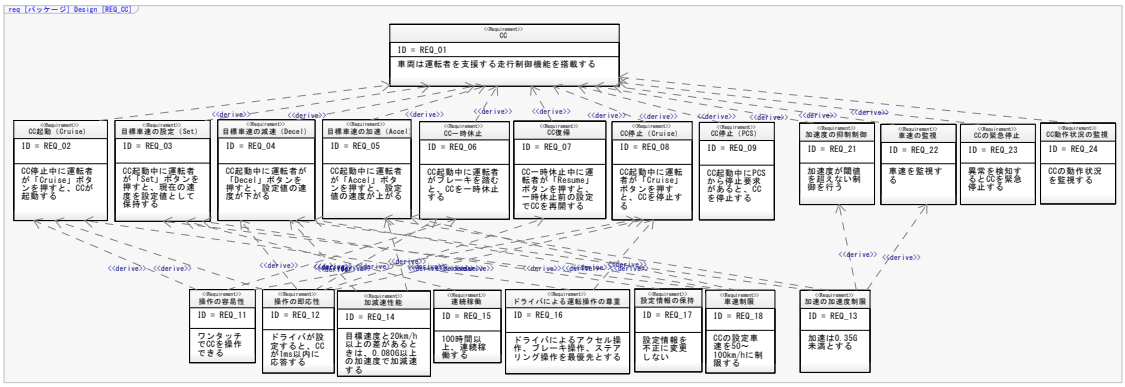

Figure 3　要求図

6.1　機能に関する要求

- [REQ_01] 車両は運転者を支援する走行制御機能を搭載する。
- [REQ_02] CC 停止中に運転者が「Cruise」ボタンを押すと、CC が起動する。
- [REQ_03] CC 起動中に運転者が「Set」ボタンを押すと、現在の速度を設定値として保持する。
- [REQ_04] CC 起動中に運転者が「Decel」ボタンを押すと、設定値の速度が下がる。
- [REQ_05] CC 起動中に運転者が「Accel」ボタンを押すと、設定値の速度が上がる。
- [REQ_06] CC 起動中に運転者がブレーキを踏むと、CC を一時休止する。
- [REQ_07] CC 一時休止中に運転者が「Resume」ボタンを押すと、一時休止前の設定で CC を再開する。
- [REQ_08] CC 起動中に運転者が「Cruise」ボタンを押すと、CC を停止する。
- [REQ_09] CC 起動中に PCS から停止要求があると、CC 停止する。

6.2　性能・品質に関する要求

- [REQ_11] ワンタッチで CC を操作できる。
- [REQ_12] ドライバが設定すると、CC が 1ms 以内に応答する。
- [REQ_13] 加速は 0.35G 未満とする。
- [REQ_14] 目標速度と 20km/h 以上の差があるときは、0.080G 以上の加速度で加減速する。
- [REQ_15] 100 時間以上、連続稼働する。
- [REQ_16] ドライバによるアクセル操作、ブレーキ操作、ステアリング操作を最優先とする。

- [REQ_17] 設定情報を不正に変更しない。
- [REQ_18] CC の設定車速を 50～100km/h に制限する。

6.3 機能安全に関する要求

- [REQ_21] 加速度が閾値を超えない制御を行う。
- [REQ_22] 車速を監視する。
- [REQ_23] 異常を検知すると CC を緊急停止する。
- [REQ_24] CC の動作状況を監視する

7 ハザード分析

7.1 HAZOPによるハザード分析

ID	制御出力	期待値からの逸脱状態（ガイドワード）	シチュエーション	ハザード
H_01	CC コントローラ	過大	CC 起動後	ドライバの意図より過大な加速度
H_02	CC コントローラ	不作動	CC 起動後のブレーキ時	ドライバの意図と異なる CC 動作

7.2 FTAによるハザード分析

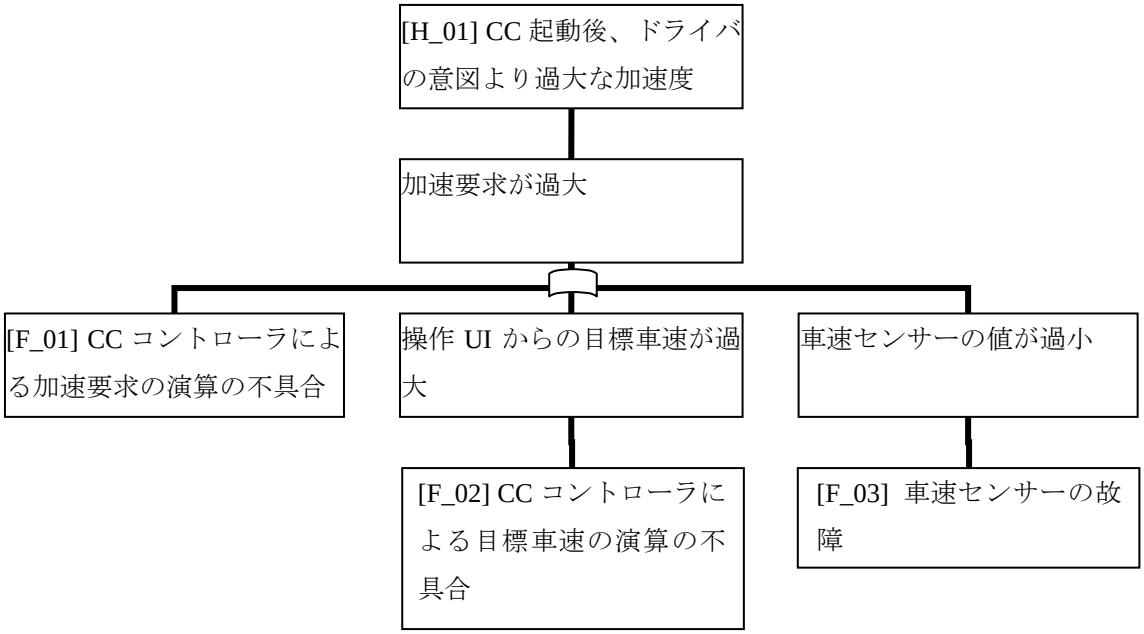

Figure 4 FTA 図（1）

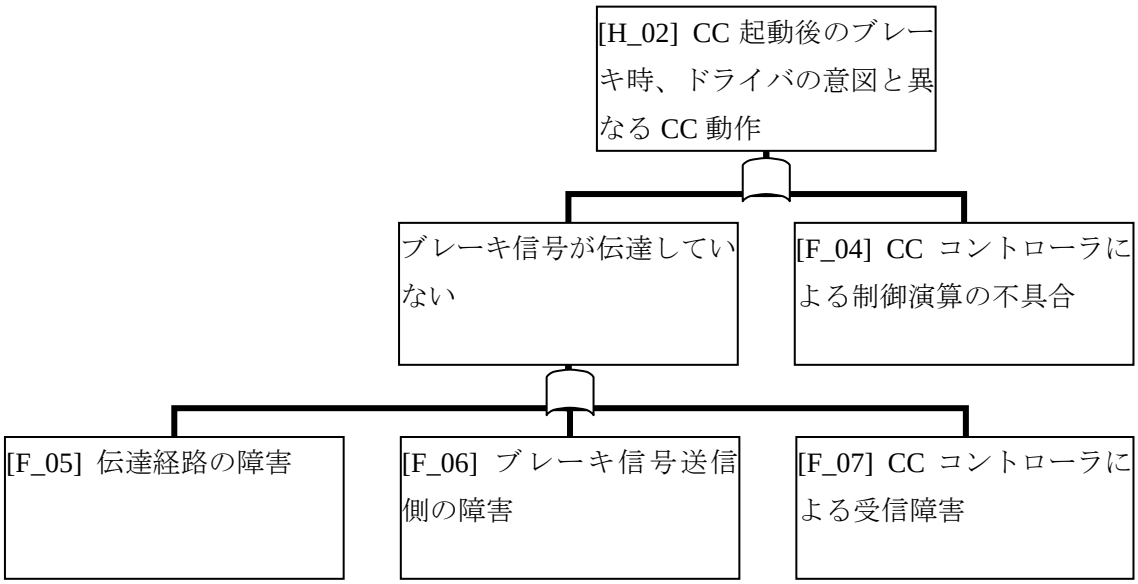

Figure 5　FTA 図（2）

7.3　FMEAによる影響分析

ID	コンポーネント	故障モード	要因	影響の深刻度	発生の頻度	検知の難易度	リスク優先度	処置	
								S/W	H/W
F_01	CC コントローラ	演算不具合（加速要求）	プログラム不具合	6（中）	1　（小）	5　（中）	30	[A_01] 加速度の抑制制御	[A_02] 車速のモニター回路
F_02	CC コントローラ	演算不具合（目標車速）	プログラム不具合	3（小）	1　（小）	1　（小）	3		
F_03	車速センサー	異常値	故障	9（大）	5　（中）	1　（小）	45	[A_03] CC の緊急停止	
F_04	CC コントローラ	演算不具合（制御）	プログラムミス	9（大）	1　（小）	1　（小）	9		[A_04] CC 動作状況のモニター回路
F_05	伝送経路	異常値	故障	9（大）	5　（中）	1　（小）	45		
F_06	ブレーキ	演算不具合（送信）	断線	9（大）	1　（小）	1　（小）	9		
F_07	CC コントローラ	演算不具合（受信）	断線	9（大）	1　（小）	5　（中）	45		

8　機能ブロック概要

8.1　ブロック定義図

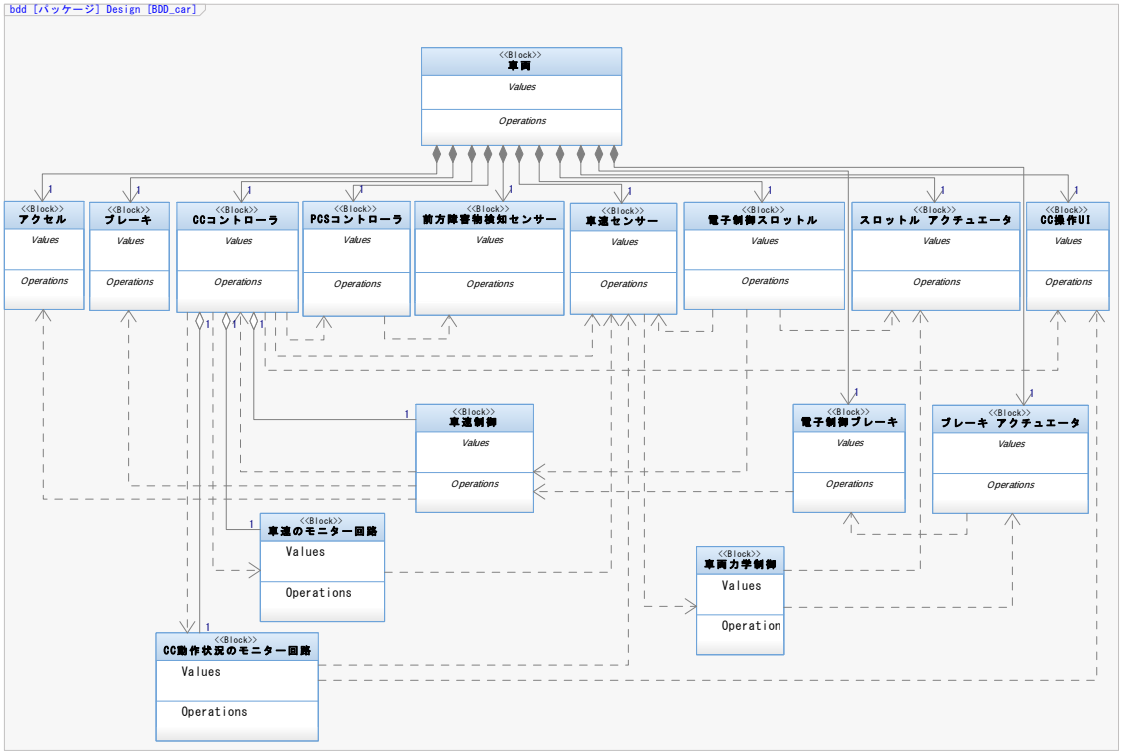

Figure 6　ブロック定義図

8.2　システムを構成する機能ブロック

機能ブロック ID	機能ブロック名	機能概要	役割分担	関連機能 ID
BL_01	CC コントローラ	クルーズコントロールを制御する	ソフト	BL_02 BL_08
BL_02	PCS コントローラ	プリクラッシュセーフティシステムを制御する	ソフト	BL_01
BL_03	ブレーキ	ブレーキ信号を CC に伝達する	通信：ソフト	BL_01
BL_04	前方障害物検知センサー	前方の障害物を検知し、PCS コントローラに伝達する	通信：ソフト	BL_03
BL_05	車速センサー	車速を CC コントローラに伝達する	通信：ソフト	BL_01
BL_06	電子制御スロットル	加速度要求をアクチュエータに伝達する	通信：ソフト	BL_07

BL_07	スロットルアクチュエータ	スロットル開度を駆動する	通信：ソフト	BL_06
BL_08	車両	CC を含む車両全体	ソフトとハード	BL_01
BL_09	CC 操作 UI	ドライバが指示した操作信号を CC に伝達する	操作 UI：ハード、通信：ソフト	BL_03
BL_10	車速のモニター回路	加速が適正範囲内であることを監視する	通信：ソフト、回路：ハード	BL_11
BL_11	車速制御	アクセルやブレーキ、CC コントローラの状態を基に、加速度要求を算出する	ソフト	BL_10
BL_12	車両力学制御	車両の速度と加速度をシミュレートする	ソフト	BL_05 BL_07
BL_13	アクセル	アクセル信号を CC に伝達する	通信：ソフト	BL_01
BL_14	CC 動作状況のモニター回路	CC がドライバの操作通りに動作し、加速度が適正範囲内であることを監視する	通信：ソフト、回路：ハード	BL_11
BL_15	電子制御ブレーキ	ブレーキ要求をアクチュエータに伝達する	通信：ソフト	BL_16
BL_16	ブレーキアクチュエータ	ブレーキを駆動する	通信：ソフト	BL_15

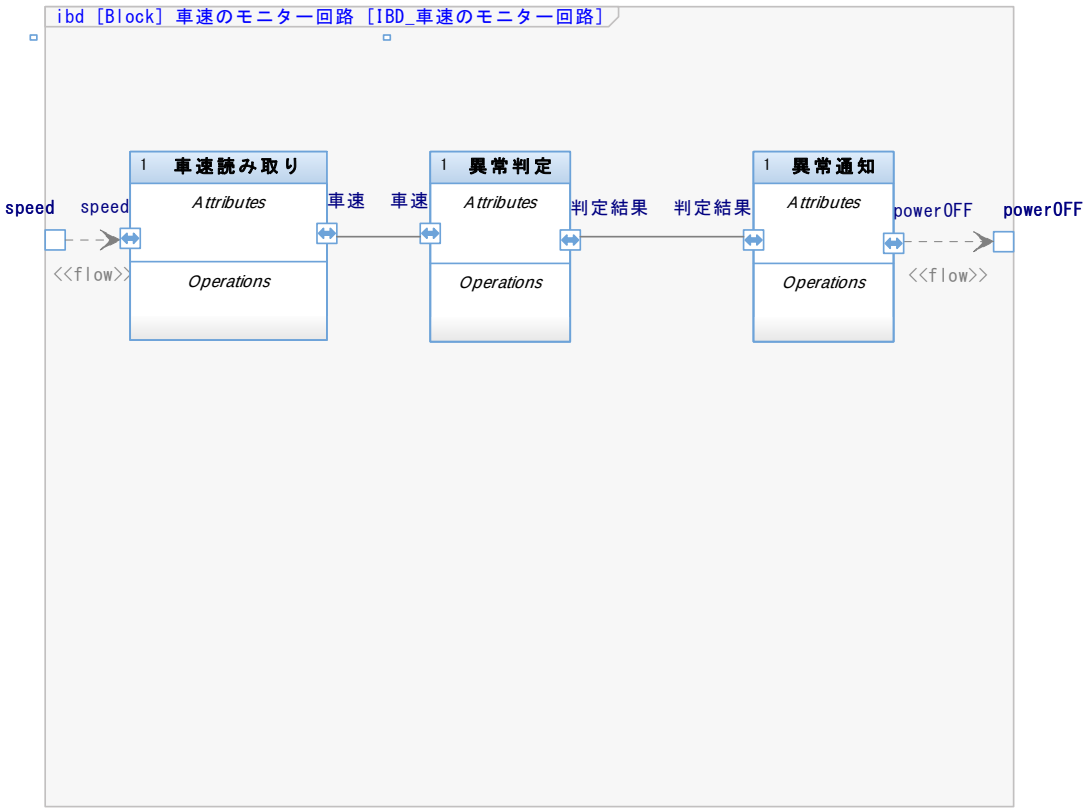

Figure 7　内部ブロック図

8.3　ユースケースと機能ブロックの対応

ユースケース ID	ユースケース名	機能ブロック ID	機能ブロック名
UC_01	CC 起動	BL_01 BL_09	CC コントローラ 操作 UI
UC_02	CC 停止	BL_01 BL_09	CC コントローラ 操作 UI
UC_03	目標車速の設定	BL_01 BL_05 BL_09	CC コントローラ 車速センサー 操作 UI
UC_04	目標車速の加速	BL_01 BL_09	CC コントローラ 操作 UI
UC_05	目標車速の減速	BL_01 BL_09	CC コントローラ 操作 UI
UC_06	CC 一時休止	BL_01 BL_03	CC コントローラ ブレーキ
UC_08	CC 再開	BL_01	CC コントローラ

		BL_09	操作 UI
UC_09	車速制御	BL_11	車速制御
UC_10	CC 動作状況の監視	BL_14	CC 動作状況のモニター回路
UC_11	CC 緊急停止	BL_01	CC コントローラ
UC_12	車速の監視	BL_10	車速のモニター回路

8.4 制約との対応

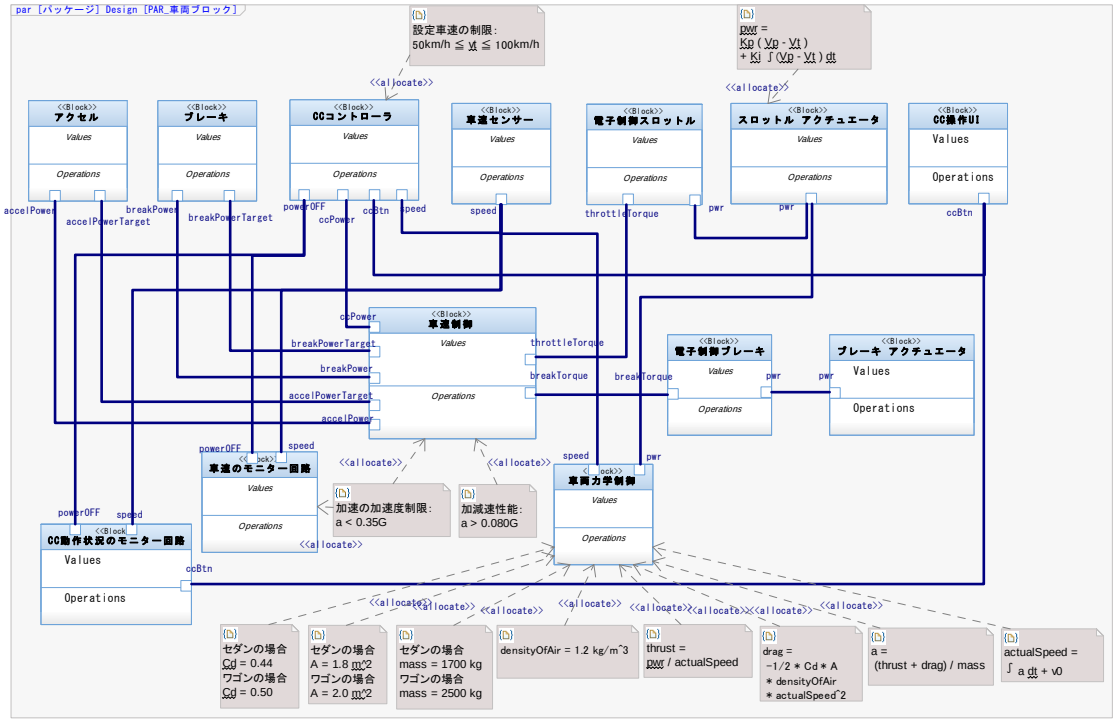

Figure 8 パラメトリック図

Figure 9　パラメトリック図（一覧）

制約ブロック ID	制約ブロック名	概要
PAR_01	制約-加速の加速度制限	加速の加速度制限： a < 0.35G
PAR_02	制約-加減速性能	加減速性能： a > 0.080G
PAR_03	制約-車速制限	設定車速の制限： 50km/h ≦ vt ≦ 100km/h
PAR_04	制約-PI制御	pwr = Kp (Vp - Vt) + Ki ∫(Vp - Vt) dt
PAR_05	制約-投射面積の参考値	セダンの場合 A = 1.8 m^2 ワゴンの場合 A = 2.0 m^2
PAR_06	制約-車重の参考値	セダンの場合

		mass = 1700 kg ワゴンの場合 mass = 2500 kg
PAR_07	制約-Cdの参考値	セダンの場合 Cd = 0.44 ワゴンの場合 Cd = 0.50
PAR_08	制約-空気密度の参考値	densityOfAir = 1.2 kg/m^3
PAR_09	制約-推進力	thrust = pwr / actualSpeed
PAR_10	制約-抵抗力	drag = -1/2 * Cd * A * densityOfAir * actualSpeed^2
PAR_11	制約-運動方程式	a = (thrust + drag) / mass
PAR_12	制約-速度	actualSpeed = ∫ a dt + v0

8.5　ステートマシン図

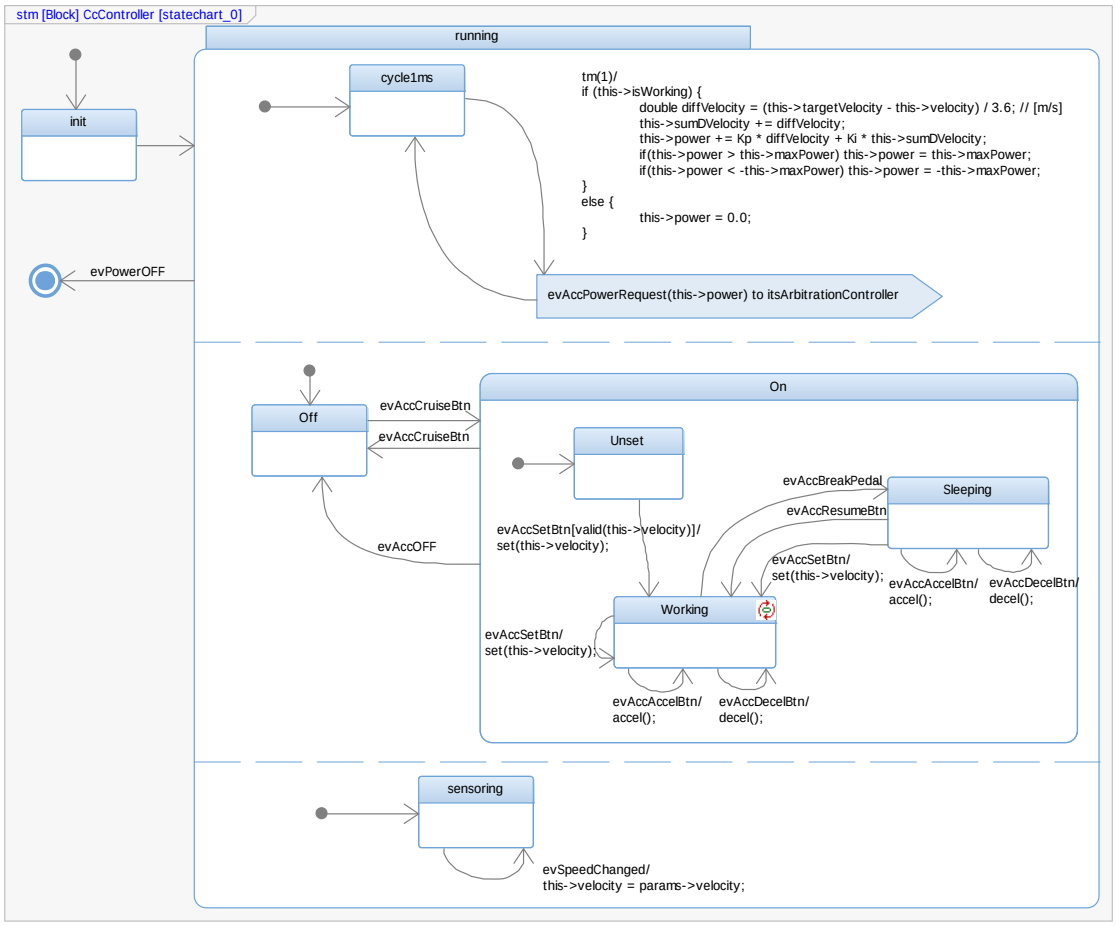

Figure 10　ステートマシン図