SCDLと他の手法との連携について

2023/11/29

SCDL活用のための手法連携SWG
発表者：ジヤトコ（株）　島中茂樹

活動メンバ

○：資料の作成＆編集者

	会社名	氏名（昇順）
○	（株）チェンジビジョン	岩永　寿来
○	おおた開発効率化プロジェクト	小笠原　豊和
	（株）デンソー	酒井　英子
○	マレリ（株）	佐々木　喜好
○	ジヤトコ（株）	島中　茂樹
○	トヨタ自動車（株）	関　康大
	（株）OTSL	田中　伸明
○	日立Astemo（株）	長谷川　直人
	（株）構造計画研究所	宮本　秀徳
○	DNV ビジネス・アシュアランス・ジャパン（株）	山下　修平
	アンソレイエ（株）	（故）内山　幹康

他　3名

もくじ

1.活動の背景と目的

自動車分野の電気／電子システムのアーキテクチャ開発では、以下のような記法や分析手法が活用されている。

記法:
- SCDL
- SysML
- UML
- EAST-ADL
- など

分析手法:
- DFMEA
- FMEA-MSR
- DRBFM
- FTA
- STAMP/STPA
- など

SCDLは機能安全専用か？
SCDLと他の手法との組み合わせ方は？

アーキテクチャ開発において、SCDLと他の手法との協調や共存について考察が必要

2.ケーススタディの前提条件

- システム開発のスタート　～　安全設計に繋がる部分　の　一連の流れをスタディ
- 仮想システムを事例に ケーススタディ実施

やってみた！

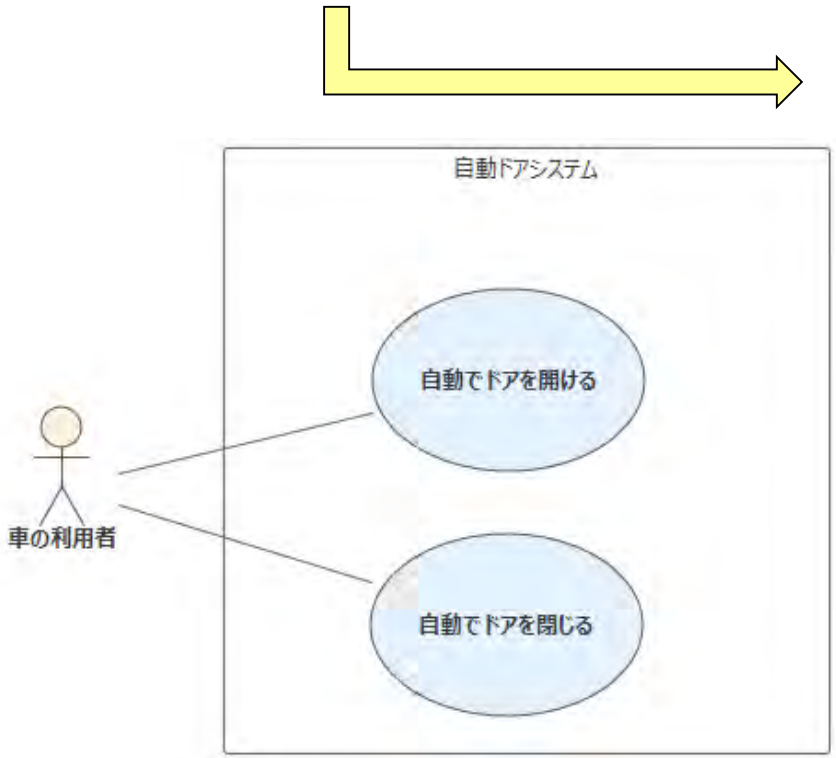
注：
本事例は、SCDLと他の手法との連携などについて考察したものであり、分析順序、連携させた情報なども「あくまで参考」であり、連携手順や方法論などを示すためのものでは無い事に注意

2.1ケーススタディで扱った仮想システム

開発に取り組んだ事例を紹介する。

取り組んだ仮想のシステムとは？

・「車両の自動開閉ドアシステム」　：手を使わずにドアを開閉できるシステム

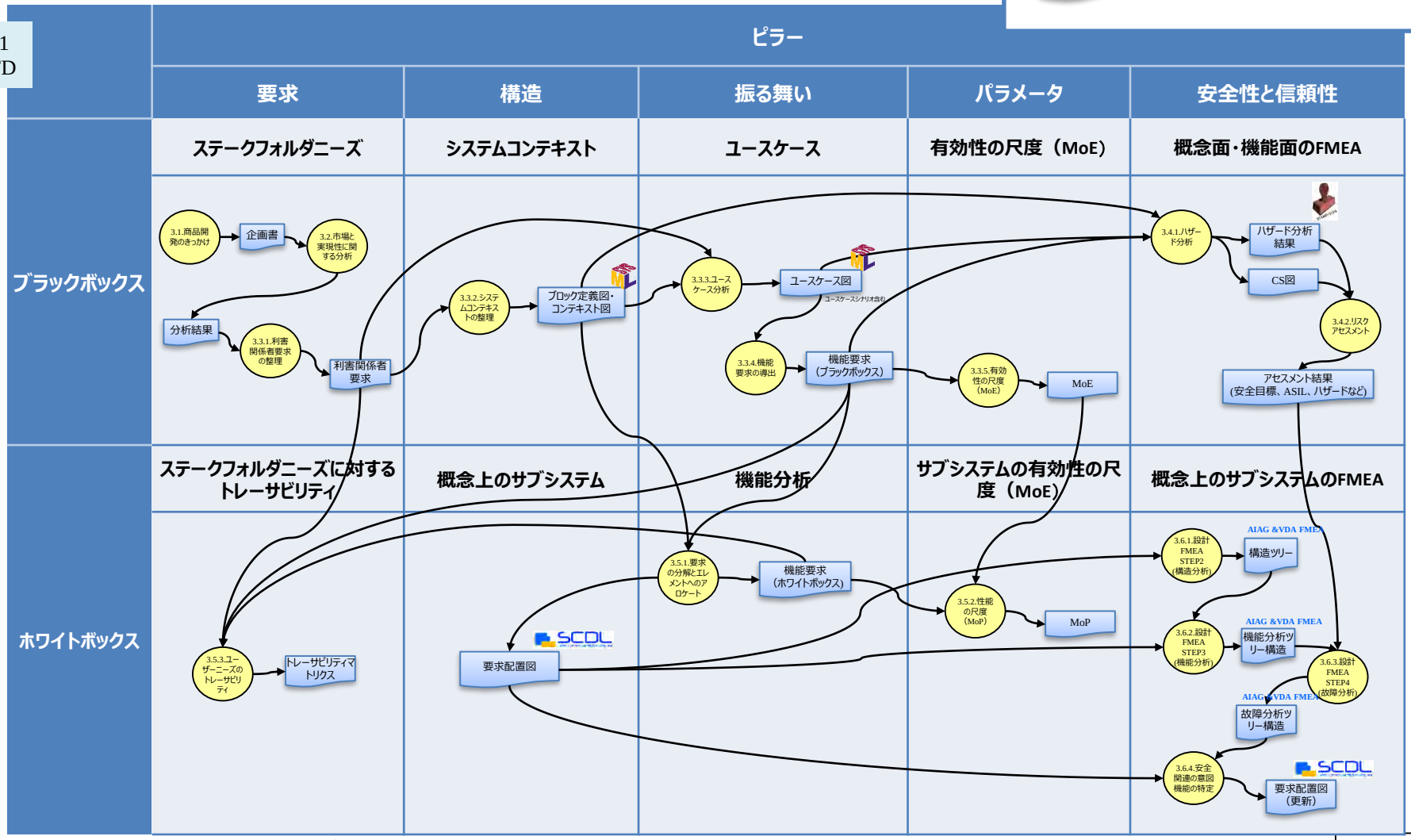


ドア種類：「ヒンジドア」

2.2ケーススタディで扱ったプロセス

※MBSEの活動で広く知られているMagicGrid上に　扱ったプロセスのマッピングを行った。
　尚、本事例はMagicGridに準拠した活動を行ったわけではないため、参考情報とする。

図1
PFD



（MagicGrid上にマッピングしたPFD）

3 .ケーススタディ

ケーススタディに用いた事例

✓ 仮想システム：「車両の自動開閉ドアシステム」

システム開発のスタート ～ 安全設計に繋がる部分 の 一連の流れをスタディ

（ブラックボックスの視点）

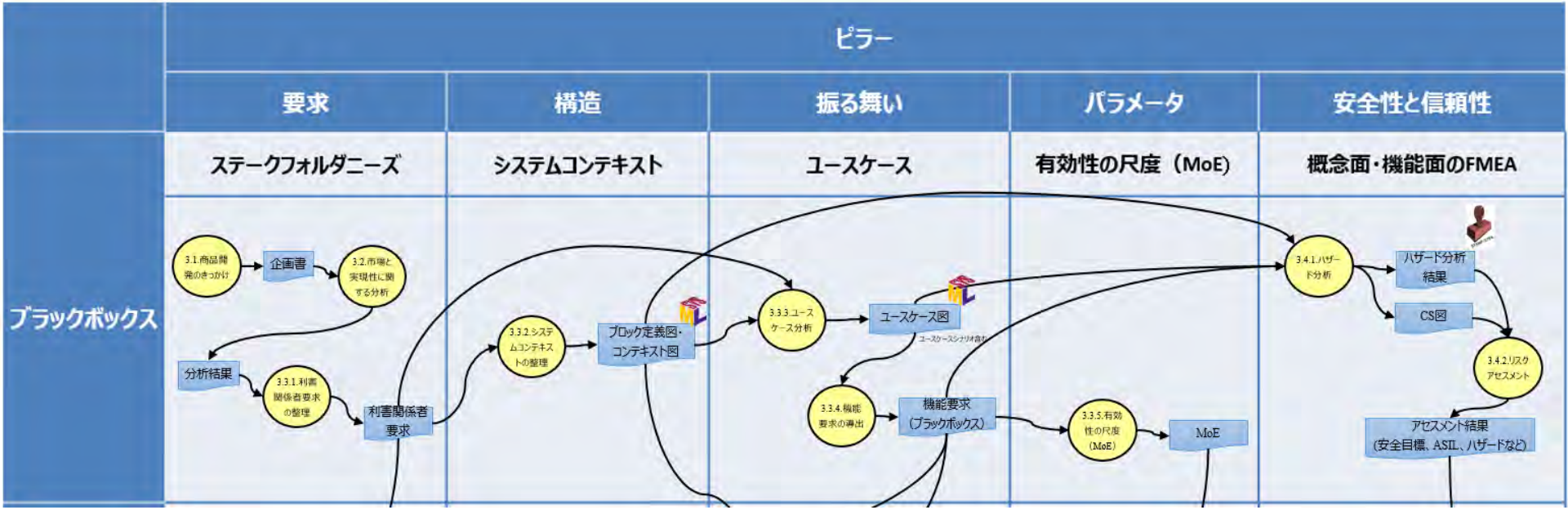
3.1 商品開発のきっかけ
3.2 市場と実現性に関する分析
3.3 対象システム(SoI：System of Interest)の分析（その１）
3.4 ハザード分析＆リスクアセスメント

（ホワイトボックスの視点）

3.5 対象システム(SoI：System of Interest)の分析（その２）
3.6 設計FMEAと安全関連の意図機能の特定

ブラックボックス視点による分析

（MagicGrid上にマッピングしたPFD）



（ブラックボックスの視点）

- 3.1 商品開発のきっかけ
- 3.2 市場と実現性に関する分析
- 3.3 対象システム(SoI：System of Interest)の分析（その１）
- 3.4 ハザード分析＆リスクアセスメント

3.1.商品開発のきっかけ

- 誰が？：自動車メーカーのR&D部門に勤めるAさん
- 何するの？：悪天候の中、知人宅に頼まれものを届けようと自宅マンションの駐車場に停めてある車で出かけようとする。
- どうなった？：傘と荷物を持ちながらドアを開け、荷物を車の中に入れようとドアから手を離した瞬間に突風が吹き、隣の車にドアをぶつけてしまった。

ヤバイよ！
ヤバイよ！

- ニーズ：風が強い日でも狭い隙間で安心して乗り降りできる自動開閉ドアの付いた車が欲しい！

⇩ 商品化できないかな？

商品企画部門の友人に相談し　市場性と実現性について分析をすることにした。

はじまり　はじまり

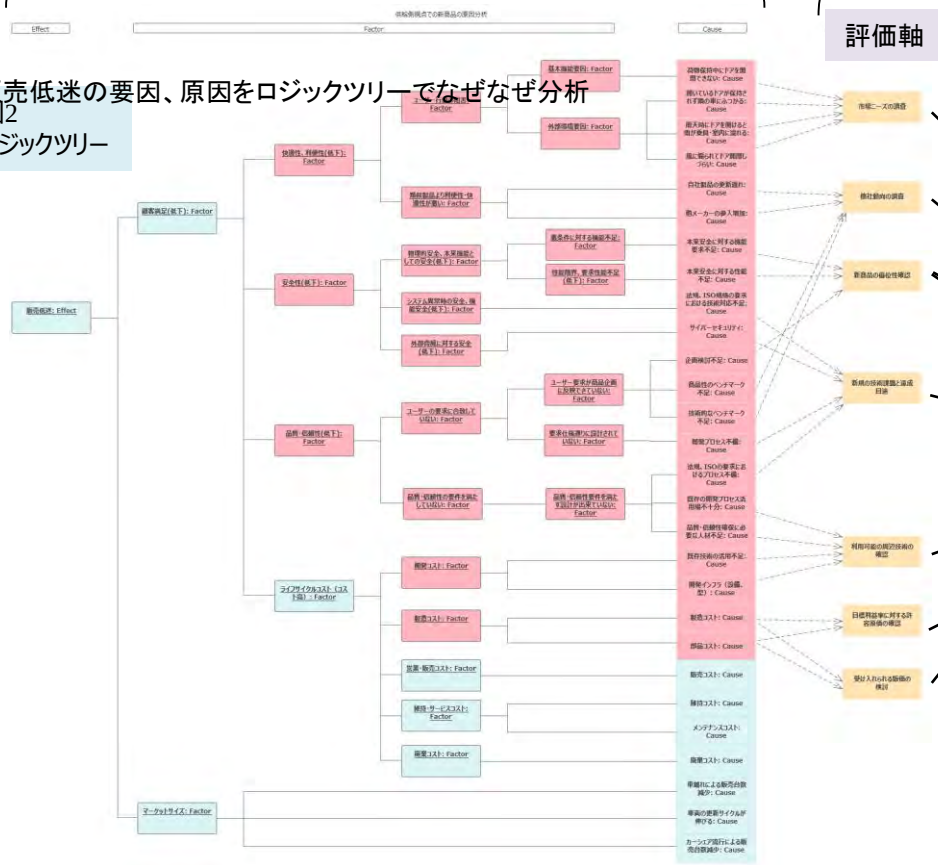
3.2.市場と実現性に関する分析

市場性や実現性を見極めるため、販売低迷に陥る要因、原因をロジックツリーで分析して評価。

How：ロジックツリー分析

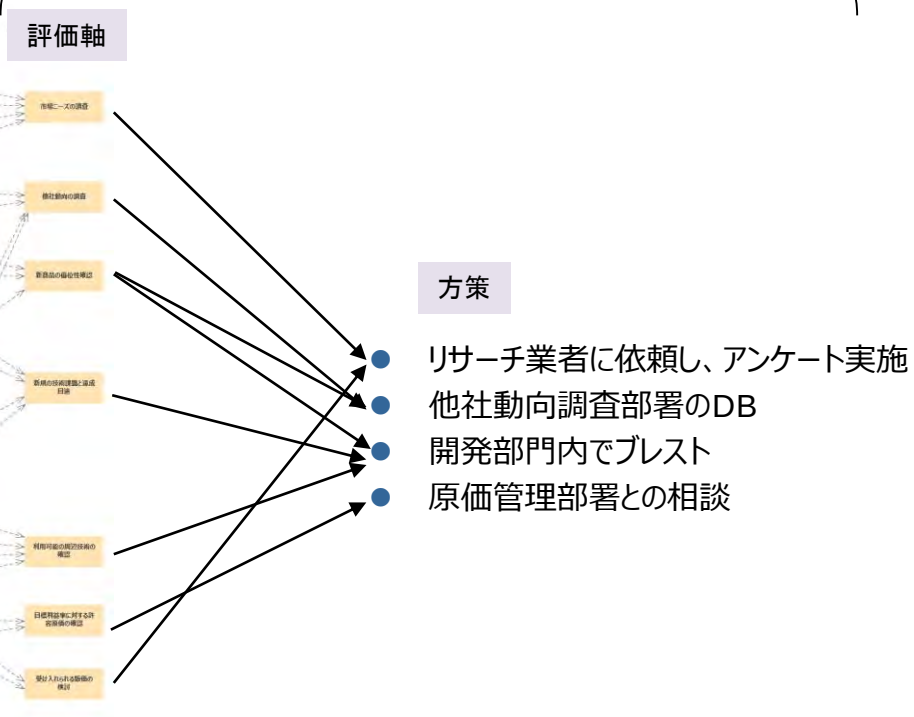
特性（Effect）、要因（Factor）、原因（Cause）の切り口で分析

原因の評価軸に対し　以下の方策で分析、評価



販売低迷の要因、原因をロジックツリーでなぜなぜ分析

図2
ロジックツリー



3.2.市場と実現性に関する分析

前頁の方策を用い　分析、評価した結果

ユーザーニーズ：

- 手がふさがっている時に　手を使わずにドアを開閉したい
- ドアが隣の車にぶつからないように維持してくれると助かる

許容販価：

- 10万円（原価管理部署との相談で許容原価は5万円）

新商品の優位性：

- ヒンジタイプのドアを開くものはない
- 自動で開くものはあるが、自動で閉じるものはない

使えそうな自社技術、技術的課題：

- 自動運転車では自車周辺の障害物が把握できる
- ドア開閉、ドア開状態の維持は自社技術が応用できる
- 開閉意図の読み取り方に課題がある

3.2.市場と実現性に関する分析の気づき、考察

で、どんな感じだった？

ロジックツリー分析（系統図）についての気づき、考察

- 開発する商品の販売低迷リスクに対し、なぜなぜで深堀りし、その原因を防止するための活動に結び付ける活動がスタディできた。

- 自動車開発では商品プロジェクトに複数の組織が参画している。
  作業の分担や、トレーサビリティを意識した本分析、評価手法は有効と考える。

3.3.対象システム(SoI：System of Interest)の分析（その１）

利害関係者ニーズ実現のために、 対象システム(SoI)が何をすべきかを明確化

What：

システムに求められる機能要求、非機能要求の導出

How：

こんな流れで 分析してみた！

- 利害関係者要求の整理：3.3.1.表を用いて整理
- システムコンテキストの整理：3.3.2.コンテキスト図を用いて整理
- ユースケース分析：3.3.3.ユースケース図と、ユースケースシナリオで整理
- SoIに必要となる機能要求の導出：3.3.4.表を用いて整理
- SoIの機能要求に対する有効性の尺度（MoE）の導出：3.3.5.表を用いて整理

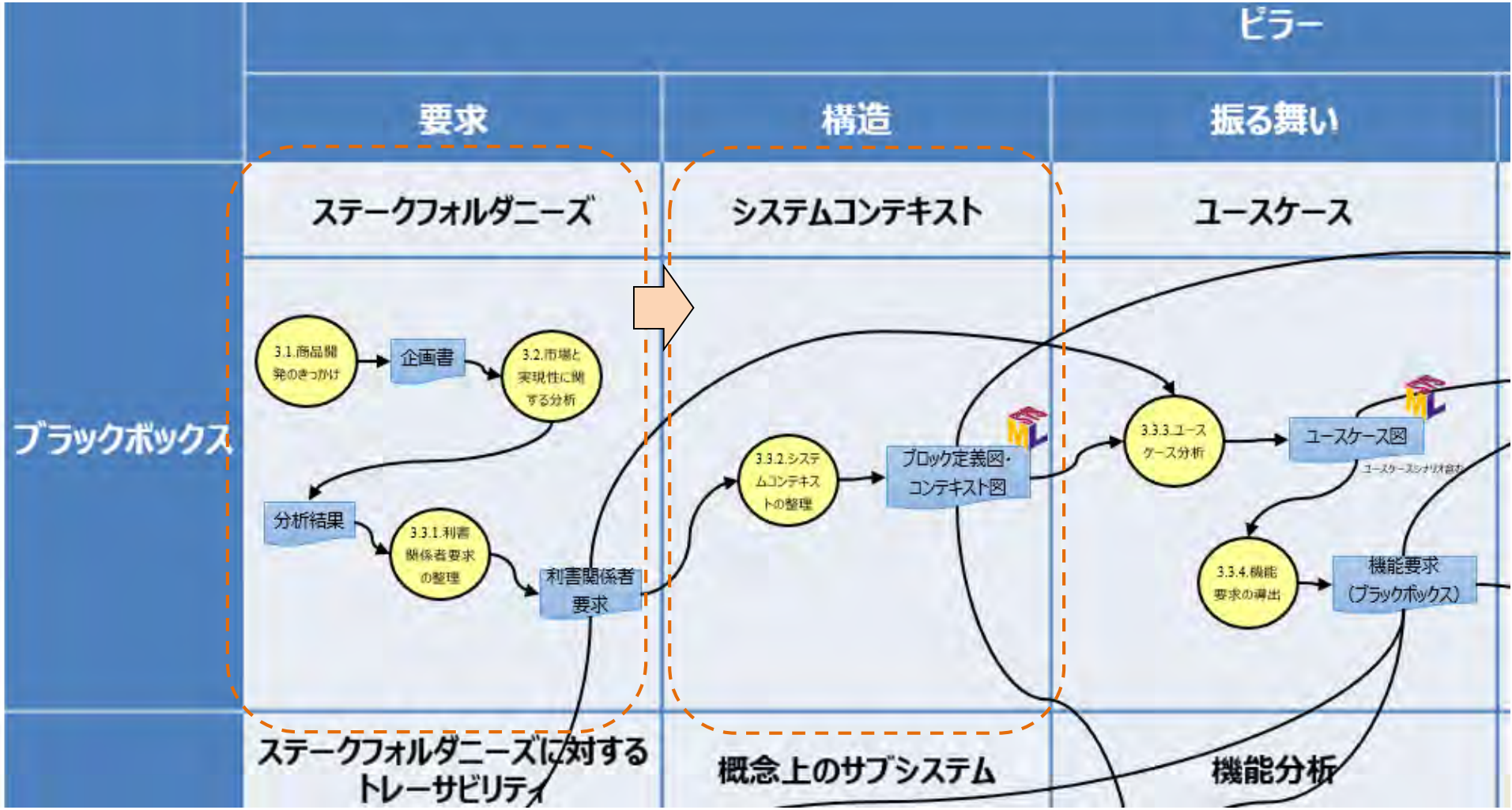
3.3.1.利害関係者要求の整理

利害関係者ニーズとシステム要求の分析結果

表1

利害関係者	（利害関係者の）ニーズ	（システムに対する）要求	
車の利用者	手を使わずにドアを開閉したい	非接触でドア開を行う	機能要求
		非接触でドア閉を行う	機能要求
		開閉動作中にドア動線上の人・物に接触しないようにする	機能要求
		手動での開閉を優先する	機能要求
	利用しないときは機能をOFFにしたい	不要時に作動を禁止する	機能要求
システム提供者	安全性を担保したい	ISO26262 第2版に準拠	非機能要求
	コストは抑えたい	コストUP 5万円以下	非機能要求

（MagicGrid上にマッピングしたPFD)



3.3.2.システムコンテキストの整理

システム、利用者、環境などとの　関係や相互作用　→　コンテキスト図で可視化

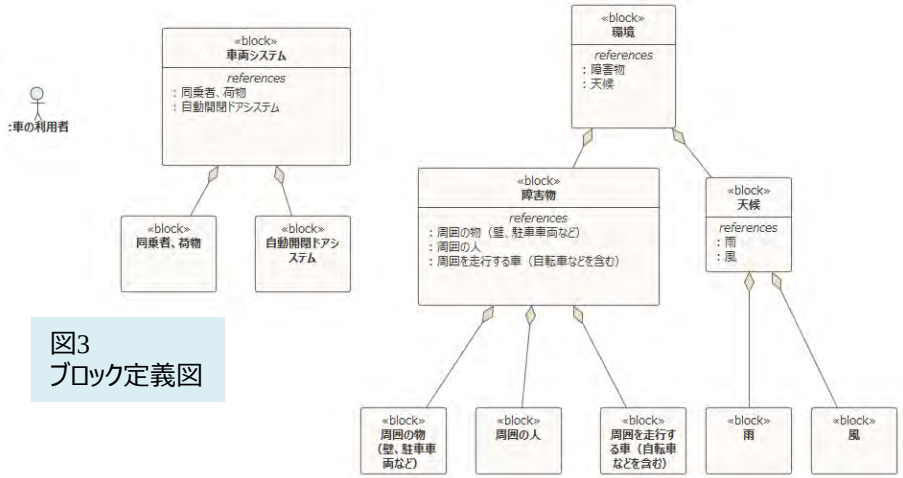


図3
ブロック定義図

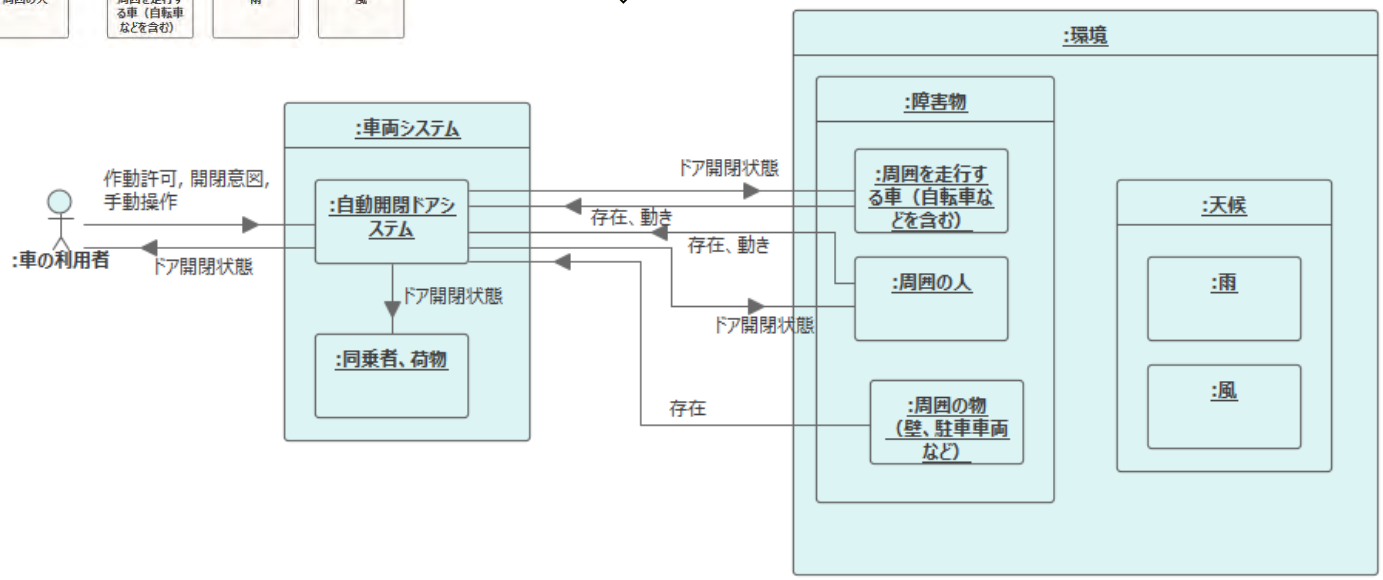


図4
コンテキスト図

3.3.3.ユースケース分析

システムに求められる機能を明らかにするためのアプローチとしてユースケース分析に取り組んだ。

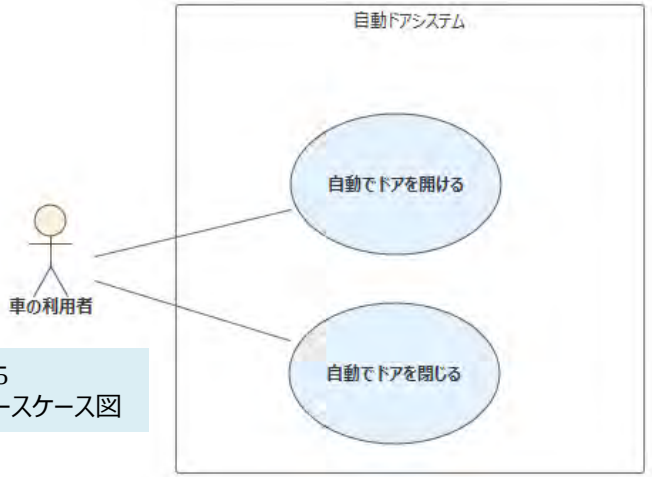


図5
ユースケース図

表2，3
ユースケースシナリオ

開いた後にドアを維持

ユースケース名		自動でドアを開ける
概要		手がふさがっているときに自動でドアを開き、車両への乗り降りをサポートする。 また、ドアが開いている状態を維持し、ドアが動くことで周囲の物にぶつかるのを防止する。
アクター		車の利用者
開始条件		システム利用許可状態で、利用者が近くにいる場合に開始
事前条件		・自動開閉ドアシステムに電源が供給されている ・利用者が特定できる。 ・車の利用者がシステムの作動を許可している ・車のドアが全て閉じている
イベントフロー	メインフロー	1　アクターがシステムに自動でドアを開く要求をする 2　システムは利用者のドアを開閉意思を検出する 3　システムは、ドアを開いても危険がないことを判定し、最も利用者に近いドアを開く。（代替a,b）（例外ｃ） 4　開いたドアの位置を維持する
	代替フローa	利用者が手動でドアを開く場合 3.1a　アクターがドアを手動で開こうとした場合は、手動のドア開閉を優先する 3.2b　4に戻る
	代替フローb	開くドアの作動範囲に障害物がある場合 3.1b　システムがドアの作動範囲に障害物があると検知する 3.2b　システムは障害物とぶつからない位置までドアを開く 3.3b　4に戻る
	例外フローc	システムの利用可能条件を満たさない場合 3.1c　システムは利用可能条件を満たしていない場合(※1)は、自動ドアシステムが作動しないことをアクターに通知する 3.2c　システムはユースケースを中断する 事後条件 ・システムは待機状態戻っていること ・アクターにシステムの動作条件を満たしていないことが通知されていること
事後条件		ドアが開いた状態で維持されていること
終了条件		システム利用禁止状態　または、利用者が近くにいない場合に終了
備考		※1　利用可能条件 ・停車状態 ・システム正常状態

ユースケース名		自動でドアを閉じる
概要		手がふさがっているときに自動でドアを閉じ、車両への乗り降りをサポートする。
アクター		車の利用者
開始条件		システム利用許可状態で、利用者が近くにいる場合に開始
事前条件		・自動開閉ドアシステムに電源が供給されている ・利用者が特定できる。 ・車の利用者がシステムの作動を許可している ・車のいずれかのドアが開いている
イベントフロー	メインフロー	1　アクターがシステムに自動でドアを閉じる要求をする 2　システムは利用者のドアを開閉意思を検出する 3　システムは、ドアを閉じても危険がないことを判定し、最も利用者に近いドアを閉じる。（代替a）（例外b）
	代替フローa	利用者が手動でドアを閉じる場合 3.1a　アクターがドアを手動で閉じようとした場合は、手動のドア開閉を優先する 3.2a　ユースケースを終了する
	例外フローb	システムの利用可能条件を満たさない場合 3.1b　システムは利用可能条件を満たしていない場合(※1)は、自動ドアシステムが作動しないことをアクターに通知する 3.2b　システムはユースケースを中断する 事後条件 ・システムは待機状態戻っていること ・アクターにシステムの動作条件を満たしていないことが通知されていること
事後条件		ドアが閉じていること
終了条件		システム利用禁止状態　または、利用者が近くにいない場合に終了
備考		※1　利用可能条件 ・システム正常状態

3.3.4.機能要求の導出

ユースケース分析の結果

↓

システムに求められる機能要求を整理

→

14個の機能要求が導出された

表4

対象システムに必要な機能要求
(01)作動の許可禁止を判定する
(02)ドア開閉状態を判定する
(03)利用者の意図を検出する
(04)利用者の位置を検出する
(05)自動開閉するドアを判定する
(06)自動でドアを開閉する
(07)周囲の状況を判断する
(08)ドアの開角度調整をする
(09)走行中であることを判断する
(10)ドア開閉可否を判定する
(11)手動操作を判定する
(12)手動操作を優先判定する
(13)ドア開角度を維持する
(14)利用者を特定する

←

3.3.5.で、対象システムの機能要求に求められる（定性的な）性能などを有効性の尺度（MoE）として定義

3.3.5.有効性の尺度（MoE）

対象システムに求められる（定性的な）性能など

MoEを定義し、機能要求に対し定義モレが無いことをマトリクス表でチェック

表5

	機能要求-MoE	MoE																	
		IGN SW ON/OFF切り替えが可能	イライラせず、危険を感じない速度	ドアが開いていることを判定可能	ドアが閉じていることを判定可能	ドアを開いても危険がないときだけ許可	ドアを開くと危険かどうかを判定する	ドアを閉じると危険かどうかを判定する	開いているドア位置を維持可能	手動でドアを開けたり閉じたりする要求を判断可能	手動操作された場合は自動開閉を禁止する	障害物がある場合はぶつからないところまで開く	対象となるドアの数と位置を識別可能	直ぐに反応	停車中でドアを開いても危険がないときだけ許可	停車中と走行中を識別可能	利用者がどのドアを操作したいか判別可能	利用者が許可・禁止を切り替え可能	利用者のドアに対する意図を判定可能	利用者を特定可能
機能要求	(01)作動の許可禁止を判定する	1																1		
	(02)ドア開閉状態を判定する			1	1															
	(03)利用者の意図を検出する																		1	
	(04)利用者の位置を検出する																1			
	(05)自動開閉するドアを判定する												1				1			
	(06)自動でドアを開閉する		1									1		1						
	(07)周囲の状況を判断する						1	1				1								
	(08)ドアの開角度調整をする											1								
	(09)走行中であることを判断する															1				
	(10)ドア開閉可否を判定する					1									1					
	(11)手動操作を判定する									1										
	(12)手動操作を優先判定する										1									
	(13)ドア開角度を維持する								1											
	(14)利用者を特定する																			1

3.3.対象システム(SoI)の分析（その１）の気づき、考察

で、どんな感じだった？

3.3.3.ユースケース分析の気づき、考察

ユースケース分析について以下の2つのステップが考えられる

①意図機能のユースケース分析

メインフロー、代替フローを意図機能の振る舞いとし、意図機能アーキテクチャの構築に役立てる

②例外フローを用い安全機構を含むユースケース分析

意図機能アーキを安全分析した結果、必要な安全機構をユースケース記述の例外フローとして記述する

②に関し、今回のスタディでは例外フローの深堀り、それとSCDLとの連携について検討しなかった。

安全機構の検討にSCDLを適用した事例は、SCDL仕様書の附属書に載っているので参考にしてください。
SCDL仕様書（ASAM仕様書ではなく、旧版のVer1.5）は以下サイトからダウンロード可能です。
https://ssl.scn-sg.com/main/ja/scdl-specification

3.3.対象システム(SoI)の分析（その１）の気づき、考察

で、どんな感じだった？

3.3.4.機能要求の導出の気づき、考察

ISO26262

✓ 既存のアーキテクチャ（PAA）を活用した派生開発を考慮

MagicGrid

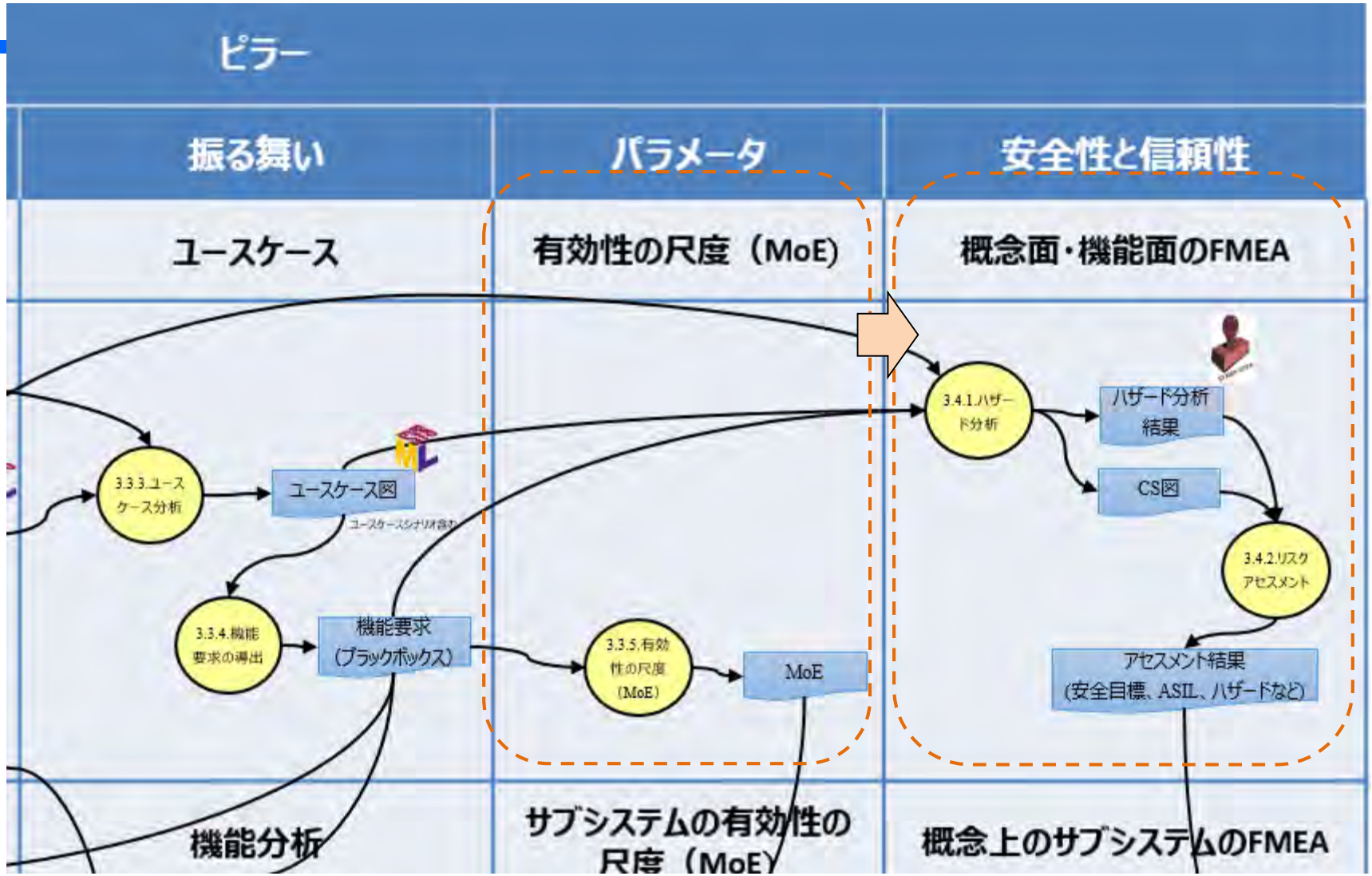
✓ 既存のアーキテクチャにとらわれずに展開

上記の違いをあまり意識せず、途中で既存のアーキテクチャ（PAA）を活用した活動に切り替えてしまった。「反省」

その結果、ここで導出した14個の機能要求はあまり活用されなかった。

PAA：preliminary architectural assumptions（初期アーキテクチャ前提）

（MagicGrid上にマッピングしたPFD)



3.4.ハザード分析＆リスクアセスメント

対象システムの安全目標を決定する。

How：

ハザード分析

- 対象システムの機能不全のふるまいにより引き起こされる危険事象を相互作用を考慮しながら網羅的に識別するために、STAMP/STPAを用いて分析することにした。（3.4.1項）

STAMP/STPA 使ってみた！

- 前提条件表
- アクシデント・ハザード・安全制約表
- コンポーネント抽出表、コントロールストラクチャ(CS)図
- Unsafe Control Action(UCA)表

リスクアセスメント

- ハザード分析の結果に対しリスク評価し、識別された許容できないリスクに対して安全目標を定義することにした。（3.4.2項）

3.4.1.ハザード分析（前提条件表）

対象システムを理解するために　前提条件表を用いて整理する。

表6
前提条件表

ID	名前
Pre-1	IGN ONで、システム許可で、ドアが全て閉状態で開始
Pre-2	IGN OFF又は、システム禁止したら終了
Pre-3	利用者のドア開意図を検出し、停車中　且つ　ドアを開けても危険がないと判断されれば利用者に最も近いドアを開する
Pre-4	ドア開の角度によって、障害物とのクリアランスがなくなる場合は、クリアランスを確保できる角度まで開する
Pre-5	利用者のドア閉意図を検出し、ドアを閉じても危険がないと判断されれば利用者に最も近いドアをドアを閉する
Pre-6	ドア閉により自車及び周囲に危害を加えるときは自動閉しない
Pre-7	利用者の手動ドアを開閉操作は優先される
Pre-8	ドアが開いた状態（自動開、手動開を問わない）で開始。ドアが開いた状態を維持する

で、どんな感じだった？

■ 気づき、考察

ユースケースシナリオでも代用可能

3.4.1.ハザード分析（アクシデント、ハザード、安全制約の識別）

分析対象システムのアクシデントと、それにつながるハザードを明確にし、それに対する安全制約を整理する。

ｱｸｼﾃﾞﾝﾄID	アクシデント	ハザードID	ハザード	安全制約ID	安全制約
A1	急にドアが開き人が転げ落ちる	H1	意図せずドアが開く	SC1	ユーザーにドアを開ける意志がない限りドアを開かない
A1	急にドアが開き人が転げ落ちる	H1	意図せずドアが開く	SC2	ユーザーにアイテムの異常を認識させる
A1	急にドアが開き人が転げ落ちる	H2	システムの作動許可条件外で作動する	SC2	ユーザーにアイテムの異常を認識させる
A1	急にドアが開き人が転げ落ちる	H3	意図したよりドアの開くタイミングが遅い	SC3	ドアが開くタイミングは常に一定である
A1	急にドアが開き人が転げ落ちる	H3	意図したよりドアの開くタイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる
A1	急にドアが開き人が転げ落ちる	H4	ドア付近の障害物の検知が途中で止まる	SC2	ユーザーにアイテムの異常を認識させる

省略

A25	ドアが更に開きドアが周囲の物にぶつかる	H6	ドアの開位置が維持できない	SC2	ユーザーにアイテムの異常を認識させる
A25	ドアが更に開きドアが周囲の物にぶつかる	H16	手動操作と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A25	ドアが更に開きドアが周囲の物にぶつかる	H18	ドアの開閉状態が伝わらない	SC2	ユーザーにアイテムの異常を認識させる
A25	ドアが更に開きドアが周囲の物にぶつかる	H18	ドアの開閉状態が伝わらない	SC5	手動でドア開閉できる
A26	外からドアを開けようとしたときにすぐ開かずに様子見で近づいたときにいきなりドアが開き、ぶつかる	H3	意図したよりドアの開くタイミングが遅い	SC3	ドアが開くタイミングは常に一定である
A26	外からドアを開けようとしたときにすぐ開かずに様子見で近づいたときにいきなりドアが開き、ぶつかる	H3	意図したよりドアの開くタイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる

表7
アクシデント・ハザード・安全制約表

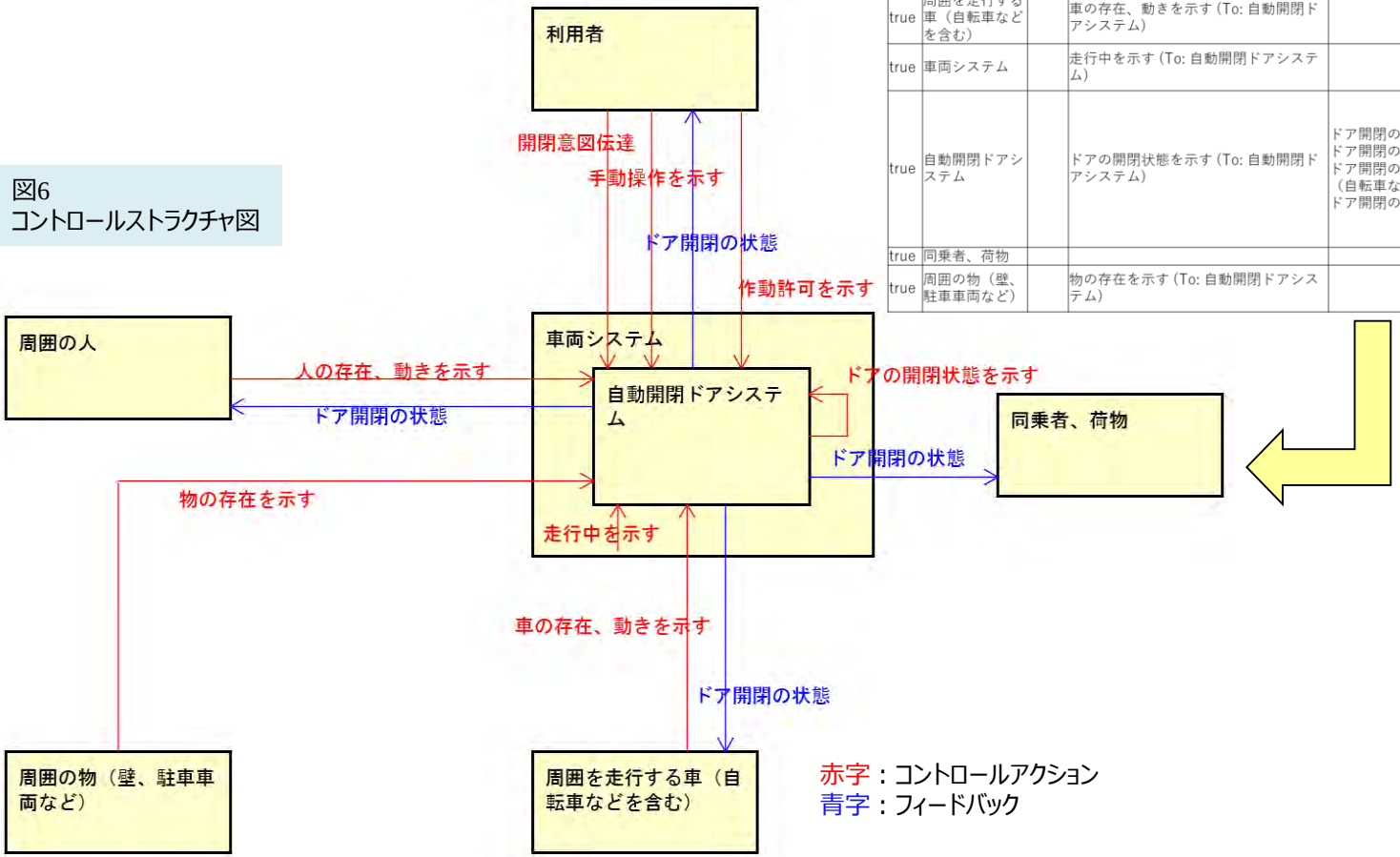
3.4.1.ハザード分析（CS図）

分析対象の構造とその依存関係をコンポーネント抽出表を用いて把握し、その結果をもとにコントロールストラクチャー図を作成する。

対象	登場人物	責務	コントロールアクション	フィードバック	入出力	備考
true	利用者		開閉意図伝達（To: 自動開閉ドアシステム） 手動操作を示す（To: 自動開閉ドアシステム） 作動許可を示す（To: 自動開閉ドアシステム）			
true	周囲の人		人の存在、動きを示す（To: 自動開閉ドアシステム）			
true	周囲を走行する車（自転車などを含む）		車の存在、動きを示す（To: 自動開閉ドアシステム）			
true	車両システム		走行中を示す（To: 自動開閉ドアシステム）			
true	自動開閉ドアシステム		ドアの開閉状態を示す（To: 自動開閉ドアシステム）	ドア開閉の状態（To: 利用者） ドア開閉の状態（To: 周囲の人） ドア開閉の状態（To: 周囲を走行する車（自転車などを含む）） ドア開閉の状態（To: 同乗者、荷物）		
true	同乗者、荷物					
true	周囲の物（壁、駐車車両など）		物の存在を示す（To: 自動開閉ドアシステム）			

表8
コンポーネント抽出表

図6
コントロールストラクチャ図



3.4.1.ハザード分析（UCA表）（Unsafe Control Action表）

コントロールアクション毎に4つのガイドワードで、そのコントロールアクションがどのようなハザード/アクシデントにつながるか？ を分析
&
安全制約との関連付け

ハザードにつながり得る制御動作の不具合を識別するためUCA表を用いて分析

表9
UCA表

No	CA コントロールアクション	From	To	CA提供条件	Not Providing	Providing causes hazard	Too early / Too late	Stop too soon / Applying too long
1	開閉意図伝達	利用者	自動開閉ドアシステム		(UCA1-N-1) 利用者の開閉意図が伝わらず、自動開閉が行われない [SC2][SC5]	(UCA1-P-1) 利用者の開閉意図が無いのに自動開閉が発生する [SC1][SC2][SC7]	(UCA1-T-1) 利用者の意図と異なるタイミングで自動開閉が発生する [SC2][SC5][SC3]	(UCA1-D-1) 意図した状態にドア開閉されない（途中で止まってしまう） [SC2][SC5]
2	人の存在、動きを示す	周囲の人	自動開閉ドアシステム		(UCA2-N-1) 周囲の人の存在や動きが伝わらず、ドア開閉によりぶつかる [SC1][SC2][SC7]	(UCA2-P-1) 周囲に人が存在しないのに誤認識して自動ドア開閉が実施されない [SC2][SC5]	(UCA2-T-1) 人の存在や動きの認識が遅れ、ドア開閉によりぶつかる [SC2][SC5]	(UCA2-D-1) 人の存在や動きの存在の通知が途中で止まってしまい、ドア開閉が始まりぶつかる [SC2]
3	車の存在、動きを示す	周囲を走行する車（自転車などを含む）	自動開閉ドアシステム		(UCA3-N-1) 周囲の車の存在や動きが伝わらず、ドア開によりぶつかる [SC2] (UCA3-N-2) 周囲の車の存在や動きが伝わらず、ドア開を避けて事故になる [SC2]	(UCA3-P-1) 周囲に車が存在しないのに誤認識して自動ドア開閉が実施されない [SC2][SC5]	(UCA3-T-1) 車の存在や動きの認識が遅れ、ドア開によりぶつかる [SC2][SC3]	(UCA3-D-1) 車の存在や動きの存在の通知が途中で止まってしまい、ドア開が始まりぶつかる [SC2]
4	物の存在を示す	周囲の物（壁、駐車車両など）	自動開閉ドアシステム		周囲の物の存在が伝わらずドアが開きドアや周囲の物に傷がつく	(UCA4-P-1) 障害物を誤検知し、意図したがドアが開かず、熱中症になるなどする [SC2][SC5]		
5	走行中を示す	車両システム	自動開閉ドアシステム		(UCA5-N-1) 走行中に急にドアが開き、乗員が落下する [SC2]	(UCA5-P-1) 走行中と誤判定し、停車しているのに自動でドアが開かない [SC2][SC5]		
6	手動操作を示す	利用者	自動開閉ドアシステム		(UCA6-N-1) 手動操作が優先されず手動開閉できない [SC2][SC5]	(UCA6-P-1) 手動操作が誤判定され自動開閉が行われない [SC2] (UCA6-P-2) 手動操作が誤判定されドア開維持されない [SC2]		
7	作動許可を示す	利用者	自動開閉ドアシステム		(UCA7-N-1) 作動許可が伝わらず、自動開閉されない [SC2]	(UCA7-P-1) 作動許可が誤判定され許可条件外で自動開閉してしまう [SC2]		
8	ドアの開閉状態を示す	自動開閉ドアシステム	自動開閉ドアシステム		(UCA8-N-1) ドア開の状態が伝わらずドア開が維持されない [SC2] (UCA8-N-2) ドアの開閉状態が伝わらず自動開閉が実施されない [SC2][SC5]	(UCA8-P-1) ドアの開閉状態が逆に伝わり自動開閉が実施されない [SC2][SC5]		

3.4.2.リスクアセスメント

ハザード分析にて抽出したアクシデントに対し、不合理なリスクを避けるために、危険事象ごとにシビアリティ（S） ,曝露の確率（E） , コントローラビリティ（C）の評価と それに基づくASILの決定と、安全目標、安全状態の導出を行った。（詳細は割愛）

リスクアセスメントの例を以下に示す

表10

ハザードID	ハザード	アクシデントID	アクシデント	ハザーダスイベントID	ハザーダスイベント	遭遇頻度E	回避可能性C	重篤度S	FTTI	ASIL	安全状態ID	安全状態	安全目標ID	安全目標
H2	システムの作動許可条件外で作動する	A1	急にドアが開き人が転げ落ちる	HE1	乗員乗車中かつ自車走行中に意図せずドアが開く。	E3:乗車中 E4：自車走行中 ⇒全体のE：E3	C1：シートベルト着用	S2~S3：路上に転落する(重傷～致命傷)		QM～ASIL A	SS1	手動開閉に切り替える	SG1	意図せず自動でドアが開かないようにする。
											SS2	ユーザーがシステムの異常を認識する		
				HE2	乗員乗車中かつ自車停止中に意図せずドアが開く。	E3：乗車中 E4：自車停止中 ⇒全体のE：E3	C1：ドアに寄りかからない C1：荷物の確実な収納	S1～S2：路上に転落する(軽傷～重傷)		QM		—		—
		A2	急にドアが開き物が転げ落ちる	HE1	乗員乗車中かつ自車走行中に意図せずドアが開く。	E3:乗車中 E4：自車走行中 ⇒全体のE：E3	C1：荷物の確実な収納	S0：物の落下のみ		QM		—		—
				HE3	乗員が乗車していない、かつ自車停止中に意図せずドアが開く。	E4：乗車なし ⇒全体のE：E4	C1：荷物の確実な収納	S0：物の落下のみ		QM		—		—
		A8	ドアが開き物が盗まれる	HE25	自車停止中、乗員が近くにいないときにドアが意図せず開く。	E4：自車停止中 E4：乗員ナシ ⇒全体のE：E4	C3：回避行動不可能	S0：盗難のみなので負傷しない		QM		—		—
		A18	閉じたドアに人が挟まれる	HE27	ユーザーがドア可動域にあるときに、ドアが意図せず閉まる。	E3：ドアが開いている E4：ドア付近に人がいる ⇒ドア開と人の存在は独立でないので、全体のEはE3	C2：ドアに挟まれるの回避するのは十分可能（容易かどうかは？）	S1～S2：軽傷もしくは骨折程度		ASIL A	SS1	手動開閉に切り替える	SG5	意図せず自動でドアが閉じないようにする。
											SS2	ユーザーがシステムの異常を認識する		

3.4.2.リスクアセスメント

SG毎にリスクアセスメントした結果を整理した例を以下に示す。

表11

安全目標ID	安全目標	ハザードID	SG侵害の原因となる　ハザード	最高ASIL
SG1	意図せず自動でドアが開かないようにする。	H1	意図せずドアが開く ※「人・車の進路にドアが開いている」を包含する	ASIL C
		H2	システムの作動許可条件外で作動する	
		H3	意図したよりドアの開くタイミングが遅い	
		H4	ドア付近の障害物の検知が途中で止まる	
		H5	走行中が判定できない	
		H6	ドアの開位置が維持できない	
		H7	ドアの開く速度が速い	
		H8	障害物の検出タイミングが遅い	
		H9	ドア付近の障害物を検知しない	
		H10	障害物の検出距離が実測より長い	
SG2	意図せずドアが開かないことがないようにする。	H11	意図したのにドアが開かない	ASIL B
		H15	走行中と誤判定する	
		H17	システムが作動許可にならない	
		H18	ドアの開閉状態が伝わらない	
		H19	ドアの開閉状態が逆に伝わる	
		H20	手動操作が優先されない	
SG3	意図より遅い速度でドアが閉じないようにする	H21	ドアが閉じる速度が遅い	
SG4	意図より速い速度でドアが閉じないようにする	H23	ドアが閉じる速度が速い	
SG5	意図せず自動でドアが閉じないようにする。	H2	システムの作動許可条件外で作動する	ASIL A
		H6	ドアの開位置が維持できない	
		H9	ドア付近の障害物を検知しない	
		H24	意図しないのにドアが閉じる	
SG6	意図より速い速度でドアが開かないようにする	H7	ドアの開く速度が速い	
SG7	意図せず自動でドアが閉じないことがないようにする。	H16	手動操作と誤判定する	
		H17	システムが作動許可にならない	
		H18	ドアの開閉状態が伝わらない	
		H19	ドアの開閉状態が逆に伝わる	
		H22	閉まり切らずにドアが途中で止まる	
		H25	意図したのにドアが閉じない	
		H26	意図よりドアの閉じるタイミングが遅い	

3.4.ハザード分析＆リスクアセスメントの気づき、考察

で、どんな感じだった？

3.4.1.ハザード分析の気づき、考察

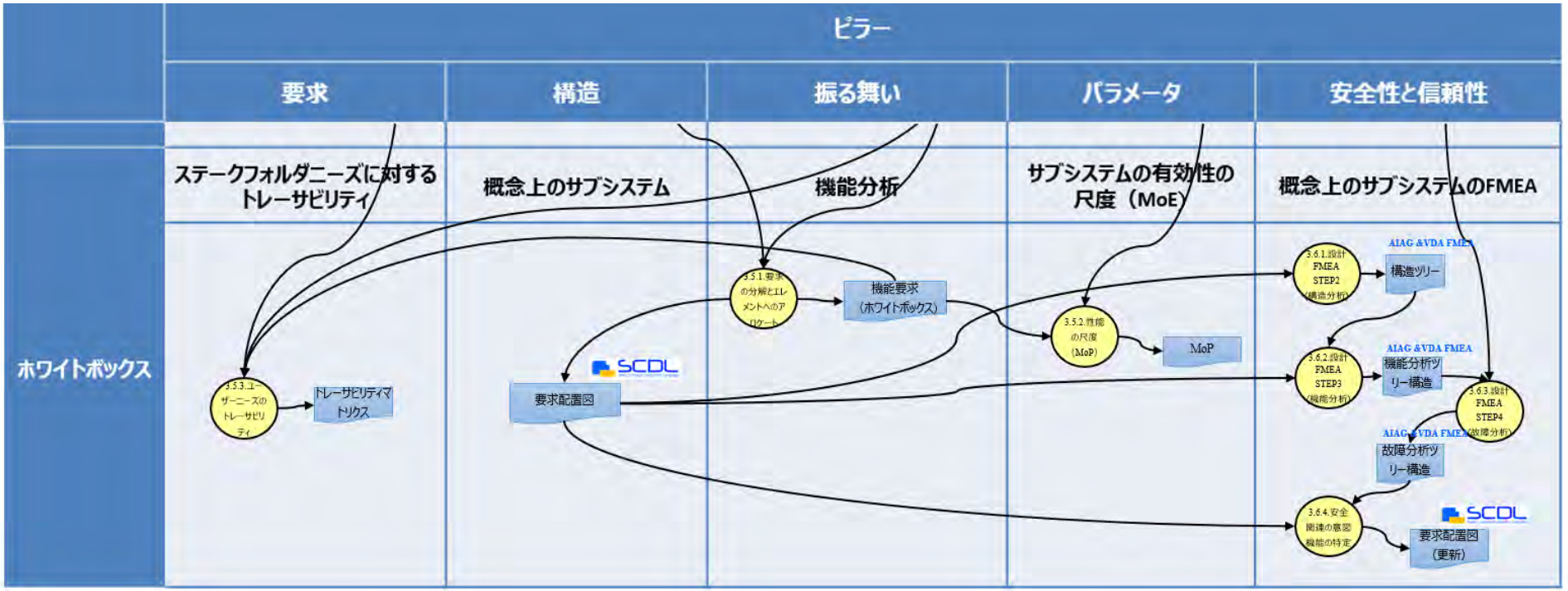
後ほど出てくるDFMEAではHAZOPガイドワードを使用したが、UCA表では4種類のガイドワードを用いている。

慣れていないこともあり、それぞれの分析結果に不整合が発生した。

各ガイドワードの守備範囲を事前にしっかり理解しておくことが重要だと感じた。

ホワイトボックス視点による分析

（MagicGrid上にマッピングしたPFD）



（ホワイトボックスの視点）

3.5 対象システム(SoI：System of Interest)の分析（その２）

3.6 設計FMEAと安全関連の意図機能の特定

3.5.対象システム(SoI：System of Interest)の分析（その２）

ここでは、物理的な構造（エレメント）を意識し、対象システムのSoIを明らかにする活動として、以下のような分析活動に取り組んでみた。

What：

詳細化した対象システム(SoI)のサブシステムの特定と機能要求、非機能要求（性能要求）の導出

How：

こんな流れで 分析してみた！

- サブシステムを特定し、要求の分解とアロケート（3.5.1項）
- 分解された要求のトレーサビリティ確認（3.5.2項）
- 分解されたの機能要求に対する性能の尺度（MOP：Measure of Performance）の導出（3.5.3項）

3.5.1.要求の分解とエレメントへのアロケート

物理的な構造に対する機能要求として22個に分解し、エレメントにアロケートした

利害関係者ニーズとシステム要求の分析結果

表1

利害関係者	（利害関係者の）ニーズ	（システムに対する）要求	
車の利用者	手を使わずにドアを開閉したい	非接触でドア開を行う	機能要求
		非接触でドア閉を行う	機能要求
		開閉動作中にドア動線上の人・物に接触しないようにする	機能要求
		手動での開閉を優先する	機能要求
	利用しないときは機能をOFFにしたい	不要時に作動を禁止する	

利害関係者ニーズ

システム要求

図7
要求図

表4

対象システムに必要な機能要求
(01)作動の許可禁止を判定する
(02)ドア開閉状態を判定する
(03)利用者の意図を検出する
(04)利用者の位置を検出する
(05)自動開閉するドアを判定する
(06)自動でドアを開閉する
(07)周囲の状況を判断する
(08)ドアの開角度調整をする
(09)走行中であることを判断する
(10)ドア開閉可否を判定する
(11)手動操作を判定する
(12)手動操作を優先判定する
(13)ドア開角度を維持する
(14)利用者を特定する

14個の機能要求

22個の機能要求に分解

エレメントにアロケート

3.5.1.要求の分解とエレメントへのアロケート

エレメントに対する機能要求のアロケート結果をSCDLの要求配置図で表現

表12

エレメント	機能要求	内容
Body制御システム	IF-01	作動の許可・禁止切り替え機能	人のSW操作などにより、自動ドアシステムの使用許可/禁止を切り替える機能
	IF-02	作動の許可・禁止判定機能	切り替えSWなどの状態により自動ドアシステムの使用許可/禁止判定する機能
	IF-03	走行検出機能	車両が走行中であることを検出する機能
	IF-04	走行中判定機能	検出された信号から走行中か停止中かを判定する機能

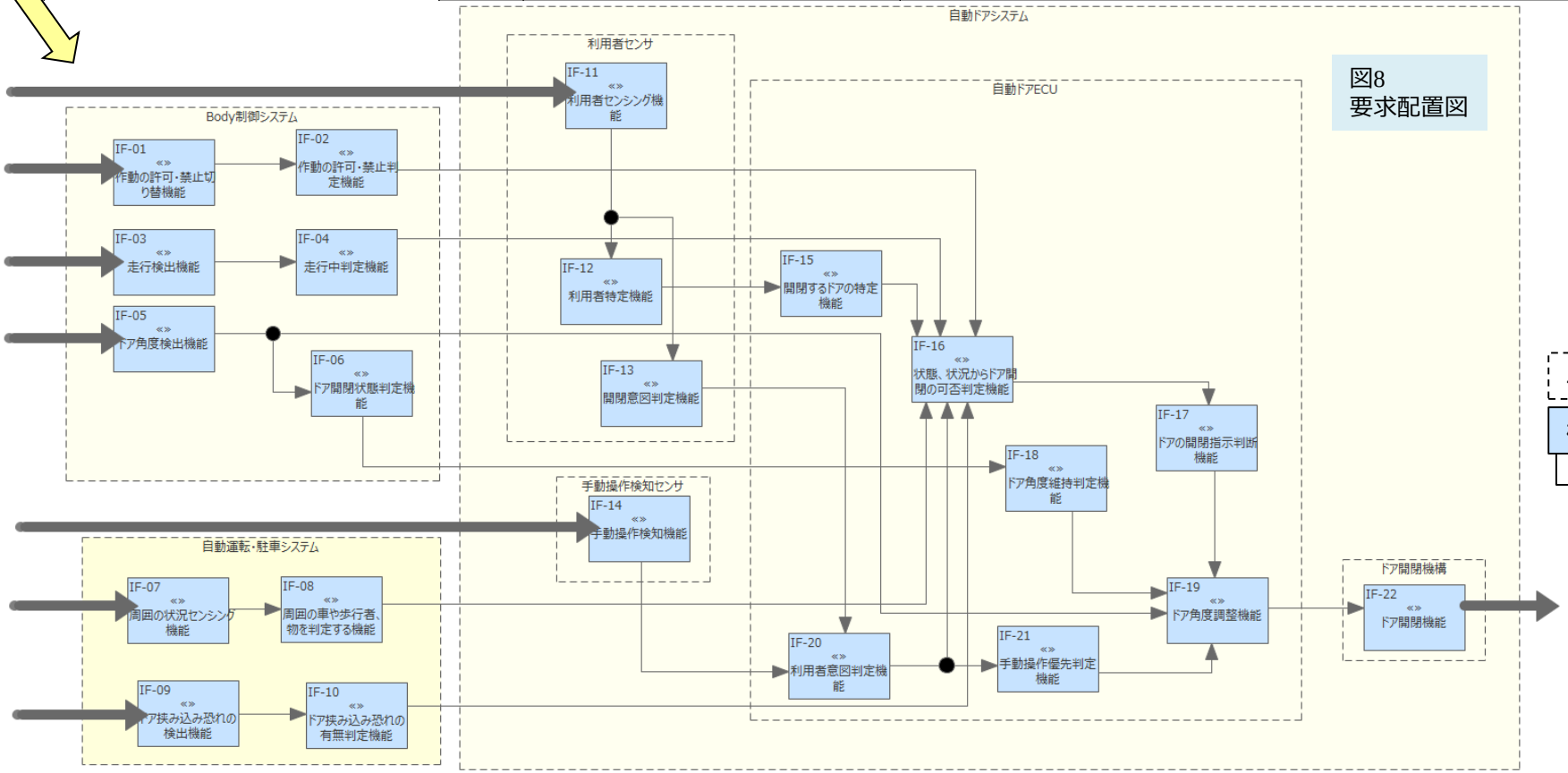
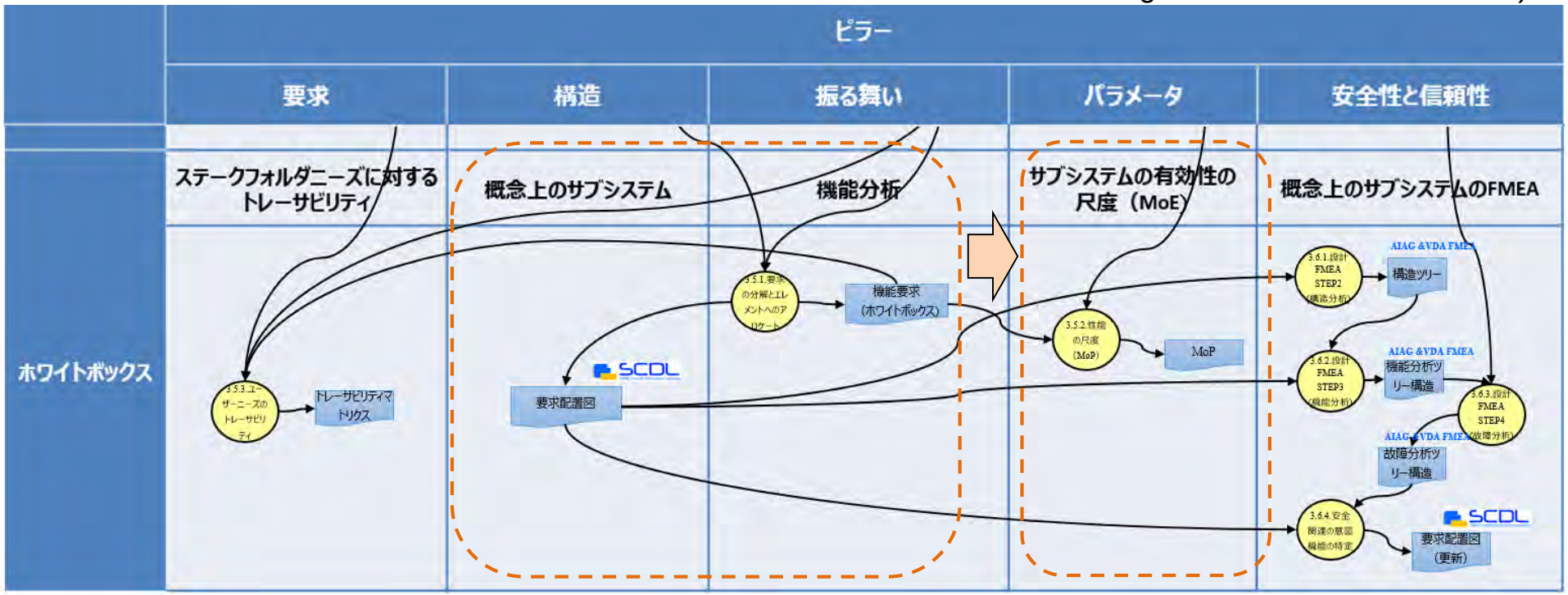


図8
要求配置図

（MagicGrid上にマッピングしたPFD）



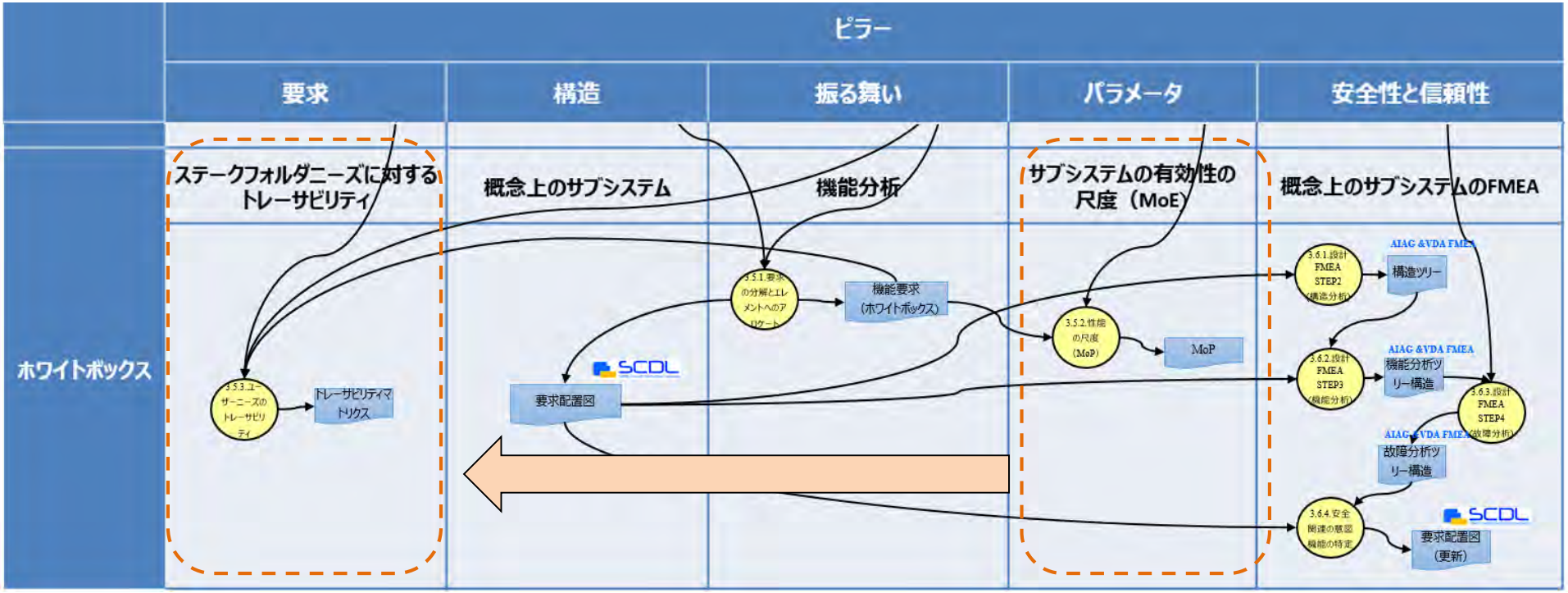
3.5.2.性能の尺度（MoP）

対象システムの機能要求に対し、求められる（定量的な）性能などが実現可能であることをチェックできるようにするために、性能の尺度（MoP）を定義した。
また、定義漏れが無いことを下記のマトリクス表でチェックした。

表13

	機能要求-MoP	MoP（Measure of Performance）																				
		＊＊Nm 以下のトルクに対し保持可能	IGN SW のON/OFF　2 択を判定	ドアのヒンジにかかるドア操作トルクの大きさにより手動操作を判定	ドアの可動範囲内の障害物を検出	ドア可動範囲の10％以上を開と判断	ドア可動範囲の10％未満を閉と判断	ドア開作動速度：30 度/秒	ドア閉作動速度：90 度/秒	パーク機能と車速のANDで停止、それ以外は走行中と判定	開くと危険か判定機能	許可・禁止の2 択を判定	作動ラグ：0．3 秒以下	指定の角度までドアを開く	自動開、自動閉、手動操作の3 種類を判別	車両バリアント情報よりドアの数、位置を識別	手動操作を検出したら出力OFF	周囲の状況判定により安全とANDで停車と判断された時だけ許可	周囲の状況判定により安全と判断された時だけ許可	障害物までの角度を算出	利用者の位置から対象ドア決定	利用者の位置を判断	利用者特定機能
機能要求	(IF-01)作動の許可・禁止切り替機能		1									1											
	(IF-02)作動の許可・禁止判定機能		1									1											
	(IF-03)走行検出機能									1													
	(IF-04)走行中判定機能									1													
	(IF-05)ドア角度検出機能													1									
	(IF-06)ドア開閉状態判定機能					1	1																
	(IF-07)周囲の状況センシング機能																			1			
	(IF-08)周囲の車や歩行者、物を判定する機能										1												
	(IF-09)ドア挟み込み恐れの検出機能				1																		
	(IF-10)ドア挟み込み恐れの有無判定機能				1																		
	(IF-11)利用者センシング機能																					1	
	(IF-12)利用者特定機能																						1
	(IF-13)開閉意図判定機能														1								
	(IF-14)手動操作検知機能			1																			
	(IF-15)開閉するドアの特定機能															1					1		
	(IF-16)状態、状況からドア開閉の可否判定機能										1												
	(IF-17)ドアの開閉指示判断機能																	1	1				
	(IF-18)ドア角度維持判定機能	1																					
	(IF-19)ドア角度調整機能													1									
	(IF-20)利用者意図判定機能														1								
	(IF-21)手動操作優先判定機能																1						
	(IF-22)ドア開閉機能							1	1				1										

（MagicGrid上にマッピングしたPFD)



3.5.3.ユーザーニーズのトレーサビリティ

ここまで分析してきたユーザニーズ、システムに対する要求、物理的な構造に対する機能要求間の対応関係(トレーサビリティ)をトレーサビリティマトリクスで明らかにした。(要求図をマトリクス表にしただけ)

図7

22個の機能要求

14個の機能要求

利害関係者ニーズ

システム要求

車の利用者要求	1.1.a 手を使わずにドアを閉める	1.1.b 手を使わずにドアを開ける	1.1.c 自動開閉時に人、物、自車に危害を加えない	1.1.d 手動での開閉を優先する	1.1.e 不要時に作動を禁止する
→ 手を使わずにドアを開けたい		←	←	←	
→ 手を使わずにドアを閉めたい	↓		←	←	
→ 利用しないときは機能をOFFにしたい					←

利害関係者	(利害関係者の)ニーズ	(システムに対する)要求	
車の利用者	手を使わずにドアを開閉したい	非接触でドア開を行う	機能要求
		非接触でドア閉を行う	機能要求
		開閉動作中にドア動線上の人・物に接触しないようにする	機能要求
		手動での開閉を優先する	機能要求
	利用しないときは機能をOFFにしたい	不要時に作動を禁止する	機能要求

表1

表14
トレーサビリティマトリクス

	(IF-01)作動の許可・禁止切り替機能	(IF-02)作動の許可・禁止判定機能	(IF-03)走行検出機能	(IF-04)走行中判定機能	(IF-05)ドア角度検出機能	(IF-06)ドア開閉状態判定機能	(IF-07)周囲の状況センシング機能	(IF-08)周囲の車や歩行者、物を判定する機能	(IF-09)ドア挟み込み恐れの検出機能	(IF-10)ドア挟み込み恐れの有無判定機能	(IF-11)利用者センシング機能	(IF-12)利用者特定機能	(IF-13)開閉意図判定機能	(IF-14)手動操作検知機能	(IF-15)開閉するドアの特定機能	(IF-16)状態、状況からドア開閉の可否判定機能	(IF-17)ドアの開閉指示判断機能	(IF-18)ドア角度維持判定機能	(IF-19)ドア角度調整機能	(IF-20)利用者意図判定機能	(IF-21)手動操作優先判定機能	(IF-22)ドア開閉機能
(01)作動の許可禁止判定	→	→																				
(02)ドア開閉状態判定					→	→																
(03)利用者の意図検出													→							→		
(04)利用者の位置検出											→											
(05)自動開閉するドアの判定															→							
(06)自動ドア開閉機能																						→
(07)周囲の状況判断							→	→	→	→												
(08)ドア開角度調整機能					→												→		→			
(09)走行中判断			→	→																		
(10)ドア開閉可否判定																→						
(11)手動操作判定														→								
(12)手動操作優先判定																					→	
(13)ドア開角度維持機能					→													→				
(14)利用者を特定する機能												→										

3.5.対象システム(SoI)の分析（その２）の気づき、考察

で、どんな感じだった？

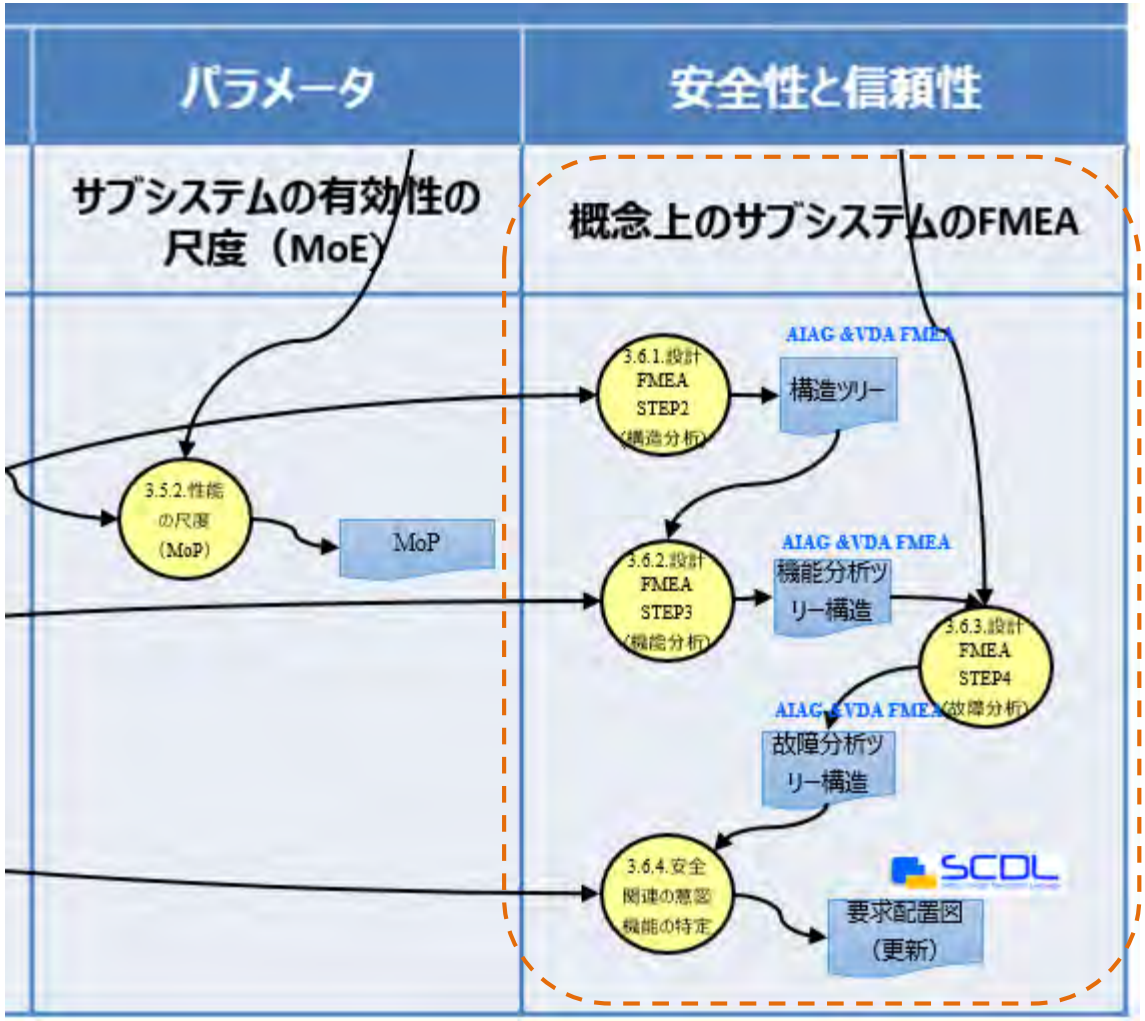
3.5.2.性能の尺度（MoP）に対する気づき、考察

実際の開発では、

評価対象である機能要求は、評価可能なレベルまで詳述化されるべきである。
今回は詳述化を実施しなかったので、MoPに対する評価はできなかった。

（MagicGridで言うところの問題領域のみ実施し、解決領域を実施していないため）

（MagicGrid上にマッピングしたPFD)



3.6. 設計FMEAと安全関連の意図機能の特定

対象システムの安全目標に対し、それを侵害する恐れのある機能要求を特定するために、AIAG&VDA-FMEAを用いて分析した。
（Step2,3,4と故障影響の厳しさ(s)の評価を実施）

AIAG&VDA-FMEA
使ってみた！

次に、FMEAの結果と安全目標(SG)を関連づけ、安全関連の意図機能を特定した。

こんな流れで 分析してみた！

3.6.1.設計FMEA STEP2：構造分析

- ✓ 分析の対象範囲を明確化するため、SCDLの要求配置図を参照し、対象となるシステムの構造を階層的に分解

3.6.2.設計FMEA STEP3：機能分析

- ✓ 各構造に対する機能と、機能間のつながりを明確化

3.6.3.設計FMEA STEP4：故障分析 及び 故障影響の厳しさ評価、故障間のつながりと安全目標(SG)の関連付け

- ✓ 各機能に対する故障モードと、故障原因，故障モード，及び故障影響間のつながりと安全目標(SG)を関連付け、故障影響に対する厳しさ(s)の評価を実施

3.6.4.安全関連の意図機能の特定

- ✓ 対象システムの各安全目標（SG）に対し、それを侵害する恐れのある機能要求を特定

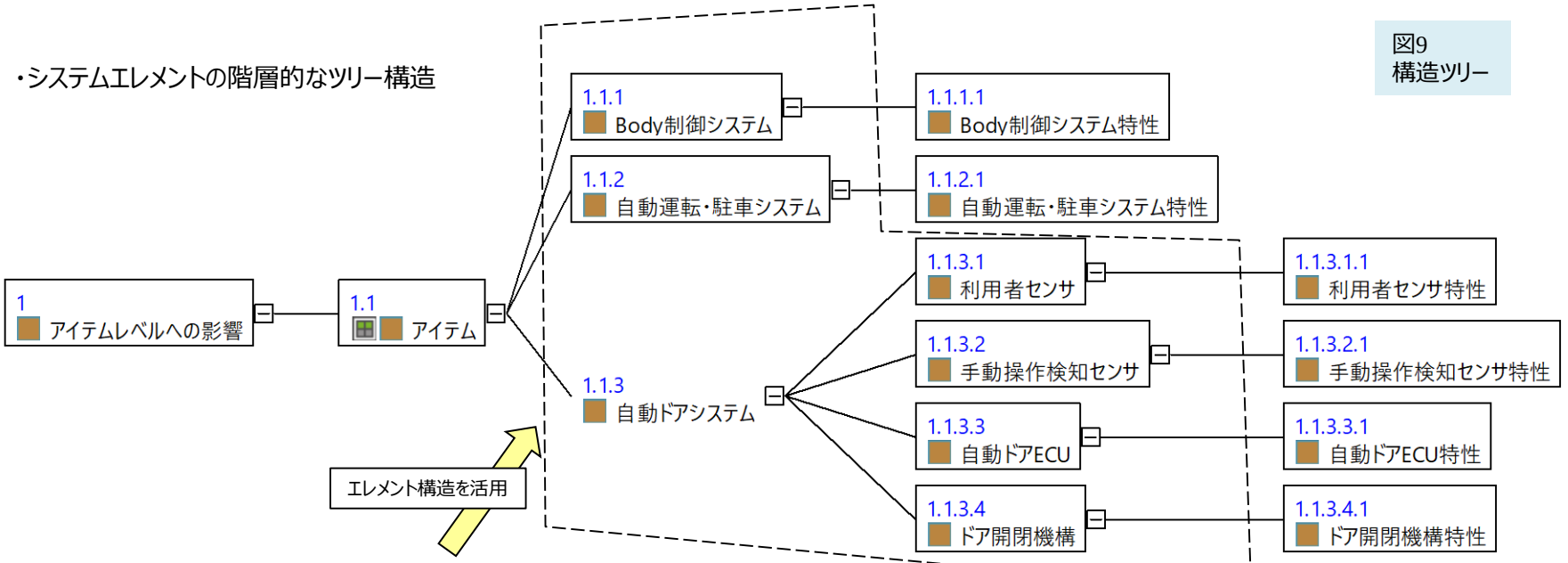
参考
- STEP1 計画策定及び準備
- STEP5 リスク分析（厳しさS,発生頻度O,検出Dの評価)
- STEP6 最適化
- STEP7 結果文書化

3.6.1.設計FMEA　STEP2：構造分析

✓ 分析の対象範囲を明確化するため、SCDLの要求配置図を参照し、対象となるシステムの構造を階層的に分解

・システムエレメントの階層的なツリー構造

図9
構造ツリー



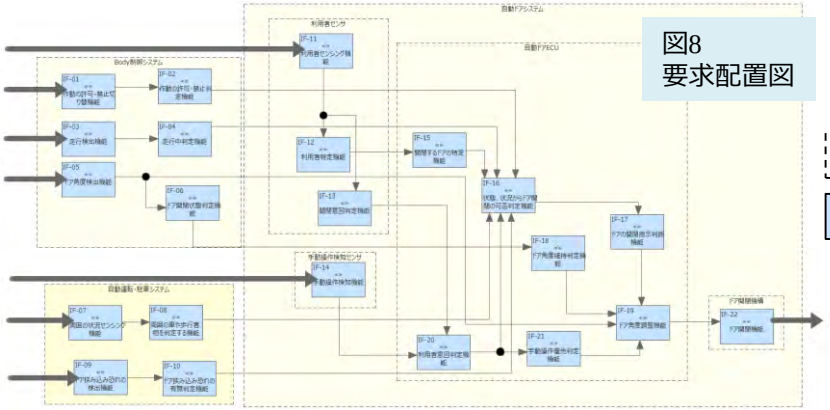


図8
要求配置図

エレメント

機能要求

3.6.2.設計FMEA　STEP3：機能分析

✓ 各構造に対する機能を明確化

・機能分析の構造ツリー

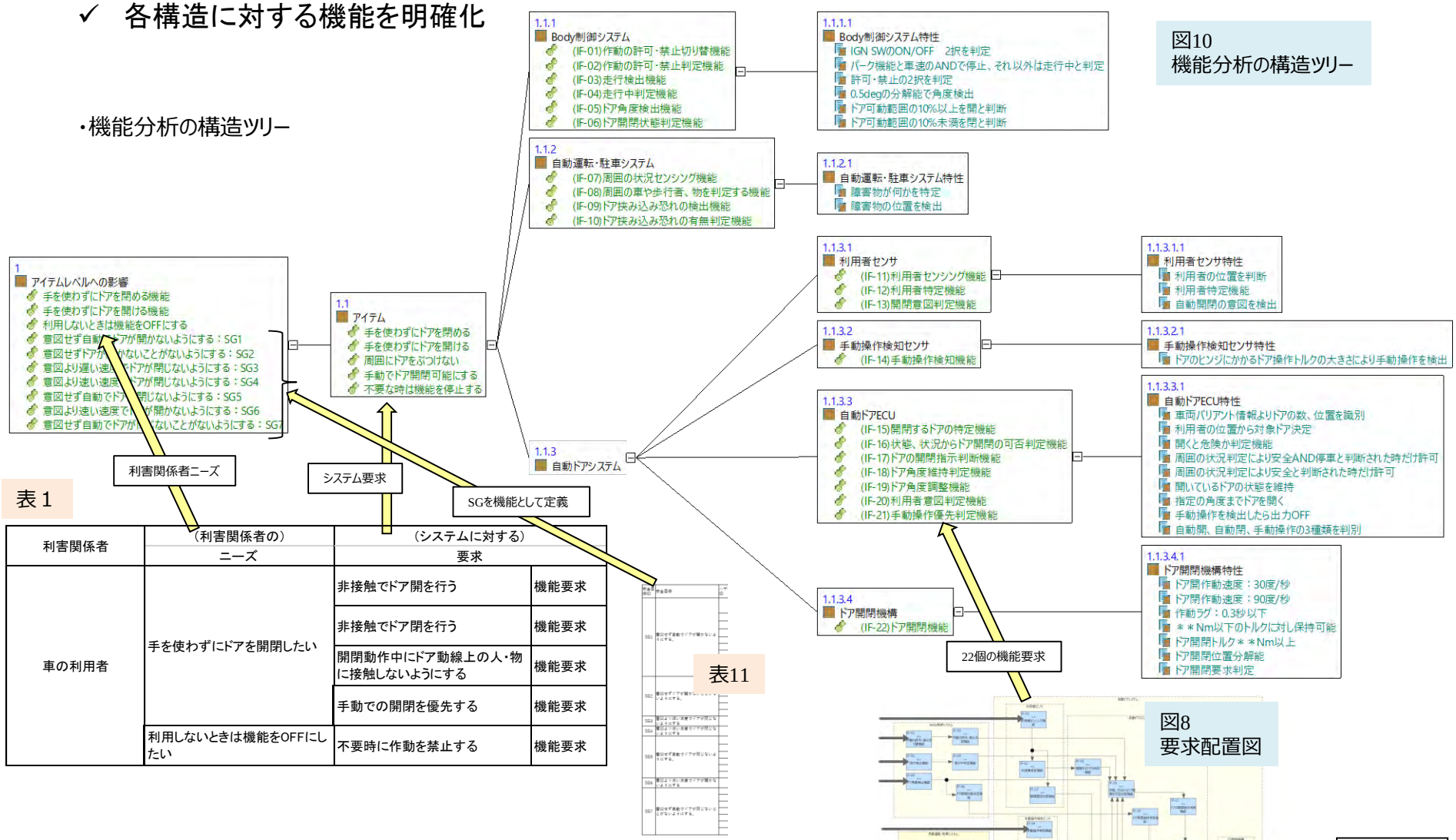


図10
機能分析の構造ツリー

表１

利害関係者	（利害関係者の）ニーズ	（システムに対する）要求	
車の利用者	手を使わずにドアを開閉したい	非接触でドア開を行う	機能要求
		非接触でドア閉を行う	機能要求
		開閉動作中にドア動線上の人・物に接触しないようにする	機能要求
		手動での開閉を優先する	機能要求
	利用しないときは機能をOFFにしたい	不要時に作動を禁止する	機能要求

表11

図8
要求配置図

3.6.2.設計FMEA　STEP3：機能分析

✓ 各階層間の機能のつながりを明確化

各階層の機能を下位の階層の機能でどのように実現するかを関連付け

・「手を使わずにドアを開ける機能」 に関する機能分析ツリー構造の例

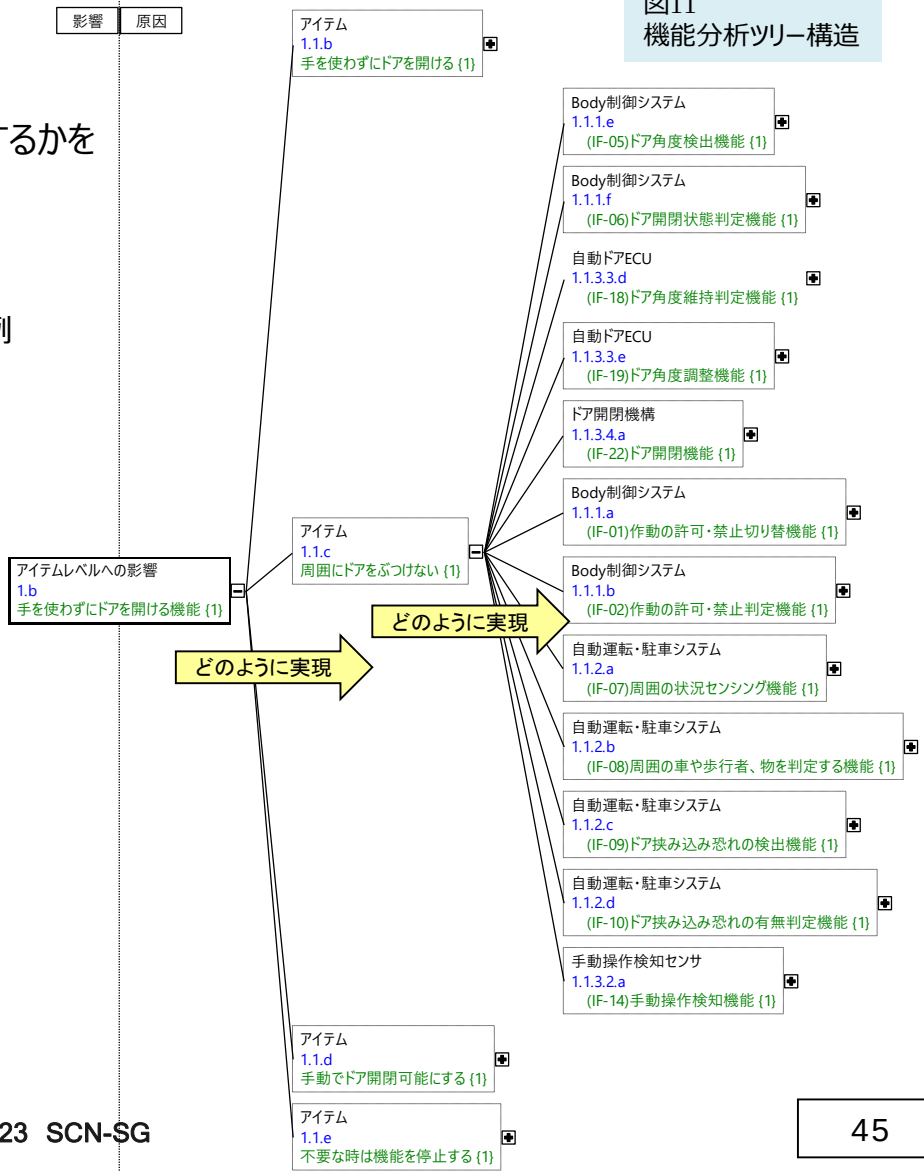


図11
機能分析ツリー構造

3.6.3.設計FMEA　STEP4：故障分析

及び故障影響の厳しさ評価、故障間のつながりと安全目標(SG)の関連付け

STEP４故障分析

✓　各機能に対する故障モードを明確化

・故障分析の構造ツリー
　機能（緑字）に対する故障モード（赤字）を示す

ハザードの原因（HAZOPガイドワードを用いて分析）

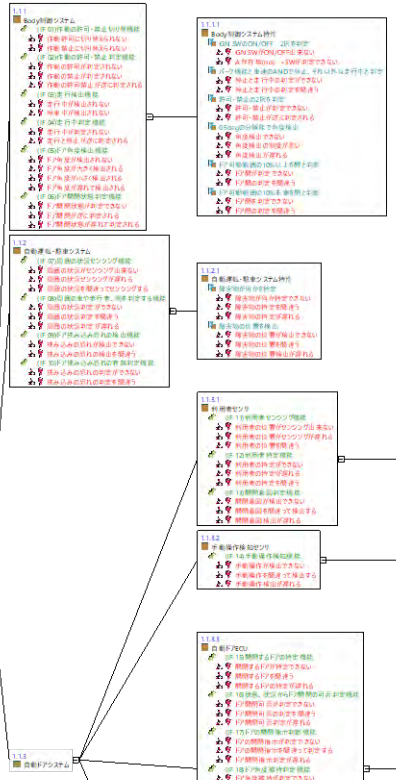


図12
故障分析の構造ツリー

表10

ハザードID	ハザード	アクシデントID	アクシデント	ハザードダスイベントID	ハザードダスイベント	遭遇頻度E
H2	システムの作動許可条件外で作動する	A1	急にドアが開き人が転げ落ちる	HE1	乗員乗車中かつ自車走行中に意図せずドアが開く。	E3:乗車中 E4：自車走行中 ⇒全体のE：E3
				HE2	乗員乗車中かつ自車停止中に意図せずドアが開く。	E3：乗車中 E4：自車停止中 ⇒全体のE：E3

SCDL Safety Concept Description Language

3.6.3.設計FMEA　STEP4：故障分析

及び故障影響の厳しさ評価、故障間のつながりと安全目標(SG)の関連付け

- ✓ 故障原因，故障モード，及び故障影響間のつながりを明確化
- ✓ 安全目標(SG)の関連付け
- ✓ 故障影響に対する厳しさ(s)の評価

・ドアが閉じる速度が遅いに関する故障分析ツリー構造（SG3の例）

図13
故障分析ツリー構造

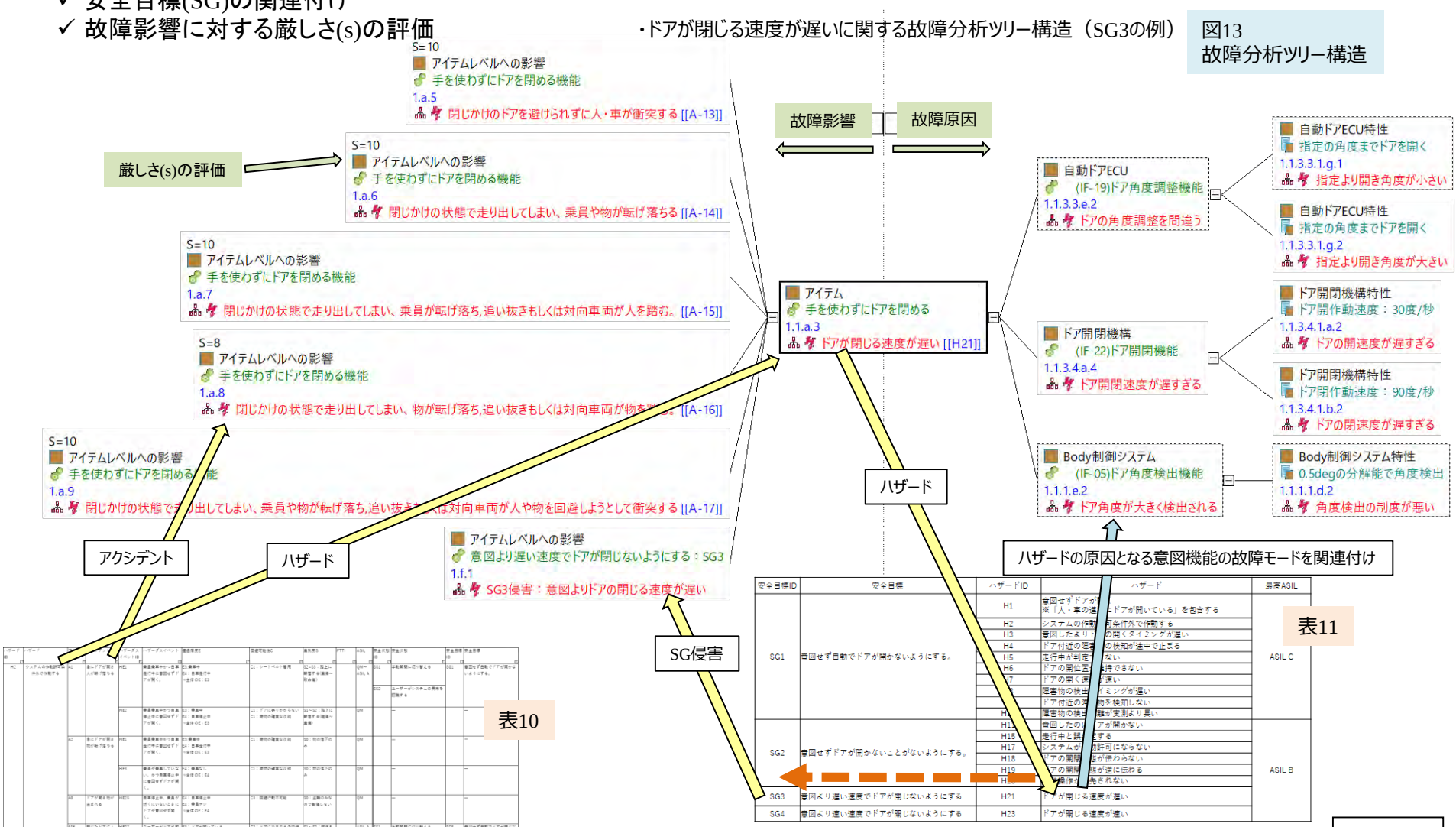


表10

安全目標ID	安全目標	ハザードID	ハザード	最高ASIL
SG1	意図せず自動でドアが開かないようにする。	H1	意図せずドアが開く※「人・車の通過にドアが開いている」を包含する	ASIL C
		H2	システムの作動条件外で作動する	
		H3	意図したよりドアの開くタイミングが遅い	
		H4	ドア付近の障害物の検知が途中で止まる	
		H5	走行中が判定できない	
		H6	ドアの開位置を維持できない	
		H7	ドアの開く速度が遅い	
			障害物の検出タイミングが遅い	
			ドア付近の障害物を検知しない	
		H1	障害物の検知距離が実測より長い	
SG2	意図せずドアが開かないことがないようにする。	H13	意図したのにドアが開かない	ASIL B
		H15	走行中と誤判定する	
		H17	システムが作動許可にならない	
		H18	ドアの開閉指令が伝わらない	
		H19	ドアの開閉指令が逆に伝わる	
		H20	操作途中で止まる	
SG3	意図より遅い速度でドアが閉じないようにする	H21	ドアが閉じる速度が遅い	
SG4	意図より遅い速度でドアが閉じないようにする	H23	ドアが閉じる速度が遅い	

表11

3.6.4.安全関連の意図機能の特定

- ✓ 対象システムの各安全目標（SG）に対し、SG侵害する恐れのある故障モードを洗い出し、安全関連の意図機能を特定

SG3侵害の原因につながる意図機能の故障モード

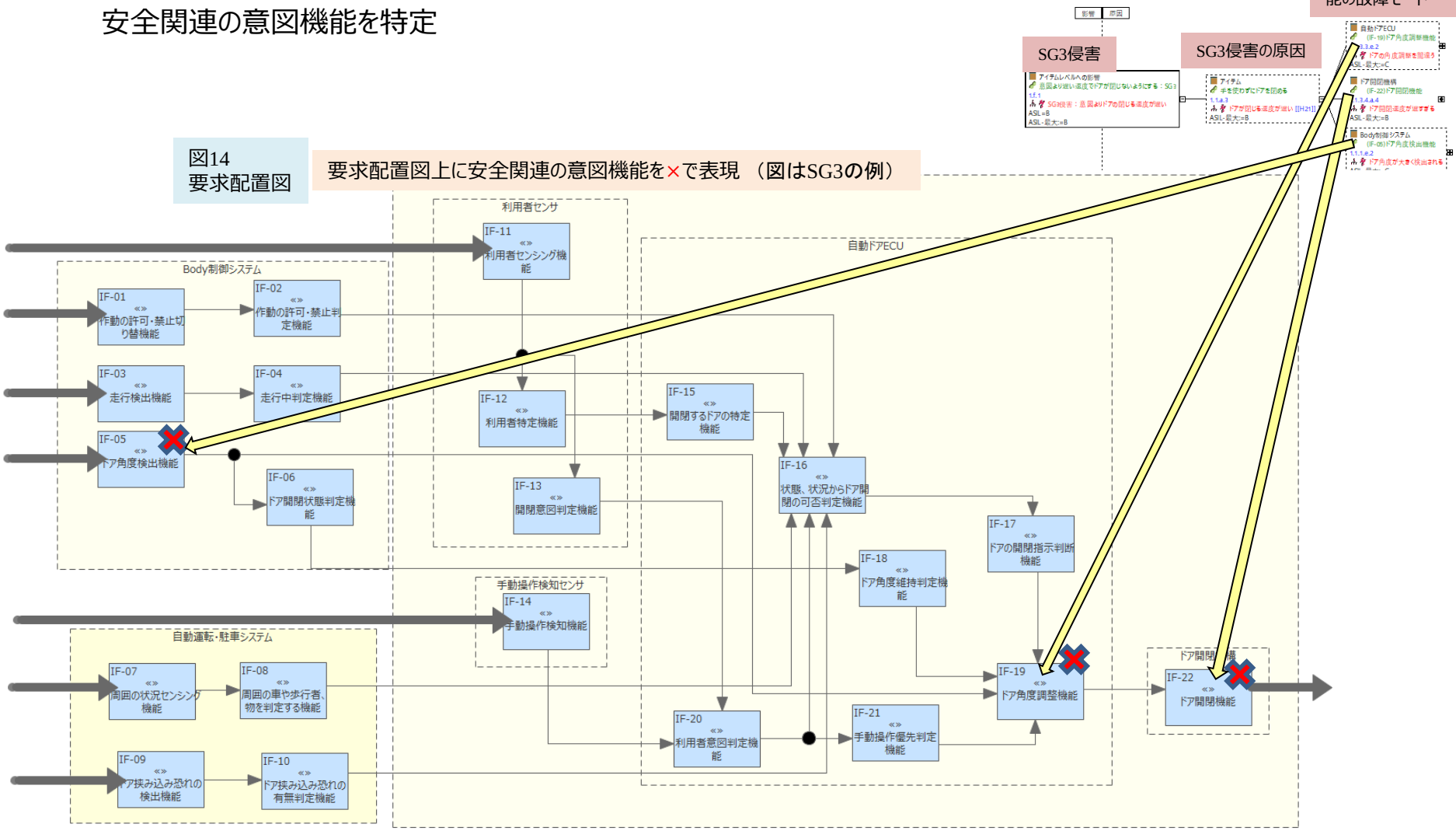


図14
要求配置図

要求配置図上に安全関連の意図機能を×で表現 （図はSG3の例）

3.6. 設計FMEAと安全関連の意図機能の特定の気づき、考察

で、どんな感じだった？

- ✓ 3.3.対象システムの分析（その１）でPAAを考慮した分析を実施しなかったので、その1の結果を設計FMEAで活用できなかった。FMEAで活用するには階層的な活動が必要。
- ✓ 各階層についてSCDLの要求配置図があれば、STEP2,3にその情報がそのまま利用可能。
- ✓ 各SG侵害を車両レベルの故障影響として定義し、表11を 参照してハザードとSGを関連付けたところがポイント。そうすることにより、SG侵害に至る原因系が抽出できるようになった。

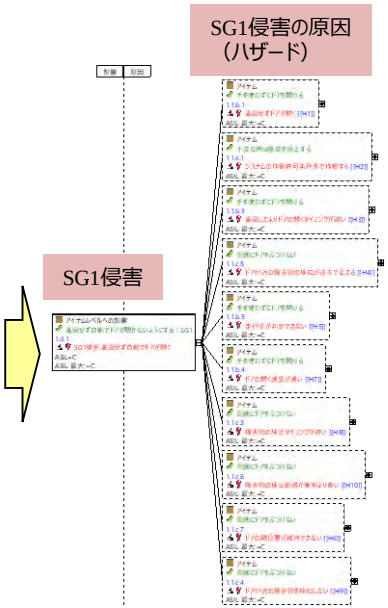


表11

安全目標ID	安全目標	ハザードID	ハザード	最高ASIL
SG1	意図せず自動でドアが開かないようにする。	H1	意図せずドアが開く ※「人・車の通路にドアが開いている」を包含する	ASIL C
		H2	システムの作動許可条件外で作動する	
		H3	意図したよりドアの開くタイミングが遅い	
		H4	ドア付近の障害物の検知が途中で止まる	
		H5	走行中が判定できない	
		H6	ドアの開位置が維持できない	
		H7	ドアの開く速度が遅い	
		H8	障害物の検出タイミングが遅い	
		H9	ドア付近の障害物を検知しない	
		H10	障害物の検出距離が実測より長い	
SG2	意図せずドアが開かないことがないようにする。	H11	意図したのにドアが開かない	ASIL B
		H15	走行中と誤判定する	
		H17	システムが作動許可にならない	
		H18	ドアの開閉状態が伝わらない	
		H19	ドアの開閉状態が逆に伝わる	
		H20	手動操作が優先されない	
SG3	意図より遅い速度でドアが閉じないようにする	H21	ドアが閉じる速度が遅い	
SG4	意図より速い速度でドアが閉じないようにする	H23	ドアが閉じる速度が速い	

4.まとめ

- システム開発のスタート　～　安全設計に繋がる部分　の一連の流れを仮想システム：「車両の自動開閉ドアシステム」 を用いてスタディしました。

- 今回のスタディで使用した主な手法は以下
  - 分析手法
    - ✓ ロジックツリー分析
    - ✓ ユースケース分析
    - ✓ STAMP/STPA
    - ✓ AIAG&VDA FMEA
  - ダイアグラム
    - ✓ コンテキスト図
    - ✓ ユースケース図
    - ✓ コントロールストラクチャー図
    - ✓ 要求図
    - ✓ 要求配置図（SCDL）

- SCDLは安全アーキテクチャでの活用だけでなく、意図機能のアーキテクチャやDFMEAにおいても、直感的にわかりやすいことで有用であることが分かりました。

- SCDLと各種ダイアグラムや分析手法を組み合わせ、その連携を考慮しながら取り組むことが必要であることが分かりました。

ご清聴ありがとうございました。

Appendix

参考文献、WEBサイト

- magicgrid-book-of-knowledge-ebook-ja.pdf / ダッソーシステムズ（株）
- AIAG&VDA FMEAハンドブック スタディガイド / （株）ジャパン・プレクサス
- はじめてのSTAMP/STPA ～システム思考に基づく新しい完全性解析手法～ / (独)情報処理推進機構
- STAMP Workbench リファレンスマニュアル / (独)情報処理推進機構
- https://navi.dropbox.jp/fishbone-diagram
- https://xtech.nikkei.com/it/article/Watcher/20071009/283860/
- https://www.asam.net/standards/detail/scdl/#backToFilters
- https://ssl.scn-sg.com/main/ja/scdl-specification

SCDL Safety Concept Description Language

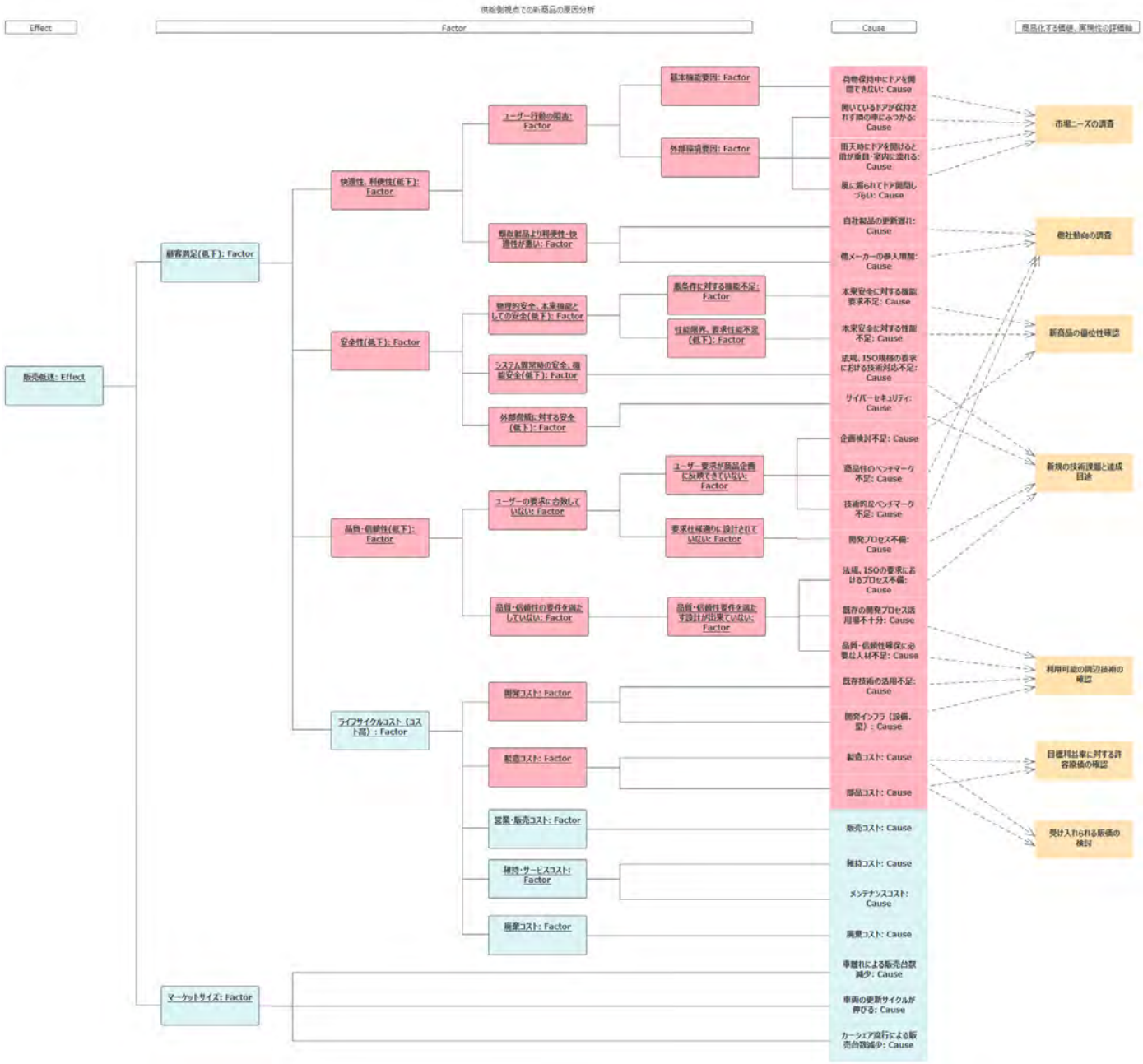


図2
ロジックツリー

3.3.3.ユースケース分析

表2
ユースケースシナリオ

ユースケース名		自動でドアを開ける
概要		手がふさがっているときに自動でドアを開き、車両への乗り降りをサポートする。 また、ドアが開いている状態を維持し、ドアが動くことで周囲の物にぶつかるのを防止する。
アクター		車の利用者
開始条件		システム利用許可状態で、利用者が近くにいる場合に開始
事前条件		・自動開閉ドアシステムに電源が供給されている ・利用者が特定できる。 ・車の利用者がシステムの作動を許可している ・車のドアが全て閉じている
イベントフロー	メインフロー	1　アクターがシステムに自動でドアを開く要求をする 2　システムは利用者のドアを開閉意思を検出する 3　システムは、ドアを開いても危険がないことを判定し、最も利用者に近いドアを開く。（代替a,b）（例外ｃ） 4　開いたドアの位置を維持する
	代替フローa	利用者が手動でドアを開く場合 3.1a　アクターがドアを手動で開こうとした場合は、手動のドア開閉を優先する 3.2b　4に戻る
	代替フローb	開くドアの作動範囲に障害物がある場合 3.1b　システムがドアの作動範囲に障害物があると検知する 3.2b　システムは障害物とぶつからない位置までドアを開く 3.3b　4に戻る
	例外フローc	システムの利用可能条件を満たさない場合 3.1c　システムは利用可能条件を満たしていない場合(※1)は、自動ドアシステムが作動しないことをアクターに通知する 3.2c　システムはユースケースを中断する 事後条件 ・システムは待機状態戻っていること ・アクターにシステムの動作条件を満たしていないことが通知されていること
事後条件		ドアが開いた状態で維持されていること
終了条件		システム利用禁止状態　または、利用者が近くにいない場合に終了
備考		※1　利用可能条件 ・停車状態 ・システム正常状態

3.3.3.ユースケース分析

表3
ユースケースシナリオ

ユースケース名		自動でドアを閉じる
概要		手がふさがっているときに自動でドアを閉じ、車両への乗り降りをサポートする。
アクター 開始条件		車の利用者 システム利用許可状態で、利用者が近くにいる場合に開始
事前条件		・自動開閉ドアシステムに電源が供給されている ・利用者が特定できる。 ・車の利用者がシステムの作動を許可している ・車のいずれかのドアが開いている
イベントフロー	メインフロー	1　アクターがシステムに自動でドアを閉じる要求をする 2　システムは利用者のドアを開閉意思を検出する 3　システムは、ドアを閉じても危険がないことを判定し、最も利用者に近いドアを閉じる。（代替a）（例外b）
	代替フローa	利用者が手動でドアを閉じる場合 3.1a　アクターがドアを手動で閉じようとした場合は、手動のドア開閉を優先する 3.2a　ユースケースを終了する
	例外フローb	システムの利用可能条件を満たさない場合 3.1b　システムは利用可能条件を満たしていない場合(※1)は、自動ドアシステムが作動しないことをアクターに通知する 3.2b　システムはユースケースを中断する 事後条件 ・システムは待機状態戻っていること ・アクターにシステムの動作条件を満たしていないことが通知されていること
事後条件		ドアが閉じていること
終了条件		システム利用禁止状態　または、利用者が近くにいない場合に終了
備考		※1　利用可能条件 ・システム正常状態

3.4.1.ハザード分析

表8
コンポーネント抽出表

対象	登場人物	責務	コントロールアクション	フィードバック	入出力	備考
true	利用者		開閉意図伝達 (To: 自動開閉ドアシステム) 手動操作を示す (To: 自動開閉ドアシステム) 作動許可を示す (To: 自動開閉ドアシステム)			
true	周囲の人		人の存在、動きを示す (To: 自動開閉ドアシステム)			
true	周囲を走行する車 （自転車などを含む）		車の存在、動きを示す (To: 自動開閉ドアシステム)			
true	車両システム		走行中を示す (To: 自動開閉ドアシステム)			
true	自動開閉ドアシステム		ドアの開閉状態を示す (To: 自動開閉ドアシステム)	ドア開閉の状態 (To: 利用者) ドア開閉の状態 (To: 周囲の人) ドア開閉の状態 (To: 周囲を走行する車 （自転車などを含む）) ドア開閉の状態 (To: 同乗者、荷物)		
true	同乗者、荷物					
true	周囲の物 （壁、駐車車両など）		物の存在を示す (To: 自動開閉ドアシステム)			

3.5.1.要求の分解とエレメントへのアロケート

表12

エレメント			機能要求	内容
Body制御システム		IF-01	作動の許可・禁止切り替え機能	人のSW操作などにより、自動ドアシステムの使用許可/禁止を切り替える機能
		IF-02	作動の許可・禁止判定機能	切り替えSWなどの状態により自動ドアシステムの使用許可/禁止判定する機能
		IF-03	走行検出機能	車両が走行中であることを検出する機能
		IF-04	走行中判定機能	検出された信号から走行中か停止中かを判定する機能
		IF-05	ドア角度検出機能	ドアの開角度を検出する機能
		IF-06	ドア開閉状態判定機能	ドアの開角度からドアの状態が開か閉かを判断する機能
自動運転・駐車システム		IF-07	周囲の状況センシング機能	車両の周囲の状況（車、歩行者、物の有無など）を検出する機能
		IF-08	周囲の車や歩行者、物を判定する機能	車両の周囲の状況を検出するセンサの情報から周囲の車や、歩行者、物の存在を判定する機能
		IF-09	ドア挟み込みの恐れ検出機能	開いたドアと、車両との間に何かあるかを検出する機能
		IF-10	ドア挟み込みの恐れ有無判定機能	センサの情報から、ドアを閉めると挟み込む恐れがあるかを判定する機能
自動ドアシステム	利用者センサ	IF-11	利用者センシング機能	人の位置と動作を検出する機能
		IF-12	利用者特定機能	どの人が自動ドアシステムを利用しようとしているかを特定する機能
		IF-13	開閉意図判定機能	人の動作から利用者の意図が開なのか閉なのかを判定する機能
	手動操作検知センサ	IF-14	手動操作検知機能	手動でのドア開閉を検知する機能
	自動ドアECU	IF-15	開閉するドアの特定機能	特定された自動ドアシステムを利用しようとしている人に最も近いドアを判定する機能
		IF-16	状態、状況からドア開閉の可否判定機能	ドアの自動開閉の可否を判定する機能
		IF-17	**ドアの開閉指示判断機能**	**ドアの開閉、停止を判断する機能**
		IF-18	ドア角度維持判定機能	維持すべきドア角度を判定する機能
		IF-19	**ドア角度調整機能**	**ドア開閉指示、ドア開度維持の指示、フリー指示、ドア角度情報からドアの角度を調整する機能**
		IF-20	利用者意図判定機能	利用者の意図が、手動開閉なのか、自動開閉なのかを判定する機能
		IF-21	手動操作優先判定機能	手動での開閉判定情報により自動開閉より手動操作を優先することを判定する機能
	ドア開閉機構	IF-22	ドア開閉機能	指示によりドアを開閉動作、保持、フリーにする機能