SCDLと他の手法との連携について

2023/12/20

SCDL活用のための手法連携SWG

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

昨今、自動車分野を中心に電気／電子システムのアーキテクチャ開発において、様々な記法や分析手法が活用されてきている。例えば、記法としては、SysMLなどがあり、分析手法としてはFMEA、FTAやSTAMP/STPAなどが知られている。

自動車の安全に関するアーキテクチャ開発では、安全コンセプト記述言語（Safety Concept Description Language: SCDL）が活用されてきている。SCDLは安全分野での活用だけではなく、アーキテクチャ開発全般に適用して活用することが期待されている。アーキテクチャ開発にてSCDLを活用するためには、他の記法や分析手法との連携や使い分けなど、いくつかの検討しなければならない課題がある。

そこで、自動車分野でのアーキテクチャ開発における一連の開発フローの一部分について仮想の事例を用いてケーススタディすることで、SCDLと他の記法や分析手法との協調や共存について考察を行った。

2.ケーススタディの前提条件

本書で取り扱うケーススタディについて、前提条件を本章で定義する。

- 本書では、システム開発の上流工程から安全設計に繋がる部分について、一連の流れをケーススタディした。
- 仮想のシステムを事例にケーススタディする事にした。

注：

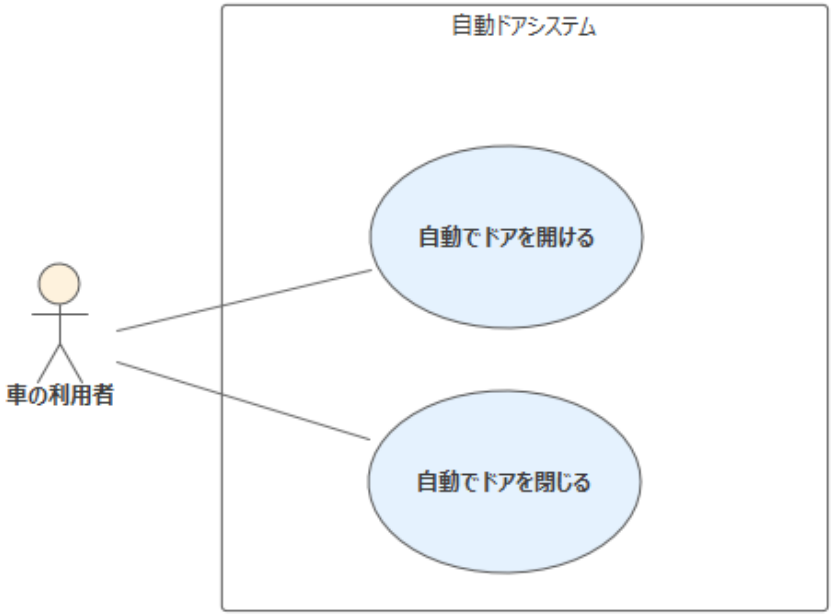
本事例は、SCDLと他の手法との連携などについて考察したものであり、分析順序、連携させた情報なども「あくまで参考」であり、連携手順や方法論などを示すためのものでは無い事に注意

2.1ケーススタディで扱った仮想システム

今回のケーススタディでは、仮想システムとして「車両の自動開閉ドアシステム」に取り組んだ事例を紹介する。

仮想のシステム「車両の自動開閉ドアシステム」は、乗り降りする際に手を使わずにドアを開閉できるシステムである。ドアの種類は「ヒンジドア*」を想定している

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

本書ではシステム開発全般において、SCDLと他の記法や分析手法との連携について考察する事を目的としている。
今回は、システム開発の上流工程から安全設計に繋がる部分について、仮想システムを事例に用い、以下の一連の流れを通してケーススタディした。

仮想システムを用いたケーススタディにおける一連の流れ

- 「車両の自動開閉ドアシステム」の開発に取り組むことになったきっかけ
- マーケット、実現性に関する分析
- システムに求められる機能要求、非機能要求の導出
- システムに対するハザード分析＆リスクアセスメント
- 安全目標侵害につながる意図機能とその故障原因の特定

次ページにて、ケーススタディで扱った「開発プロセス」と「成果物」の関係性を記す。

※全体構成が分かりやすい様に、MBSEの活動で広く知られているMagic Gridを参考にマッピングを行った。
尚、本事例はMagic Grid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。

「3章ケーススタディ」では、各工程について動機・目的・適用手法を整理した後に、スタディの実施内容の紹介をし、そこでの失敗や、気づきについては主に「4章」で紹介する。

2.2ケーススタディで扱ったプロセス

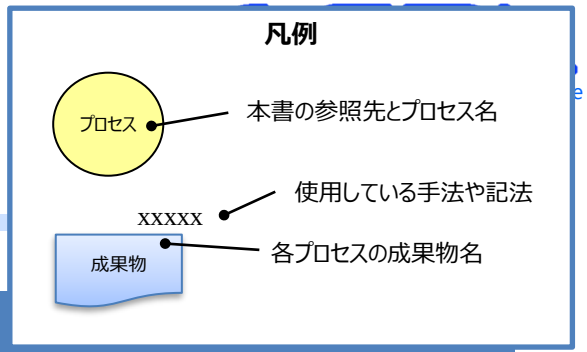
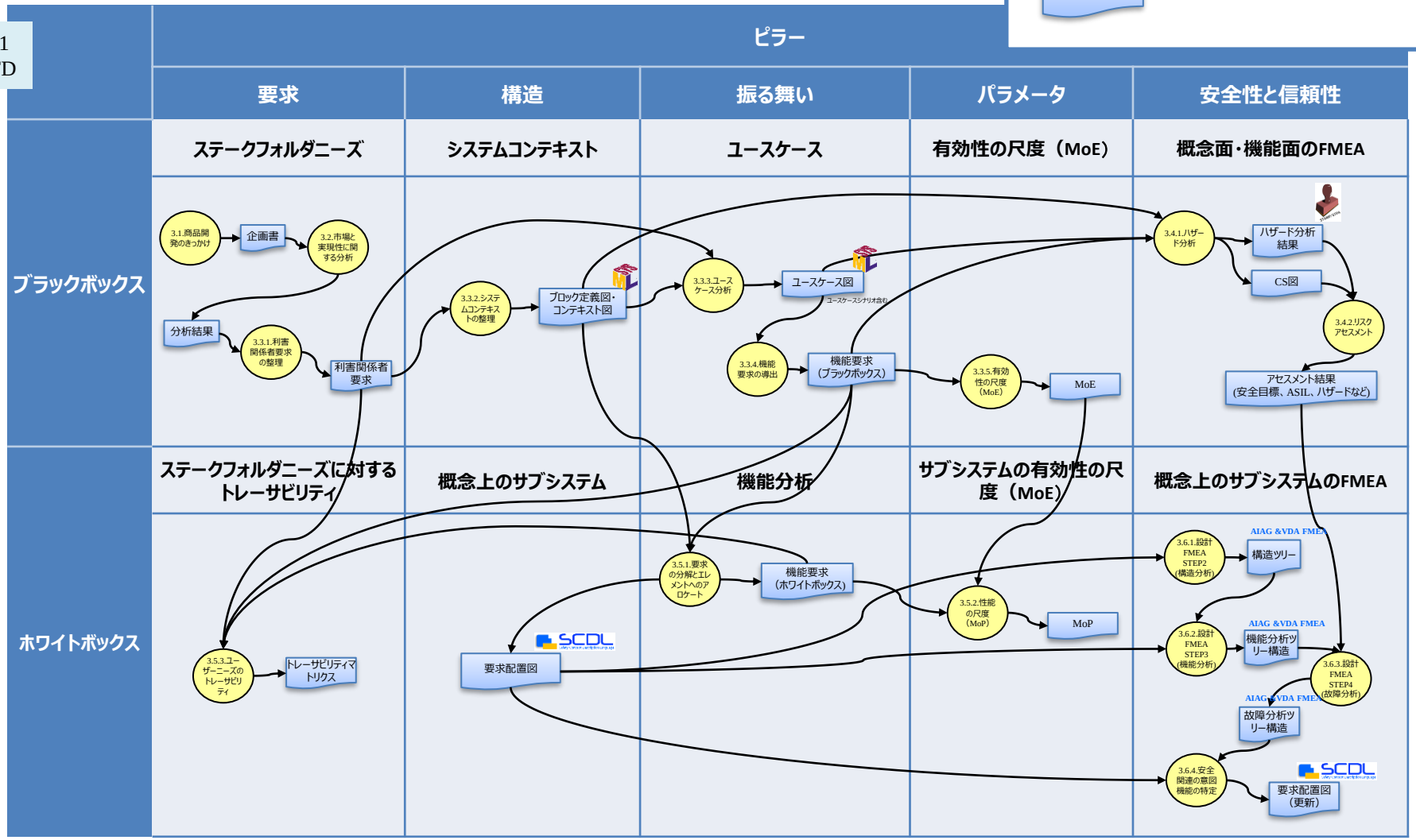


図1
PFD



（MagicGrid上にマッピングしたPFD）

3 .ケーススタディ

本章では、前提条件で定義した内容をもとに手法連携のケーススタディを実施した結果を記述する。

各節の概要

（ブラックボックスの視点）

3.1　商品開発のきっかけ

本書のスタディ対象システムに対し、仮想的な開発のきっかけを記す。

3.2　市場と実現性に関する分析

プロジェクト初期段階における、市場性や実現性を見極めるための分析をロジックツリーなどを用いてスタディした。

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

一般的にプロジェクト初期分析の次のステップとしてブラックボックス視点のSoIを明らかにする活動があるとされており、今回はSysMLの記法などを用いその活動をスタディ実施した。

3 .ケーススタディ

各節の概要（つづき）

3.4 ハザード分析＆リスクアセスメント

本書のスタディ対象システムが、そのシステムライフサイクルにおいて安全性を担保できるようにするため、STAMP/STPAを用いたハザード分析を実施後、リスクアセスメントした。

（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）

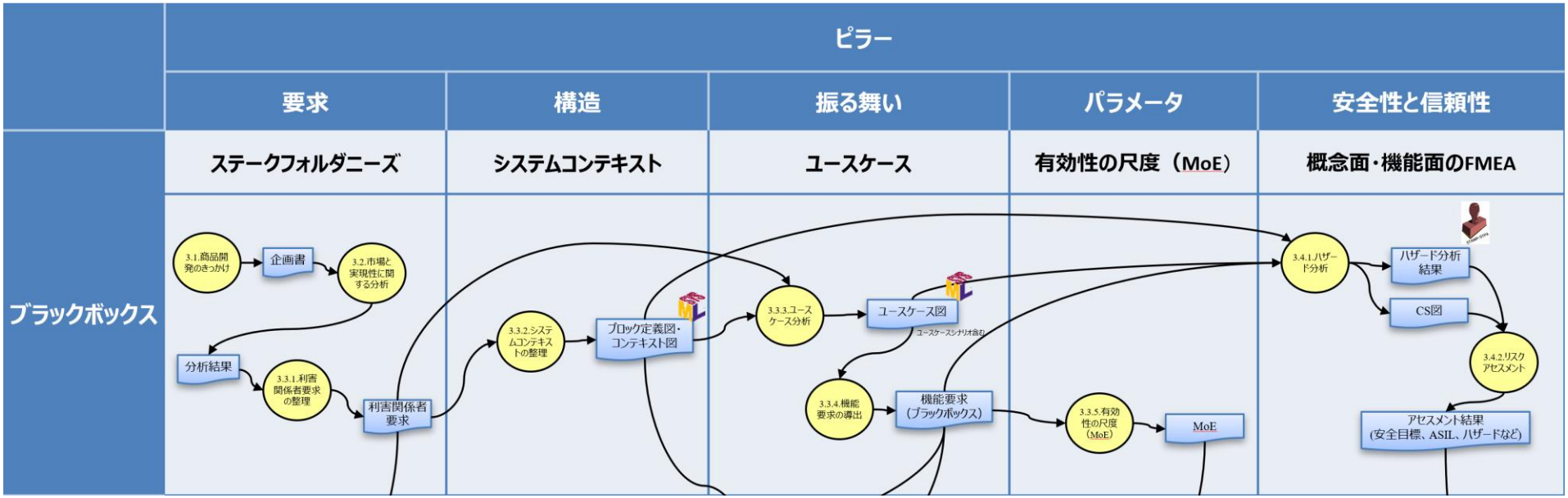
一般的にプロジェクト初期分析の次のステップとしてホワイトボックス視点のSoIを明らかにする。活動があるとされており、今回はSCDL,SysMLなどの記法を用いその活動をスタディした。

3.6 設計FMEAと安全関連の意図機能の特定

スタディ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の分析手法を用いたスタディを実施し、安全関連の意図機能の特定まで行った。

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

自動車メーカーのR&D部門に勤めるAさんは、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自分の車に向かった。

駐車場は屋外にあり、あいにくその日は暴風雨が吹き荒れていた。

悪天候のためマンションの住民も出かける人は少なく、自車の両側の駐車スペースには車が停まったままであった。

傘を持っていたので苦労しながら荷物を持つ手でドアを開け、傘を持つ手でドアを支えながら荷物を車の中に入れたところまではよかったが、傘をたたむためにドアから手を離した瞬間に突風が吹き、ドアが勢いよく開き、隣の車にドアをぶつけてしまった。

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があったらなぁ　と商品開発のアイデアが浮かんだ。

⇒ 商品化できないかな？

Aさんは、商品化の価値や実現性を評価するために、商品企画部門の友人に相談して市場と実現性について分析をすることにした。

3.2.市場と実現性に関する分析

プロジェクト初期段階における市場性や実現性を見極める手法として、ロジックツリー分析、特性要因図などを適用してみた。
以下プロジェクト初期段階の分析についての動機・目的・適用手法を以下に整理する。

Why:

思いついた新商品の企画に対し、商品化する価値、実現性がありそうか、判断したい。

What:

- 企画段階において、商品性の評価軸を『ユーザー側の視点』から『供給側の視点』に移す（＝座標軸を変える）ことによって、開発・製造の工程に落とし込めるようにする
- 商品化を阻害する要因、原因を分析する

How:

以下の視点で、販売低迷に対する要因、原因をロジックツリー分析、特性要因図（フィッシュボーン）などを用いて分析する

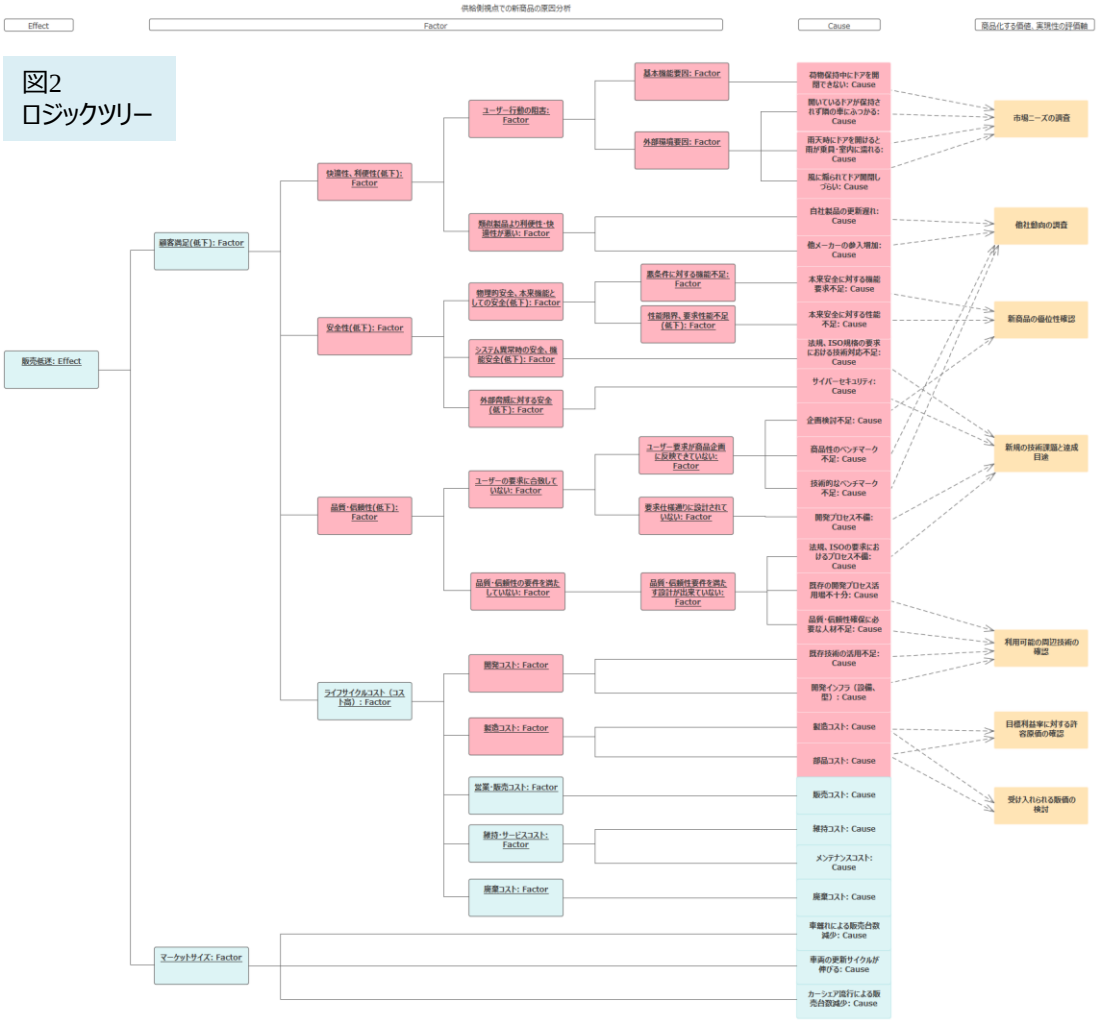
- 顧客満足低下
  a. 快適性、利便性
  b. 安全性
  c. ライフサイクルコスト
  d. 品質、信頼性
- マーケットサイズ

3.2.市場と実現性に関する分析

ロジックツリー分析

ロジックツリー分析により、特性（Effect）、要因（Factor）、原因（Cause）の切り口で分析し、商品化に対する価値、実現性の評価軸を抽出した。

図2
ロジックツリー



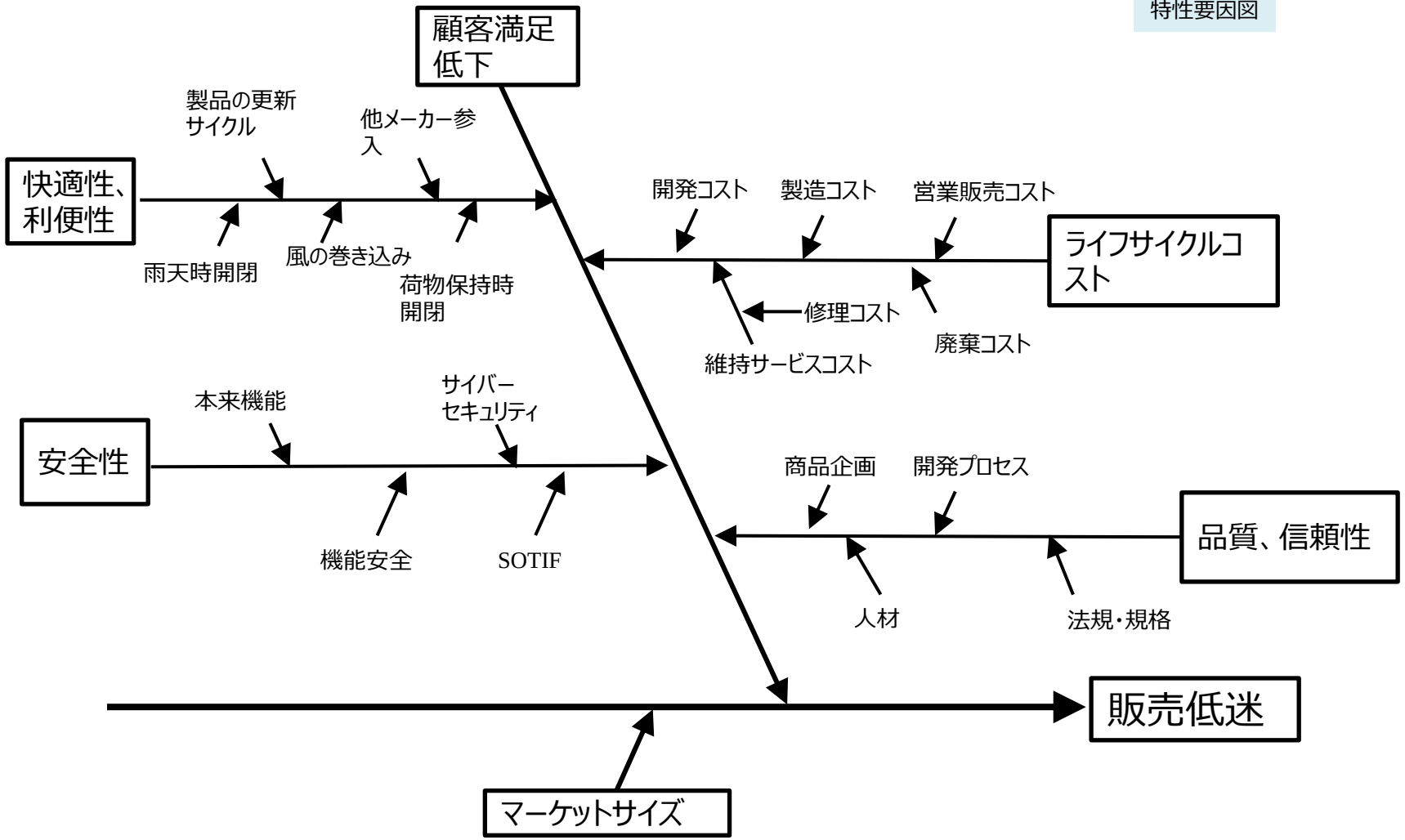
分析の観点を
・快適性、利便性
・安全性
・品質、信頼性
・ライフサイクルコスト
・マーケットサイズ
に分類。

ピンクの網掛け部を本スタディにおける要求の対象とした。

3.2.市場と実現性に関する分析

■ 特性要因図（フィッシュボーン）

図3
特性要因図



3.2.市場と実現性に関する分析

商品化判断時の市場性と実現性に関する分析として、今回の仮想プロジェクトとしては、以下のような目的に対応した分析が実施され、Howに示す活動を行ったことにより次ページのような分析結果が得られたことにした。

Why:

商品化する価値、実現性の評価軸に対し、商品化する価値、実現性がありそうか、判断したい。

What:

以下の評価軸に対し見極める

- ✓ 市場のニーズ
- ✓ 他社の動向
- ✓ 新商品企画の優位性
- ✓ 受け入れられる販価
- ✓ 目標利益率から来る許容原価
- ✓ 使えそうな自社技術
- ✓ 新開発が必要な技術領域と実現の目途

How:

以下の方策で見極める。

- リサーチ業者に依頼し、アンケート実施
- 他社動向調査部署のDB
- 原価管理部署との相談
- 開発部門内でブレスト

3.2.市場と実現性に関する分析

商品化する価値、実現性の分析結果：

車両の自動ドアに対するアンケート調査の結果以下のようなユーザーニーズがあることが分かった

- 荷物や傘などを持っていて手がふさがっているときに手を使わずにドアを開閉したい
- 素早く乗り降りしたいので、事前にドアが開いていると助かる
- ドアを大きく開くと隣とぶつかるような状況で、限界まで開いて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）

車両の自動ドアに対する社内DBを用いた調査結果以下の他社事例、新商品の優位性が分かった

- リアハッチやスライドドアを開くものが存在する
- 運転席や助手席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
- タクシーは後席左側のみ運転手の操作による自動開閉

社内ブレストにより以下のような新商品優位性、使えそうな自社技術、技術的課題が分かった

- 隣の車にぶつからないようにドア位置を維持する機能は自動開閉時以外にもニーズがある
- 自動運転車では自車周辺の障害物が把握できる
- 自動運転車のサイバーセキュリティ対応プロセスや方策の活用が可能
- ドア開閉、ドア開状態の維持は自社のモータリンク機構が応用できる可能性あり
- 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

ロジックツリー分析の気づき、考察

本SWG活動においては、ロジックツリー分析を用いて分析を行った。
理由は下記の通り。

- 商品の市場性・実現性に関する分析の全体像を俯瞰できる。
- 「課題提起」、「要求分析」、「解決策提示」の工程を構造化し明確化できる。
- 市場性・実現性分析に対して、課題提起～解決に向けた課題の提示までのトレーサビリティを取ることができる。

⇒ 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。
作業工程の層別とトレーサビリティを意識した本分析手法は特に有効と考える。

一方、フィッシュボーンは問題の要因を演繹的に分析する手法として便利であり、分析を進捗させる観点でロジックツリー分析と併用する活用方法も考えられる。

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

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。

その活動の動機・目的・適用手法を以下に整理する。

Why:

利害関係者の期待を適切に実現するためには、対象システム(SoI)が何をすべきかを明確にしたい。

What：

システムに求められる機能要求、非機能要求の導出

How：

- 利害関係者要求の整理(3.3.1項)
- システムコンテキストの整理(3.3.2項)
- ユースケース分析(3.3.3項)
- 対象システムに必要となる機能要求の導出(3.3.4項)
- 対象システムの機能要求に対する有効性の尺度（MoE）の導出(3.3.5項)

3.3.1.利害関係者要求の整理

SoI分析のうち利害関係者ニーズの分析について、動機・目的・適用手法を以下に整理する。

Why　：

利害関係者の要求を分析することで、登場人物は誰で、誰がどんなシーンでどんなニーズをもっているかを明らかにする。

What:

以下の項目について分析を行う。

- 利害関係者
- 利害関係者ニーズ
- ニーズから導出されるシステムに対する要求

How:

表を用いて上記項目を整理する。

3.3.1.利害関係者要求の整理

■ 要求分析における用語の整理

要求，要件などの語が頻出するので　分析に先立ちここでの用語の使い方を整理しておく

ニーズ：

利害関係者（ここでは、車の利用者と、開発者・製品提供者）のシステムに対する 要求，要望，期待，希望・・・などを述べたものとする。（車の利用者のニーズは、ユーザ目線でシステムに求める機能や使い勝手の表現になる）

それ以外にもシステムを取り巻く周辺状況（コンテキスト）からの制約なども含むべき。（例えば社会的制約や市場受容性などもニーズとして利害関係者に紐づけることとする）

↓

視点・立ち位置を変えることでニーズは要求にブレークダウンすることができる

↓

要求：

対象システムが満たすべき　あるいは達成すべき機能や性質を述べたものとする。（要求，要件，制約（コンストレインツ），条件（コンディション）・・などを含む）

例えばシステムの機能要求，非機能要求，性能要求，QCD的要件，法規要件，量産性に関する制約事項，メンテ容易性に関する条件　などになる。このうちのいくつかは非機能要求に分類される。

・要求の源泉をすべて利害関係者のニーズに帰着するか，システムを取り巻く状況に求めるかは、考え方によっていくつかの取り扱いがあると考える。例えば安全性は社会的要請というコンテキスト側からも 製品供給者の指向からも紐づけることが出来ると言える。

・‘要求’ や ‘コンテキスト’ は、各分析毎に粒度の配慮が必要となる。

3.3.1.利害関係者要求の整理

表1

利害関係者ニーズとシステム要求の分析結果

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

3.3.2.システムコンテキストの整理

システムと利用者や環境などとの関係を明らかにするためのアプローチとしてシステムコンテキストの可視化に取り組んだ。 その活動の動機・目的・適用手法を以下とした。

Why:

システム実現するための課題と解決策を抽出可能とするために、対象システムと周囲との相互作用を可視化する。

What：

対象システムとその周囲について、分析することにした。

How：

ブロック定義図（図３）と、コンテキスト図（図４）にまとめる。

まずは、前ページの分析表を参考に、システムコンテキスト（ 対象システムと各アクター ）をブロック定義図に記載した。

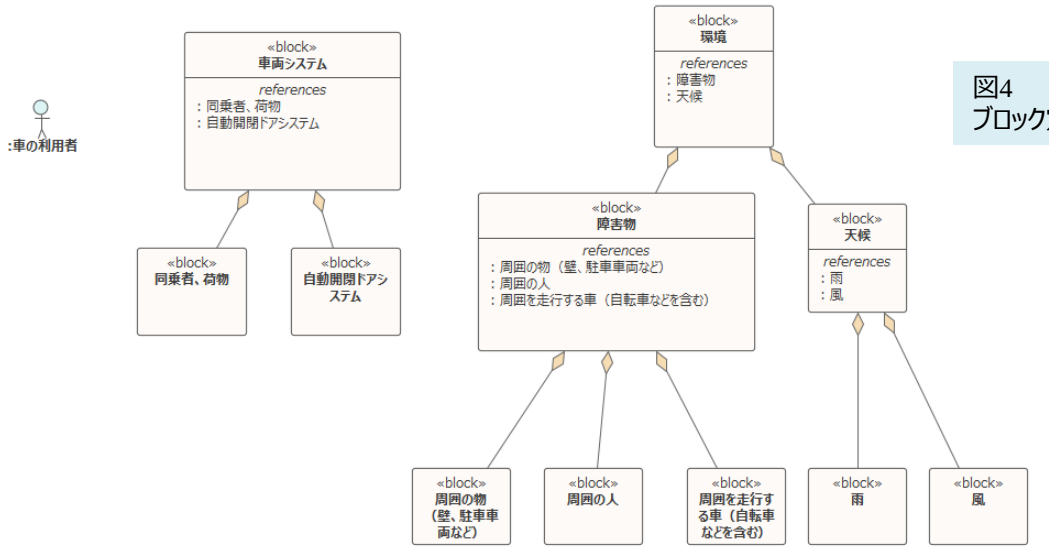
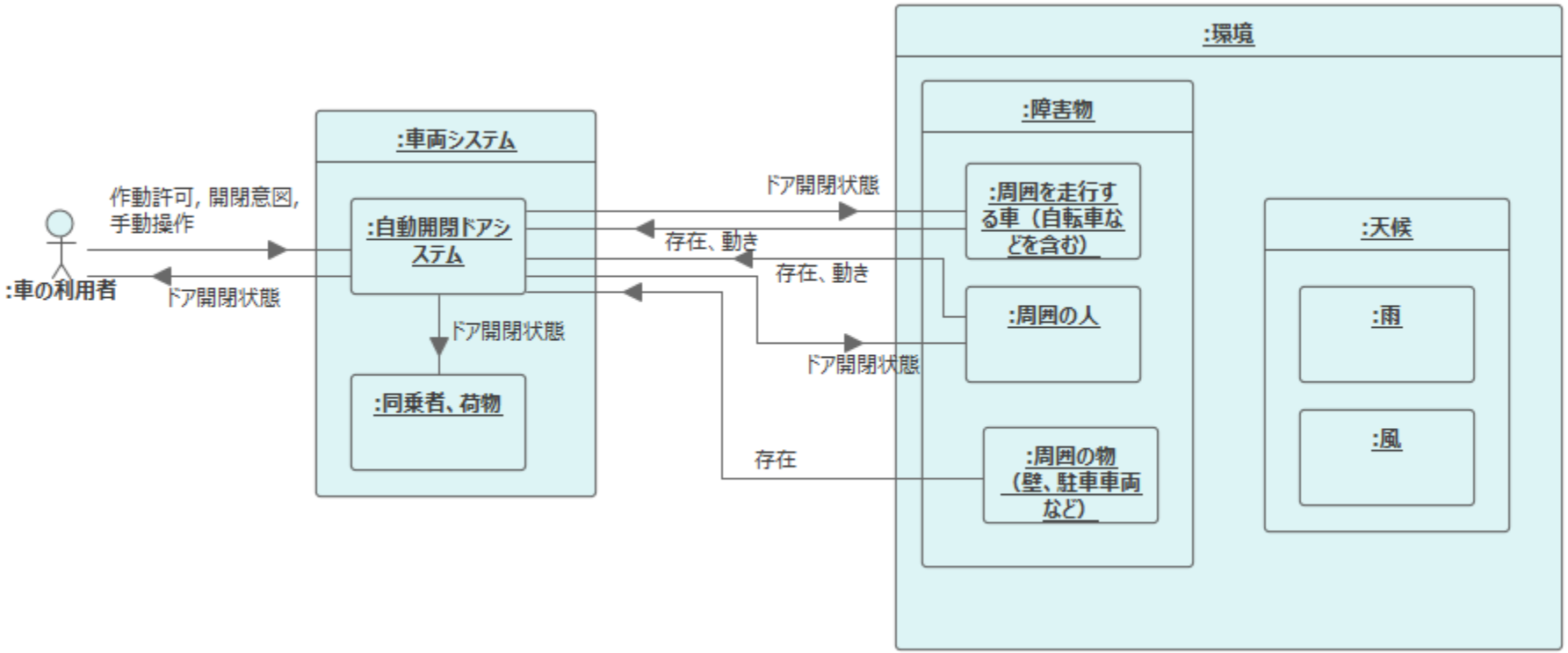


図4
ブロック定義図

3.3.2.システムコンテキストの整理

前ページのブロック定義図と分析表から、対象システムと各アクター、それらの間の相互作用をアイテムフローとし、コンテキスト図にまとめた。

図5
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取り組んだ。 その活動の動機・目的・適用手法を以下とした。

Why, What：

対象システムに求められる機能を明らかにしたい

How：

ユースケース図（図５）、ユースケースシナリオ（表２， ３）を用いて分析

まず、利害関係者要求の分析結果に基づき、対象システムに必要な機能をユースケース図にまとめることにした。

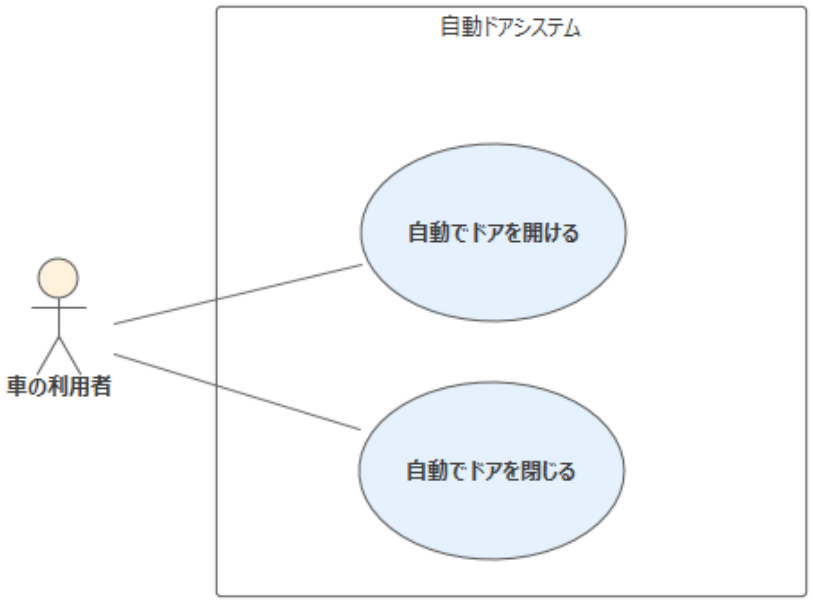


図6
ユースケース図

3.3.3.ユースケース分析

次に、ユースケース図のユースケース毎に　ユースケースシナリオを表2と表3にまとめた。

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		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

前項のユースケース分析の結果を用い、システムに求められる機能要求を明らかにするための活動に取り組んだ。 その活動の動機・目的・適用手法を以下とした。

Why, What：

対象システムに求められる機能要求を明らかにしたい。

How：

ユースケースシナリオを元に、対象システムに必要な機能要求として整理した。

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.有効性の尺度（MoE）

前項の機能要求の導出の結果に対し、対象システムの機能要求に対し求められる性能などを明らかにするための活動に取り組んだ。 その活動の動機・目的・適用手法を以下とした。

Why, What：

対象システムの機能要求に対し、求められる（定性的な）性能などが実現できることを確認したい。

How：

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）として定義した。

また、定義漏れが無いことを表でチェックした。

3.3.5.有効性の尺度（MoE）

機能要求に対するMoE

表5

	機能要求-MoE	MoE																	
		IGN SW の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

3.4.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ために、以下のような活動に取り組んでみた。
その活動の動機・目的・適用手法を以下に整理する。

Why：

対象システムがシステムライフサイクルにおいて安全性を担保できるようにしたい。

What：

以下を明らかにしたい。

- 対象システムに潜むハザードを漏れなく識別する。
- リスクの度合いを評価し、それに基づきリスク低減対策の要否と手厚さを判断する。

How：

今まで整理をしてきた対象システムに対し、以下の手順でハザード分析＆リスクアセスメントを実施する。

- ハザードの分析として、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）
- リスクアセスメントとして、ハザード分析の結果に対し、危険事象が事故に至る場合に想定される危害の大きさと発生確率および基準に基づきリスクを評価し、識別された許容できないリスクに対して最上位の安全要件となる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

Why:

対象システムに潜むハザードを漏れなく識別したい。

What:

対象システムの各構成要素の故障だけでなく、各構成要素の相互作用が適切に働かなくなることも含めて分析を行う。

How:

以下を用いて分析する。

- 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

3.4.1.ハザード分析（前提条件表）

Why, What:

何が、非安全なコントロールアクション（UCA)に該当するのかをしっかりと見極められるようにするため、分析対象のシステムの理解し、その分析範囲を明確にしたい。

How:

分析範囲のシステムの過程や前提条件を前提条件表を用いて時系列で整理する。

- 前提条件表

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

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）

Why:

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たい。また、UCA識別のInputとするため、安全制約も整理する。

What:

どのようなアクシデントを扱うのか、そのアクシデントにつながるハザードを抽出し、そのアクシデントに至らないように、分析対象を安全に保つための安全制約を抽出する。

How:

次ページの表を用いて、アクシデント, ハザード, 安全制約を抽出をする。

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）

- アクシデント、ハザード、安全制約表

表7
アクシデント・ハザード・安全制約表

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

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）

アクシデント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	ユーザーにアイテム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速い	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速い	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とまる	SC2	ユーザーにアイテムの異常を認識させる
A2	急にドアが開き物が転げ落ちる	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A2	急にドアが開き物が転げ落ちる	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
A2	急にドアが開き物が転げ落ちる	H2	システムの作動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
A2	急にドアが開き物が転げ落ちる	H3	意図したよりドアの開くタイミングが速い	SC3	ドアが開くタイミングは常に一定である
A2	急にドアが開き物が転げ落ちる	H3	意図したよりドアの開くタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A2	急にドアが開き物が転げ落ちる	H4	ドア付近の障害物の検知が途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A3	急にドアが開き人が転げ落ち、追い掛けましくは対向車両が人を轢く。	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A3	急にドアが開き人が転げ落ち、追い掛けましくは対向車両が人を轢く。	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
A3	急にドアが開き人が転げ落ち、追い掛けましくは対向車両が人を轢く。	H5	走行中が判定できない	SC2	ユーザーにアイテムの異常を認識させる
A4	急にドアが開き物が転げ落ち、追い掛けましくは対向車両が物を轢く。	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A4	急にドアが開き物が転げ落ち、追い掛けましくは対向車両が物を轢く。	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
A4	急にドアが開き物が転げ落ち、追い掛けましくは対向車両が物を轢く。	H5	走行中が判定できない	SC2	ユーザーにアイテムの異常を認識させる
A5	急にドアが開き人や物が転げ落ち、追い掛きもしくは対向車両が回避しようとしたが、衝突する。	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A5	急にドアが開き人や物が転げ落ち、追い掛きもしくは対向車両が回避しようとしたが、衝突する。	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
A5	急にドアが開き人や物が転げ落ち、追い掛きもしくは対向車両が回避しようとしたが、衝突する。	H5	走行中が判定できない	SC2	ユーザーにアイテムの異常を認識させる
A6	開いたドアに他の車両が衝突する。	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A6	開いたドアに他の車両が衝突する。	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
A6	開いたドアに他の車両が衝突する。	H4	ドア付近の障害物の検知が途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A6	開いたドアに他の車両が衝突する。	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
A6	開いたドアに他の車両が衝突する。	H7	ドアの開く速度が速い	SC4	ドアが開く速度は常に一定である
A6	開いたドアに他の車両が衝突する。	H7	ドアの開く速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A6	開いたドアに他の車両が衝突する。	H8	障害物の検出タイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる
A6	開いたドアに他の車両が衝突する。	H9	ドア付近の障害物を検知しない	SC2	ユーザーにアイテムの異常を認識させる
A6	開いたドアに他の車両が衝突する。	H10	障害物の検出距離が実測より狭い	SC5	手動でドア開閉できる
A7	開いているドアに気づかず人・車がドアに衝突する	H4	ドア付近の障害物の検知が途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A7	開いているドアに気づかず人・車がドアに衝突する	H8	障害物の検出タイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる
A7	開いているドアに気づかず人・車がドアに衝突する	H9	ドア付近の障害物を検知しない	SC2	ユーザーにアイテムの異常を認識させる
A7	開いているドアに気づかず人・車がドアに衝突する	H10	障害物の検出距離が実測より狭い	SC5	手動でドア開閉できる
A7	開いているドアに気づかず人・車がドアに衝突する	H7	ドアの開く速度が速い	SC4	ドアが開く速度は常に一定である
A7	開いているドアに気づかず人・車がドアに衝突する	H7	ドアの開く速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A8	ドアが開き物が当たる	H1	意図せずドアが開く	SC1	ユーザーにアイテムを開ける意志がない限りドアを開かない
A8	ドアが開き物が当たる	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
A8	ドアが開き物が当たる	H2	システムの作動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
A8	ドアが開き物が当たる	H3	意図したよりドアの開くタイミングが速い	SC3	ドアが開くタイミングは常に一定である
A8	ドアが開き物が当たる	H3	意図したよりドアの開くタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H11	意図したのにドアが開かない	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	H11	意図したのにドアが開かない	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H12	ドア付近に障害物がないのに誤検知する	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	H12	ドア付近に障害物がないのに誤検知する	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H13	障害物の検出距離が実測より狭い	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	H13	障害物の検出距離が実測より狭い	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H3	意図したよりドアの開くタイミングが速い	SC3	ドアが開くタイミングは常に一定である
A9	開くと思って乗ろうとしてドアにぶつかる	H3	意図したよりドアの開くタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H14	開きまらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H14	開きまらずにドアが途中でとまる	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	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
A9	開くと思って乗ろうとしてドアにぶつかる	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A9	開くと思って乗ろうとしてドアにぶつかる	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A9	開くと思って乗ろうとしてドアにぶつかる	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる

A10	意思もしくはECUや車になる	H11	意図したのにドアが開かない	SC5	手動でドア開閉できる
A10	意思もしくはECUや車になる	H11	意図したのにドアが開かない	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H20	手動操作が優先されない	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H20	手動操作が優先されない	SC5	手動でドア開閉できる
A10	意思もしくはECUや車になる	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A10	意思もしくはECUや車になる	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A10	意思もしくはECUや車になる	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A10	意思もしくはECUや車になる	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A11	時中確になる	H11	意図したのにドアが開かない	SC5	手動でドア開閉できる
A11	時中確になる	H11	意図したのにドアが開かない	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H20	手動操作が優先されない	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H20	手動操作が優先されない	SC5	手動でドア開閉できる
A11	時中確になる	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A11	時中確になる	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A11	時中確になる	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A11	時中確になる	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A12	投体温になる	H11	意図したのにドアが開かない	SC5	手動でドア開閉できる
A12	投体温になる	H11	意図したのにドアが開かない	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H20	手動操作が優先されない	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H20	手動操作が優先されない	SC5	手動でドア開閉できる
A12	投体温になる	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A12	投体温になる	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A12	投体温になる	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A12	投体温になる	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A13	開にかけのドアを避けられずに人・車が衝突する	H21	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A13	開にかけのドアを避けられずに人・車が衝突する	H21	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A13	開にかけのドアを避けられずに人・車が衝突する	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A14	開にかけの状態で走り出していまい、衝義や物が動け落ちる	H21	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A14	開にかけの状態で走り出していまい、衝義や物が動け落ちる	H21	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A14	開にかけの状態で走り出していまい、衝義や物が動け落ちる	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A15	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が走る。	H21	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A15	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が走る。	H21	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A15	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が走る。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A16	開にかけの状態で走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を踏む。	H21	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A16	開にかけの状態で走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を踏む。	H21	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A16	開にかけの状態で走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を踏む。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A17	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H21	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A17	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H21	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A17	開にかけの状態で走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A18	開にたドアに人が挟まれる	H23	ドアが開じる速度が速い	SC6	ドアが開じる速度は常に一定である
A18	開にたドアに人が挟まれる	H23	ドアが開じる速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A18	開にたドアに人が挟まれる	H24	意図しないのにドアが開じる	SC5	手動でドア開閉できる
A18	開にたドアに人が挟まれる	H24	意図しないのにドアが開じる	SC7	ユーザーにドアを開める意志がない限りドアを開めない
A18	開にたドアに人が挟まれる	H9	ドア付近の障害物を検知しない	SC2	ユーザーにアイテムの異常を認識させる
A18	開にたドアに人が挟まれる	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
A18	開にたドアに人が挟まれる	H2	システムの作動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
A18	開にたドアに人が挟まれる	H8	障害物の検出タイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる
A18	開にたドアに人が挟まれる	H4	ドア付近の障害物の検知が途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H25	意図したのにドアが開じない	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H26	意図よりドアの開じるタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A19	開にると思って走り出していまい、衝義や物が動け落ちる	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

A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	H25	意図したのにドアが開じない	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	H26	意図よりドアの開じるタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A20	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が人を轢く。	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
A20	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A20	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A20	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H25	意図したのにドアが開じない	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H26	意図よりドアの開じるタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	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
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A21	開にると思って走り出していまい、物が動け落ち、追い突きもしくは対向車両が物を轢く。	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H25	意図したのにドアが開じない	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H22	開まりきらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H26	意図よりドアの開じるタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H15	走行中と誤判定する	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H15	走行中と誤判定する	SC5	手動でドア開閉できる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	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
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H17	システムが作動許可にならない	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H19	ドアの開閉状態が逆に伝わる	SC2	ユーザーにアイテムの異常を認識させる
A22	開にると思って走り出していまい、人や物が動け落ち、追い突きもしくは対向車両が回避しようとしたが、衝突する。	H19	ドアの開閉状態が逆に伝わる	SC5	手動でドア開閉できる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H3	意図したよりドアの開くタイミングが速い	SC3	ドアが開くタイミングは常に一定である
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H3	意図したよりドアの開くタイミングが速い	SC2	ユーザーにアイテムの異常を認識させる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H11	意図したのにドアが開かない	SC2	ユーザーにアイテムの異常を認識させる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H11	意図したのにドアが開かない	SC5	手動でドア開閉できる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H14	開きまらずにドアが途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H14	開きまらずにドアが途中でとまる	SC5	手動でドア開閉できる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H29	意図しないのにドアが開じる	SC2	ユーザーにアイテムの異常を認識させる
A23	ドアが開じと思ってドライバーがホームよりとしたときにドアにぶつかる	H29	意図しないのにドアが開じる	SC7	ユーザーにドアを開める意志がない限りドアを開めない
A24	ドアのホルスがおれず、ぶつかる	H8	障害物の検出タイミングが遅い	SC2	ユーザーにアイテムの異常を認識させる
A24	ドアのホルスがおれず、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
A24	ドアのホルスがおれず、ぶつかる	H7	ドアの開く速度が速い	SC4	ドアが開く速度は常に一定である
A24	ドアのホルスがおれず、ぶつかる	H7	ドアの開く速度が速い	SC2	ユーザーにアイテムの異常を認識させる
A24	ドアのホルスがおれず、ぶつかる	H33	障害物の検出距離が実測より狭い	SC2	ユーザーにアイテムの異常を認識させる
A24	ドアのホルスがおれず、ぶつかる	H6	ドアの開位置が維持できない	SC5	手動でドア開閉できる
A24	ドアのホルスがおれず、ぶつかる	H4	ドア付近の障害物の検知が途中でとまる	SC2	ユーザーにアイテムの異常を認識させる
A25	ドアが閉じ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	ドアが閉じ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	ドアが閉じ開きドアが周囲の物にぶつかる	H18	ドアの開閉状態が応わらない	SC2	ユーザーにアイテムの異常を認識させる
A25	ドアが閉じ開きドアが周囲の物にぶつかる	H18	ドアの開閉状態が応わらない	SC5	手動でドア開閉できる
A25	ホルスアを開けようとしたときにドア開かずに脚子共や近づいたときにホルスドアが開き、ぶつかる	H3	意図したよりドアの開くタイミングが速い	SC3	ドアが開くタイミングは常に一定である
A25	ホルスアを開けようとしたときにドア開かずに脚子共や近づいたときにホルスドアが開き、ぶつかる	H3	意図したよりドアの開くタイミングが速い	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
表全体

3.4.1.ハザード分析（CS図）

Why:

分析対象の構造とその依存関係を把握し、その結果をもとにコントロールストラクチャーを作成する。

What:

分析対象の構造(コンポーネント)とその役割を抽出し、役割を果たすために必要となる制御、役割を果たした結果のフィードバックを抽出する。

How:

次ページに示すコンポーネント抽出表を用いて整理し、その結果を用いて、次々ページに示すコントロールストラクチャ図で表す。

3.4.1.ハザード分析（CS図）

- コンポーネント抽出表

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)			

3.4.1.ハザード分析（CS図）

- コントロールストラクチャ図

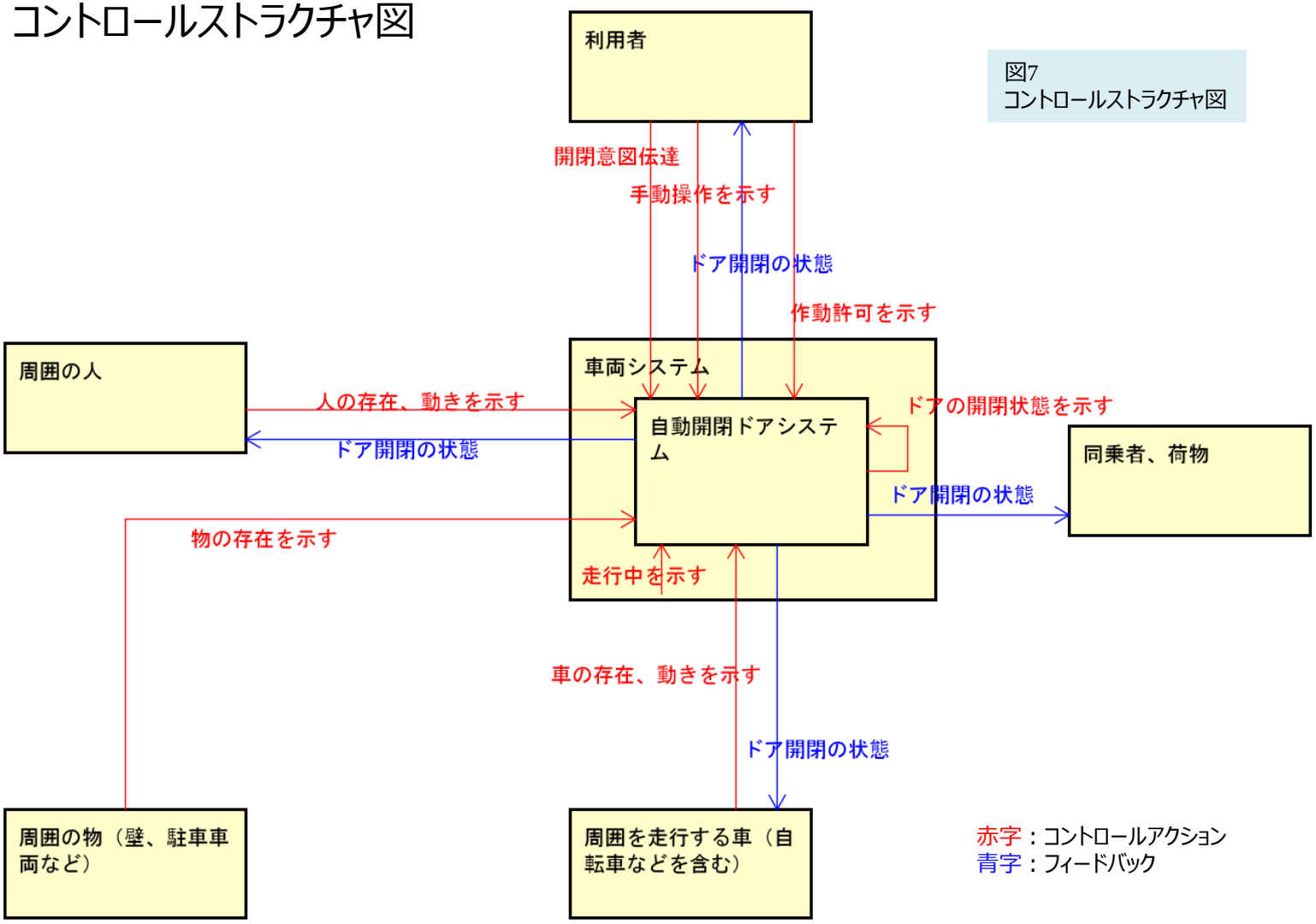


図7
コントロールストラクチャ図

3.4.1.ハザード分析（UCA表）

Why:

ハザードにつながり得る制御動作の不具合を識別する。

What:

各制御（コントロールアクション）毎にガイドワードをヒントにして、コントロールアクションがハザード/アクシデントにつながるかを分析する。

How:

次ページに示すUCA表を用いて分析する。

3.4.1.ハザード分析（UCA表）

- UCA （Unsafe Control Action）表

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	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]		

表9
UCA表

3.4.2.リスクアセスメント

Why:

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、危険事象の防止又は緩和に関連した安全度水準（ASIL）を持つ安全目標を立てたい。

What:

ハザードに対し想定されるアクシデントと、アクシデント発生に至る危険事象、危険事象ごとのシビアリティ（S）,曝露の確率（E）, コントローラビリティ（C）とそ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う。

How:

次ページの表を用いてリスクアセスメント結果を整理する。

■ 注意： 本書におけるリスクアセスメントの扱い

- リスクアセスメントの手法は本書の目的の対象外であるため、本書では扱わない。
- 本書に記載しているASILおよびE,C,Sの値は、手法連携の検討目的において便宜的に設定したものであり、参考値として取り扱う。

3.4.2.リスクアセスメント

■リスクアセスメントの例を以下に示す

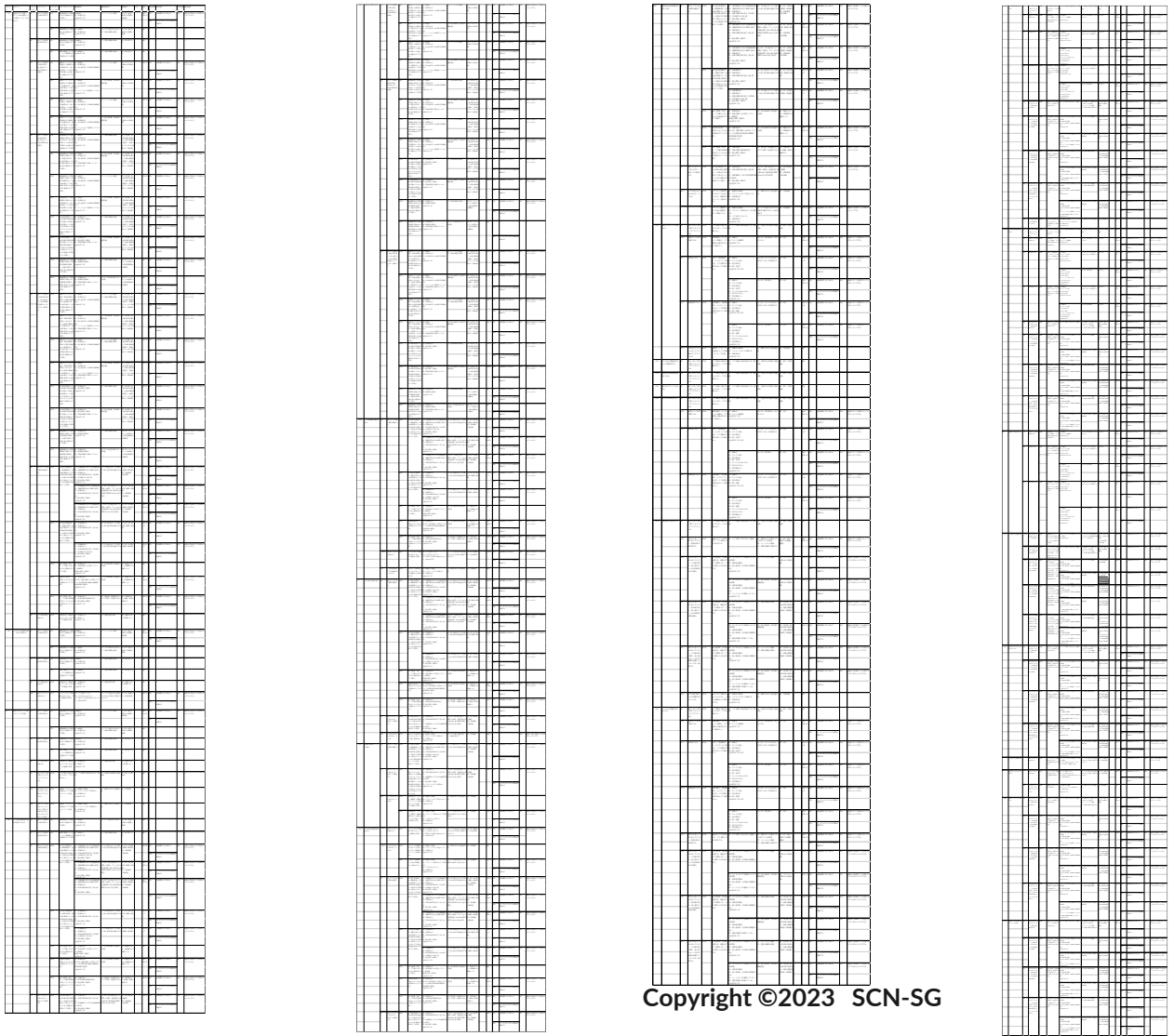
表10

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

■リスクアセスメントの例を以下に示す

表10全体



3.4.2.リスクアセスメント

■ 次に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	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

3.4.1ハザード分析の気づき、考察

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～にも、下記の記載があるように、今回のスタディでもUCA実施後に再度アクシデント・ハザード・安全制約の識別で実施した内容を修正（イタレーション）が発生した。

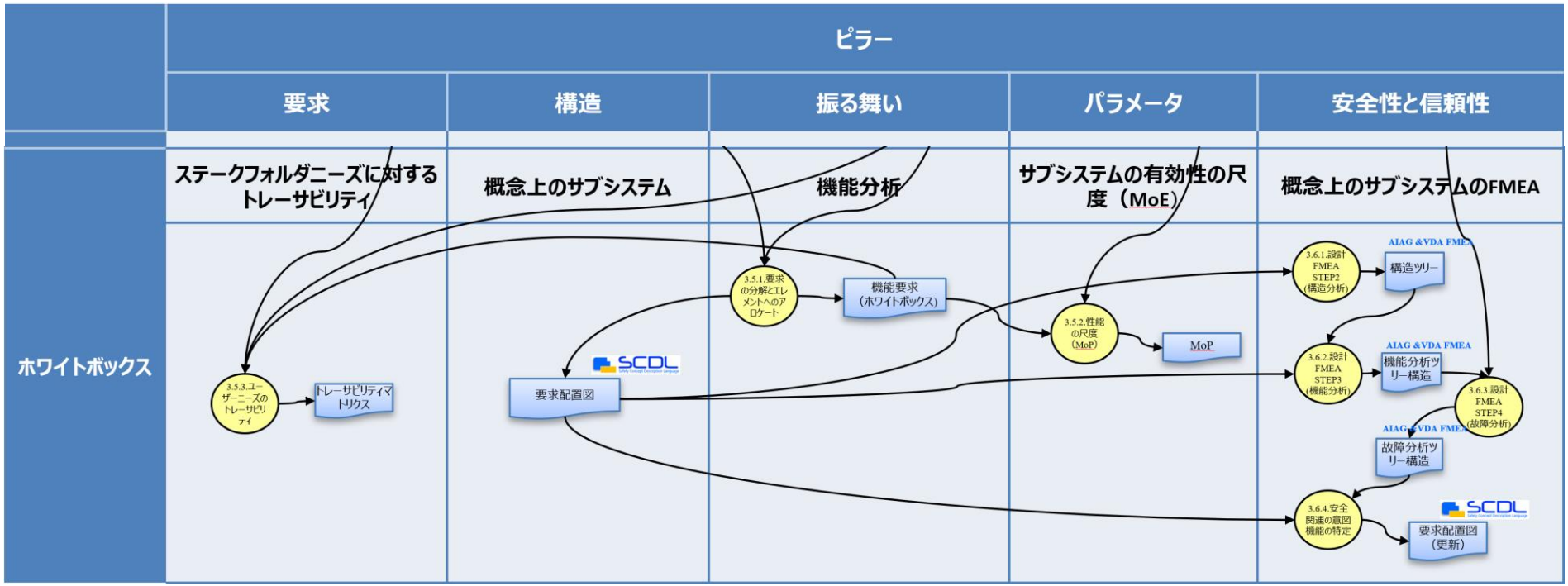
今回のスタディでは、アクシデント・ハザード・安全制約表の内容を用いてリスクアセスメントを行ったため、イタレーションの必要性に気づいたが、トップダウンで作業を進めると気付かず先に進んでしまうこともあると思われる。

UCA の分析結果で、必要に応じてアクシデント・ハザード・安全制約の結果の修正実施を手順としてより明確に記載することを提案したい。

UCA の分析から安全制約を作り出すことも可能である。このため、安全制約を最初の準備の段階でなくここで作成したり、作成済みの安全制約を UCA の分析結果をもとに見直したりすることもできる。

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）

より詳細化した対象システムの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。

その活動の動機・目的・適用手法を以下に整理する。

Why:

詳細化した対象システム(SoI)の振る舞いを把握したい。

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：

- 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

要求仕様の分解とそれらの物理層への配置法を検討した。

WHY:

高次要求を実装に近づけるために具体的サブシステム～部品すなわちエレメントの構造を明らかにし，これらの役割分担を論じたい。

WHAT:

要求仕様を分解し，エレメント構造を明らかにし，エレメント構造に機能要求を配置する。

HOW:

SysMLの要求図ベースに分析し、SCDLの要求配置図によりコンセプト構築する。

3.5.1.要求の分解とエレメントへのアロケート

■ 物理層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
		開閉動作中にドア前後上の人・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

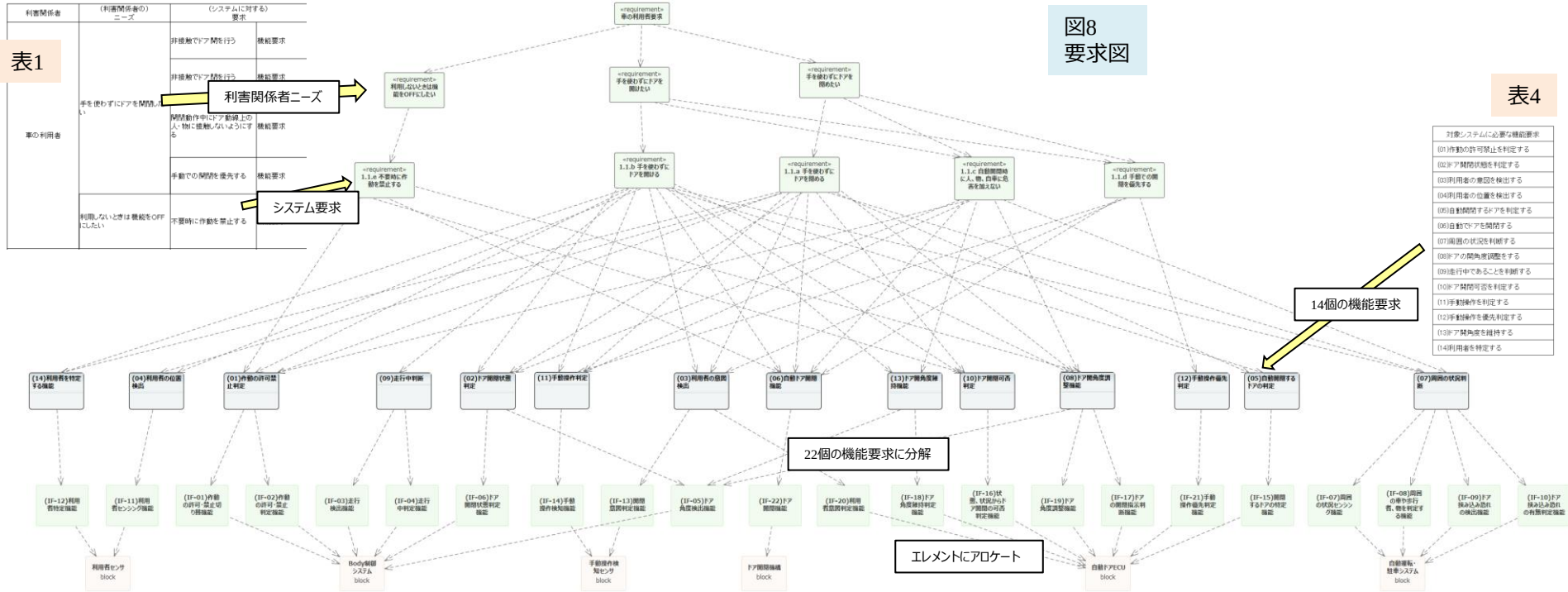


図8
要求図

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

3.5.1.要求の分解とエレメントへのアロケート

■ 前頁の内容を元に表にまとめ、その内容を整理した。

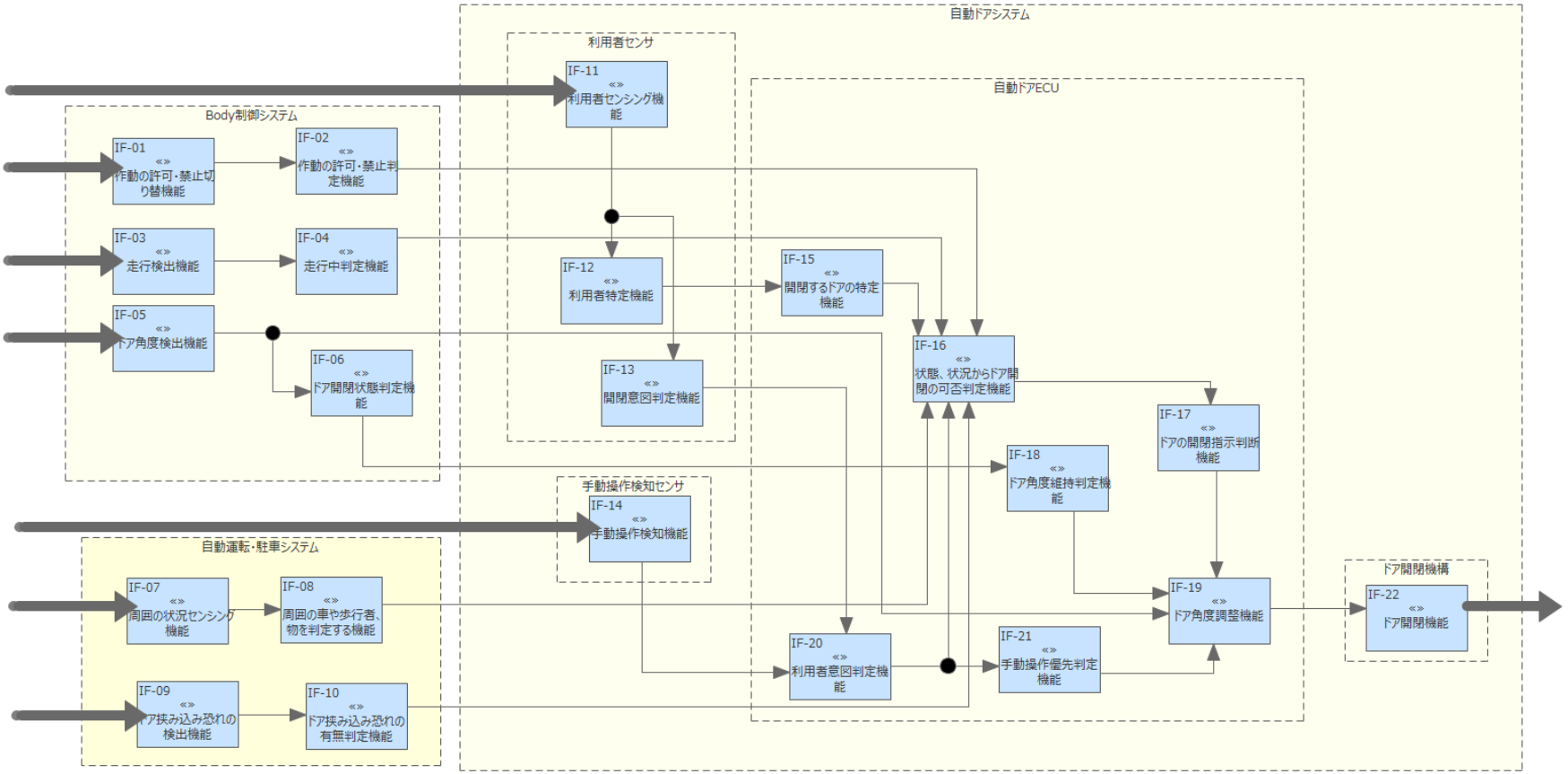
表12

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

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

図9
要求配置図



3.5.2.性能の尺度（MoP）

物理層に対する機能要求として分解された結果に対し、対象システムの機能要求に対し求められる性能などを明らかにするための活動に取り組んだ。 その活動の動機・目的・適用手法を以下とした。

Why, What：

対象システムの機能要求に対し、求められる（定量的な）性能などが実現できることを確認したい。

How：

性能の尺度（MoP）として定義した。

また、定義漏れが無いことを表でチェックした。

3.5.2.性能の尺度（MoP）

機能要求に対するMoP

表13

	機能要求-MoP	MoP																				
		＊＊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										

3.5.3.ユーザーニーズのトレーサビリティ

本書で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、システムに対する機能要求、物理層に対する機能要求間の対応関係(トレーサビリティ)を明らかにするための活動を実施した。その活動の動機・目的・適用手法を以下に整理する。

Why:

機能要求が導出された理由や、ユーザニーズが充足しているかを検証・証明するため、双方向の対応関係(トレーサビリティ)を維持する必要がある。

What :

ユーザニーズと機能要求間の双方向のトレーサビリティを維持する

How:

ユーザニーズと機能要求の対応関係を記録・管理する表であるトレーサビリティマトリックスを用いて維持する

3.5.3.ユーザーニーズのトレーサビリティ

■ ユーザーニーズに紐づく機能要求

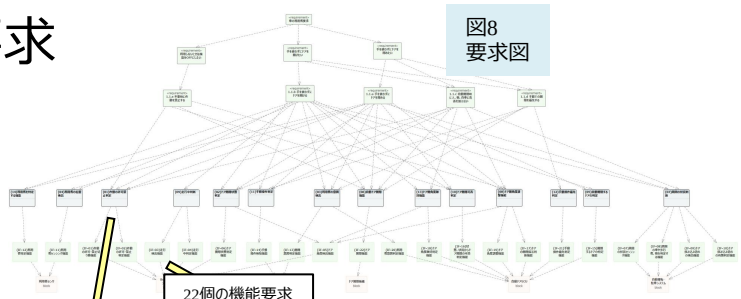


図8
要求図

車の利用者要求							
→	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					←	

利害関係者ニーズ

システム要求

14個の機能要求

22個の機能要求

利害関係者	（利害関係者の）ニーズ	（システムに対する）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	
表1 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	→	→	→		→	(01)作動の許可禁止判定
		非接触でドア閉を行う	機能要求	→	→	→			(02)ドア開閉状態判定
		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	→	→		→		(03)利用者の意図検出
		手動での開閉を優先する	機能要求	→	→				(04)利用者の位置検出
	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	→	→				(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

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
→	→																			
				→	→															
												→						→		
										→										
														→						
																				→
						→	→	→	→											
				→	→											→		→		
	→	→	→												→					
													→							
											→									
						→											→		→	

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、以下のような活動に取り組んでみた。その活動の動機・目的・適用手法を以下に整理する。

Why:

安全方策の検討（救う側の検討）に向け、各安全目標に対しそれを侵害する恐れにある機能要求の特定（救われる側の特定）をする必要がある。

What :

各安全目標毎に、それを侵害する恐れにある機能要求を特定する。

How:

AIAG&VDA-FMEAを用いて分析する。

- 設計FMEA　STEP2構造分析（3.6.1項）
- 設計FMEA　STEP3機能分析（3.6.2項）
- 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（3.6.3項）

安全関連の意図機能を特定する

- FMEAの結果と安全目標(SG)との関係性を表現し、SGを侵害する恐れのある機能要求を特定する。（3.6.4項）

参考（AIAG&VDA-FMEAの他のSTEP）

- 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

安全関連の意図機能の特定をするため、その分析の対象範囲を明確化するため、対象となるシステムの構造を階層的に分解する。その活動の動機・目的・適用手法を以下に整理する。

Why：

技術的リスク分析のために，FMEA の適用範囲を特定して，構造を階層的に分解する。

What：

階層構造で分析対象を可視化し、分析範囲を明らかにする。

How：

階層的なツリー構造を図を用いて分析する。

3.5.1項のSCDLの要求配置図を参照し、構造を階層的に分解した。

3.6.1.設計FMEA　STEP2：構造分析

システムエレメントの階層的なツリー構造

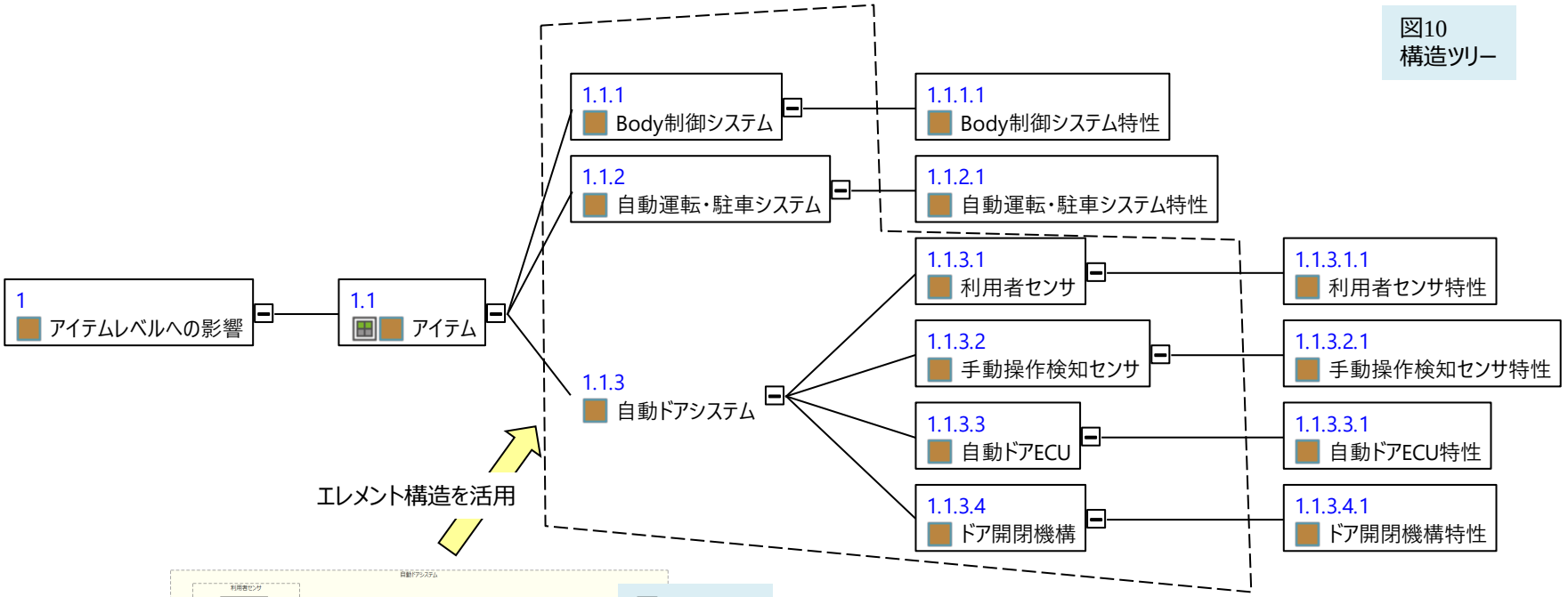


図10
構造ツリー

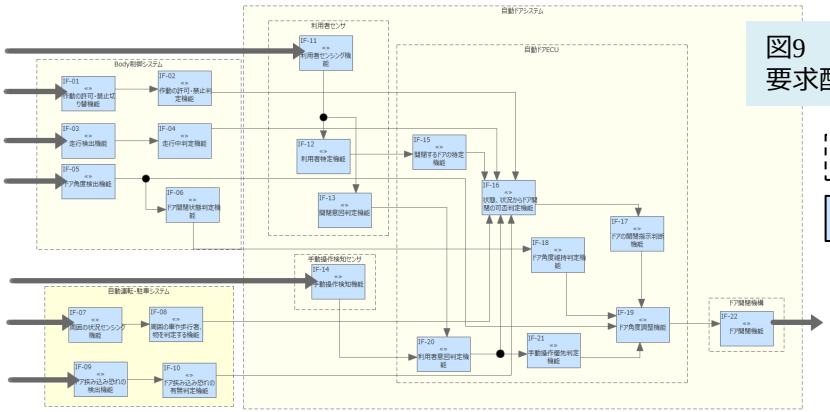


図9
要求配置図

エレメント

機能要求

3.6.2.設計FMEA　STEP3：機能分析

安全関連の意図機能の特定をするため、その各構造に対する機能と、機能間のつながりを明確化する。その活動の動機・目的・適用手法を以下に整理する。

Why：

機能が,構造に適切に配置されることを確実にする。

What：

製品機能の可視化

階層化された構造に対する機能と、それらの機能間のつながりの明確化。

How：

階層的な機能分析のツリー構造を図で表現し、機能間のつながりについても図を用いて分析する。

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

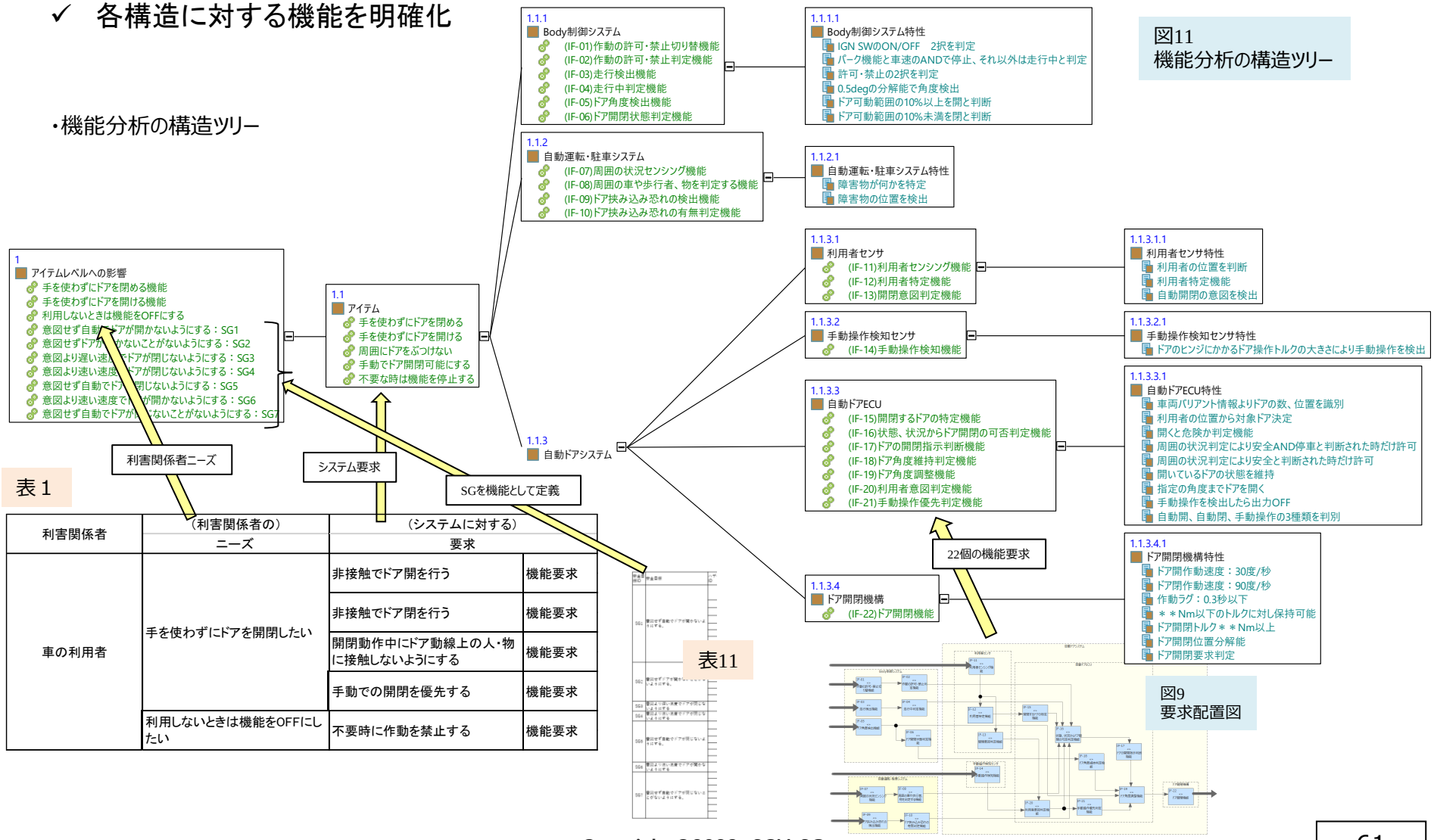


図11
機能分析の構造ツリー

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9
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

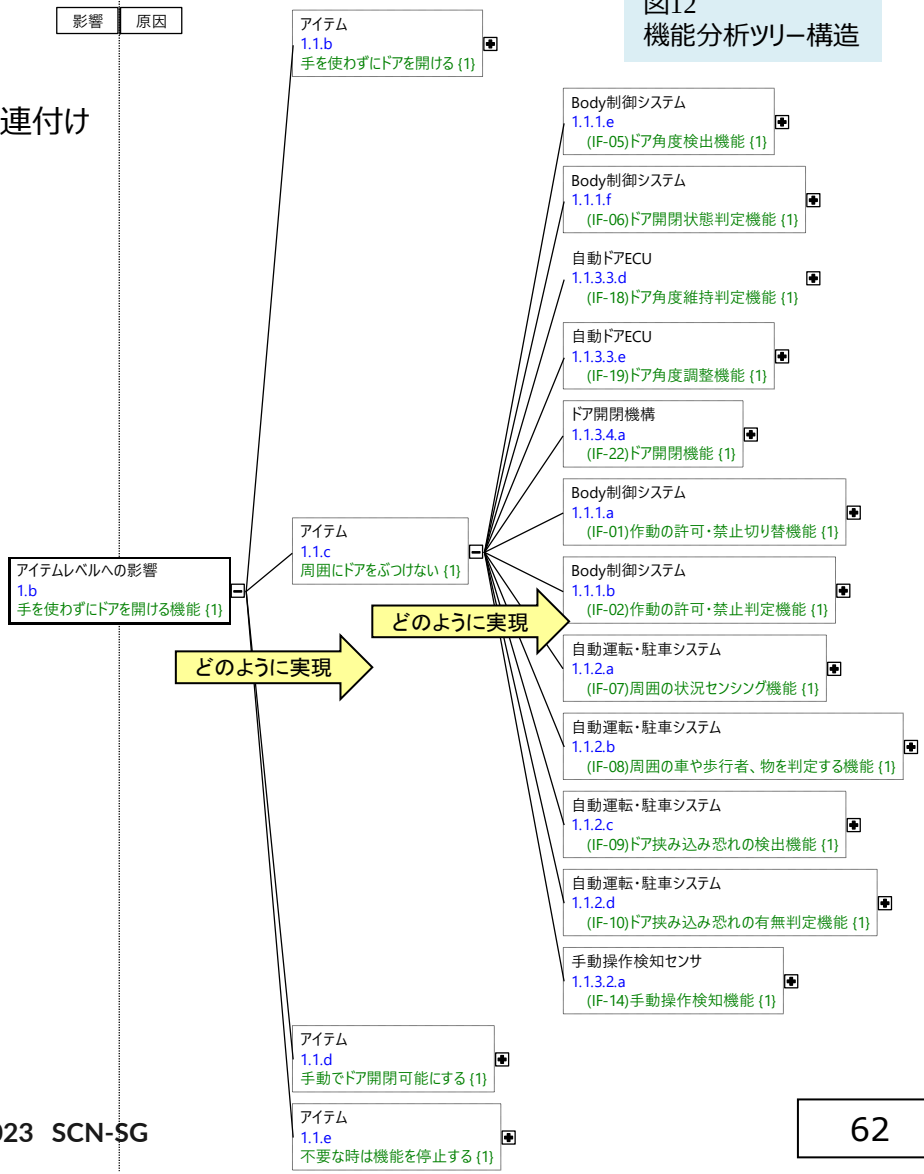


図12
機能分析ツリー構造

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)との関係性の明確化

安全関連の意図機能の特定をするため、その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)との関係を明確化し、故障影響に対する厳しさ(s)の評価を実施する。その活動の動機・目的・適用手法を以下に整理する。

Why：

リスクアセスメントを可能にするために,故障原因，故障モード，及び故障影響を特定し,それらの関係性を示す。

What：

分析対象機能の潜在的故障モードに対する故障影響,故障原因を特定する

故障間のつながりを明確化する。

How：

階層的な故障分析のツリー構造を図で表現し、故障間のつながりについても図を用いて分析する。

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)との関係性の明確化

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

アクシデント

ハザード

ハザードの原因（HAZOPガイドワードを用いて分析）

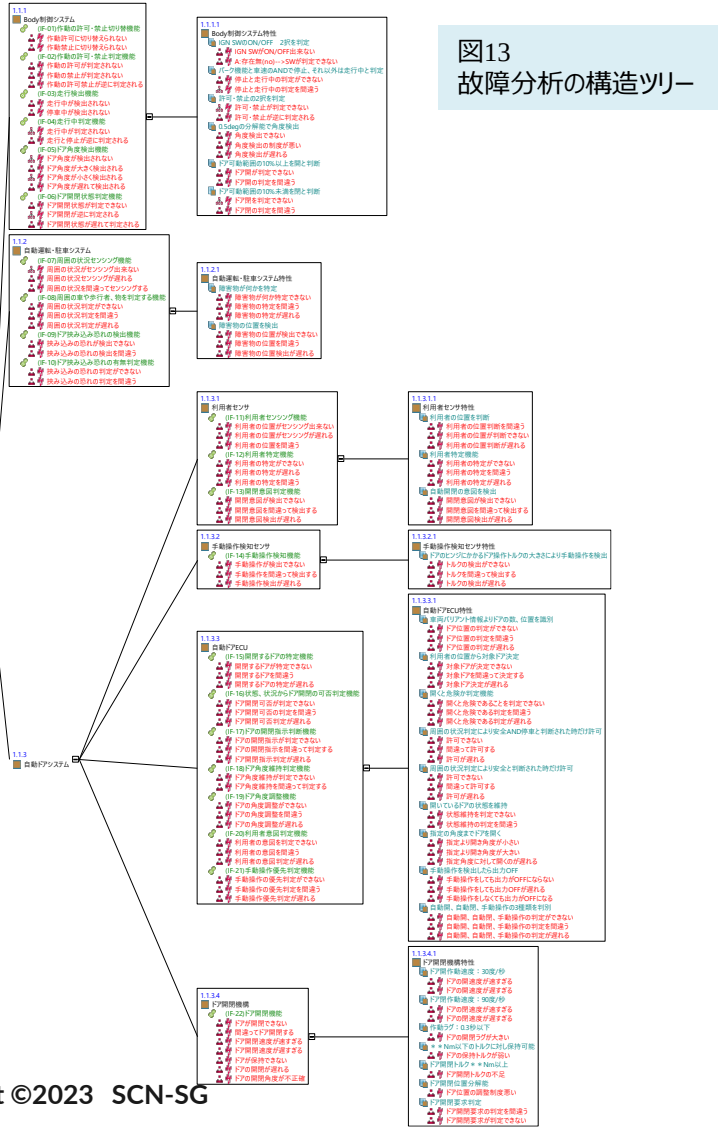


図13
故障分析の構造ツリー

SG侵害をSGの故障モードとして定義

表10

ハザードID	ハザード	アクシデントID	アクシデント	ハザードダイベントID	ハザードダイベント	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

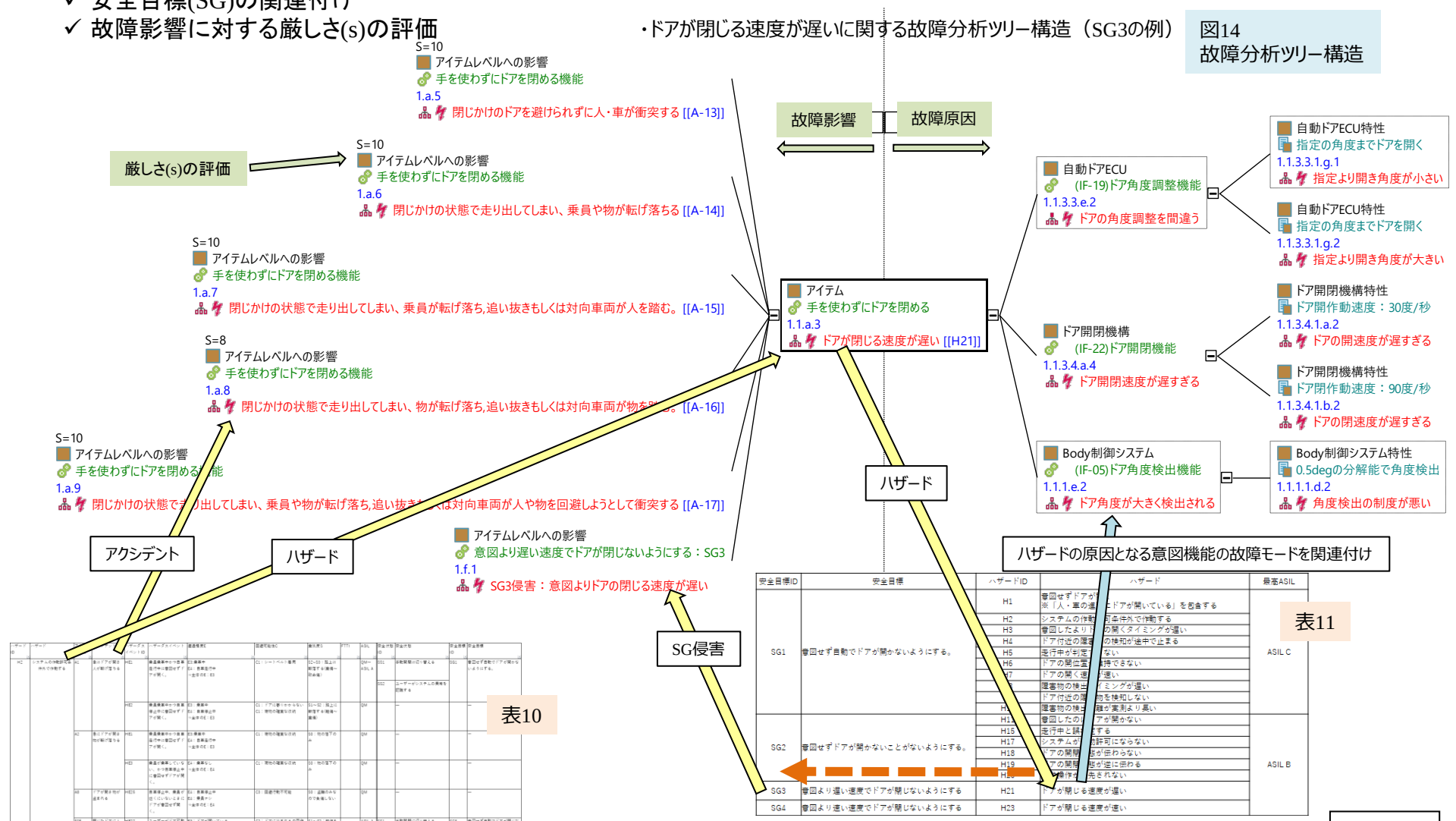
3.6.3.設計FMEA　STEP4：故障分析

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)との関係性の明確化

- ✓ 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14
故障分析ツリー構造



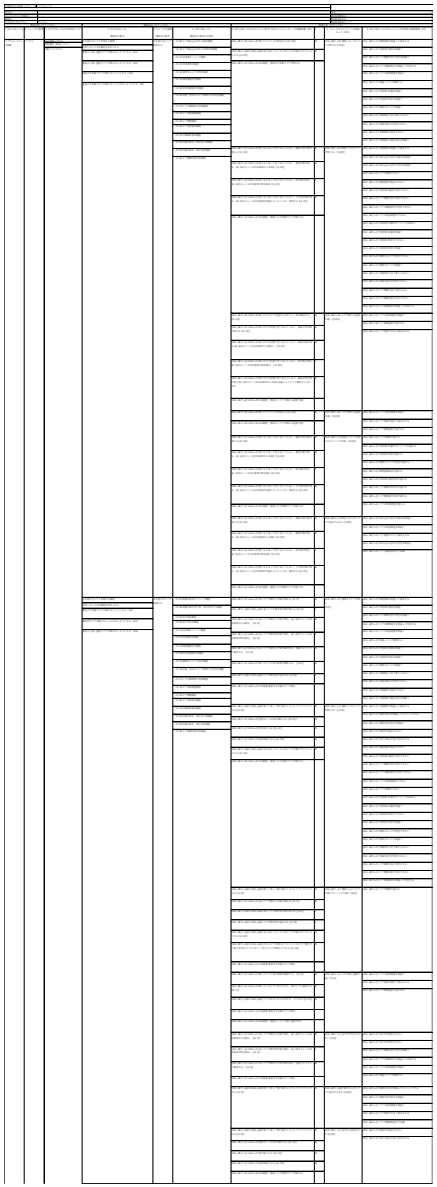
安全目標ID	安全目標	ハザードID	ハザード	最高ASIL
SG1	意図せず自動でドアが開かないようにする。	H1	意図せずドアが開く ※「人・車の通過にドアが開いている」を包含する	ASIL C
		H2	システムの作動条件外で作動する	
		H3	意図したよりドアの開くタイミングが遅い	
		H4	ドア付近の障害物の検知が途中で止まる	
		H5	走行中が判定できない	
		H6	ドアの開位置を維持できない	
		H7	ドアの開く速度が遅い	
			障害物の検出タイミングが遅い	
			ドア付近の障害物を検知しない	
		H1	障害物の検出距離が実測より長い	
SG2	意図せずドアが開かないことがないようにする。	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	システムが開の許可にならない	
		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	操作が完了と判定されない	
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

表10

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)との関係性の明確化



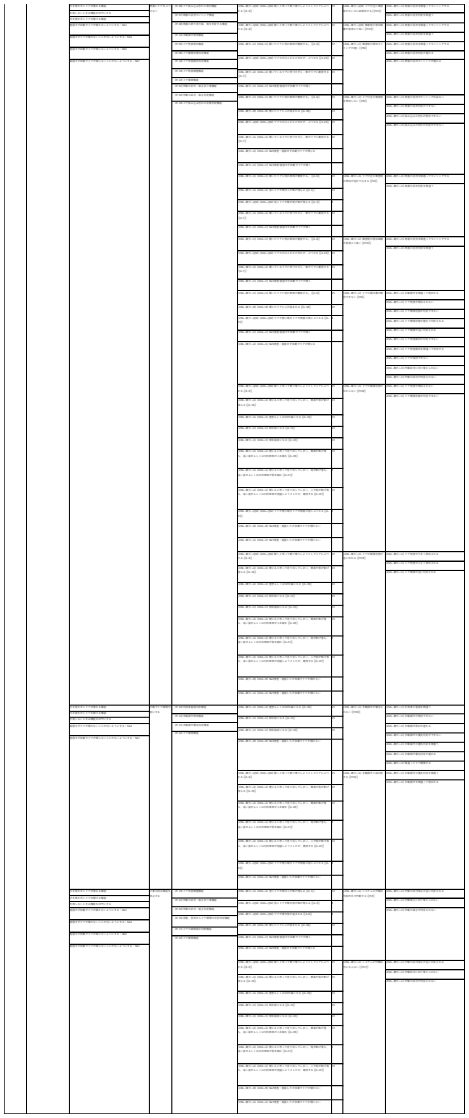


表15
DFMEA表

3.6.4.安全関連の意図機能の特定

安全方策の検討をするために、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する。

その活動の動機・目的・適用手法を以下に整理する。

Why：

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する。

What：

対象システムの機能要求（意図機能）に対し、どの機能要求が安全目標侵害するかを特定する。

How：

3.6.3項の結果から、各安全目標（SG）に関連する機能要求を特定する。

3.5.1項のSCDL要求配置図（図9）に対し、どの機能要求（意図機能）が安全目標侵害するかを×で示す。

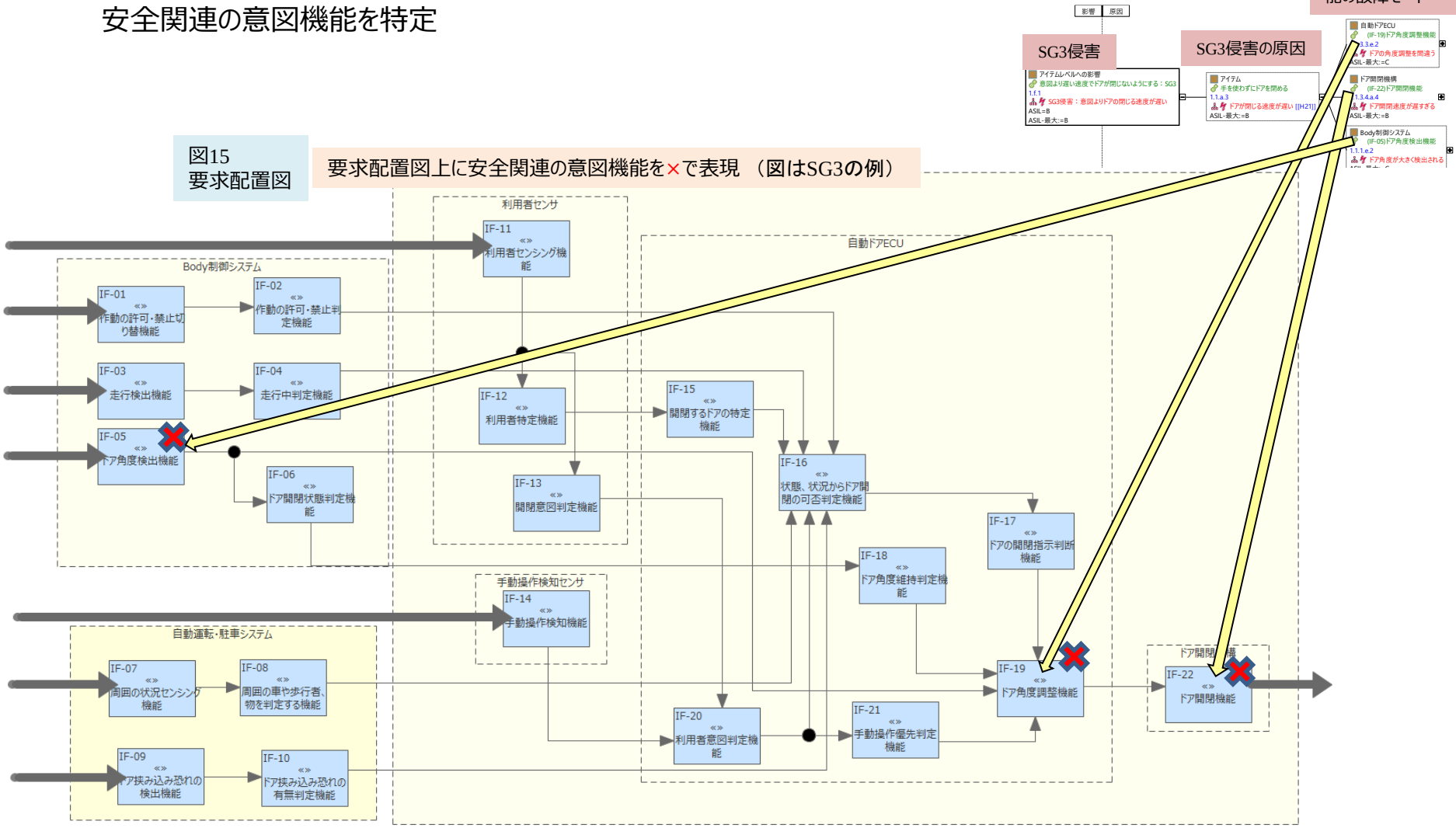
3.6.4.安全関連の意図機能の特定

- ✓ 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15
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）



4.今回のスタディでの失敗や、気づき、所感、課題など

3章では、前提条件で定義した内容をもとに手法連携のケーススタディを実施した結果を記述した。

スタディにおける失敗や、気づき、所感、課題などは、主に本章に記載している。

4.今回のスタディでの失敗や、気づき、所感、課題など

3.3.3.ユースケース分析に対する気づき、考察

機能安全における安全機構の作動は、ユースケースシナリオでは例外フローとして記述可能と言われている。

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

今回のスタディでは安全関連の意図機能の特定までを対象としたため、例外フローの深堀り、それとSCDLとの連携については紹介できていない。

SCDLを用いた安全関連の意図機能と安全機構の記述については、5.参考文献、WEBサイトに示したSCN-SGのWEBサイトから、SCDL仕様書を入手してそこに示された適用事例を参考にしていただきたい。

4.今回のスタディでの失敗や、気づき、所感、課題など

3.3.4.機能要求の導出に対する気づき、考察

- この項で導出した機能要求はアイテム定義で扱われるべき内容と考えるが、今回スタディしたプロセスはMagicGridを一部参考にしながら進めたこともあり、ISO26262で示されるものと異なり、PAA(preliminary architectural assumptions)における機能要求として定義してこなかった。
- MagicGridでは、システムの物理設計を行う際に考慮すべき要求を洗い出すために、対象システムの論理アーキテクチャを対象にしているが、今回のスタディでは、3.4節のハザード分析＆リスクアセスメント以降では物理アーキテクチャを念頭に置いた取り組みとしていることで、物理構造に対する機能要求導出結果では無いこの項の結果はあまり利用されなかった。
- ISO26262は、自動車の開発が派生開発を中心に実施されることを念頭に置いていることに対し、MagicGridでは、まずは物理アーキテクチャにとらわれることなく分析を進めるアプローチとなっていることが大きな違いで、その違いを考慮してMagicGridを参考にすべきだったと反省している。

4.今回のスタディでの失敗や、気づき、所感、課題など

3.3.5.有効性の尺度（MoE）に対する気づき、考察

3.3.4.機能要求の導出の結果があまり活用されなかったので、こちらもあまり活用されなかった。

本来であれば3.3.4.項の機能要求を更に詳細設計をした際に利用すべきものだと思われるが、今回は、 3.3.4.項の機能要求を更に詳細設計するのではなく、物理構成（エレメント）に割り付ける機能要求として再定義したため、MoEを用いた評価を実施する機会が無かった。

また、3.5.2.項で、性能の尺度（MoP）として更に細かい粒度で尺度を導出しており、今回の活動をさらに続けた場合は、性能の尺度（MoP）を用いて評価することになると考える。

4.今回のスタディでの失敗や、気づき、所感、課題など

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が、今回は詳述化を実施しなかったので、評価できなかった。
（MagicGridで言うところの解決領域を実施していないため）

4.今回のスタディでの失敗や、気づき、所感、課題など

3.5.3.ユーザーニーズのトレーサビリティに対する気づき、考察

今回のスタディでは、ユーザーニーズをTopにしてトレーサビリティを確認したが、機能安全活動では安全目標をTopにトレーサビリティを確認することになっている。

意図機能に関しても、3.1節の商品開発のきっかけに示したそもそもの課題に対するゴール（機能目標のようなもの）が解決できたのか？と言ったことをバリデートできるような活動にすべきではないかと考える。

4.今回のスタディでの失敗や、気づき、所感、課題など

3.4.1.ハザード分析

3.6.3.設計FMEA　STEP4：故障分析に対する気づき、考察（気づき・課題）

ハザード分析の結果とDFMEAで抽出した故障モードのつながりを明確化しようとしたが、双方の結果に抜け漏れが有り、うまくつなげられずに苦労した。

原因として考えられるのが、ハザード分析にはSTPAのガイドワードを用い、DFMEAにはHAZOPのガイドワードを用いたことが原因とだと思われる。

双方のガイドワードによる分析に差異が出ないように、HAZOPガイドワードのどれがSTPAのガイドワードに属するのかと言ったマッピングを事前にしておき、ガイドワード違いによる分析結果の差を防止する必要があると感じた。

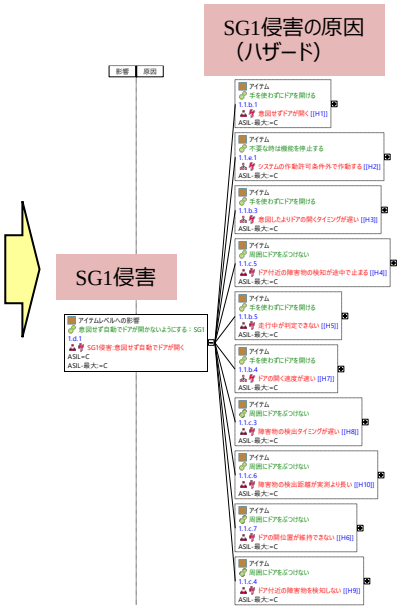
4.今回のスタディでの失敗や、気づき、所感、課題など

3.6. 設計FMEAと安全関連の意図機能の特定の気づき、考察

- ✓ 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だと考える。
- ✓ 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になると考える。
- ✓ 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	

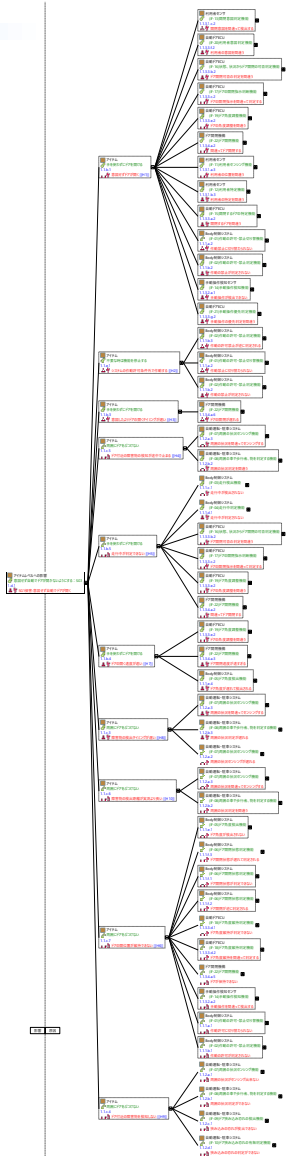


4.今回のスタディでの失敗や、気づき、所感、課題など

SG侵害に至る原因系（SG1）

表11

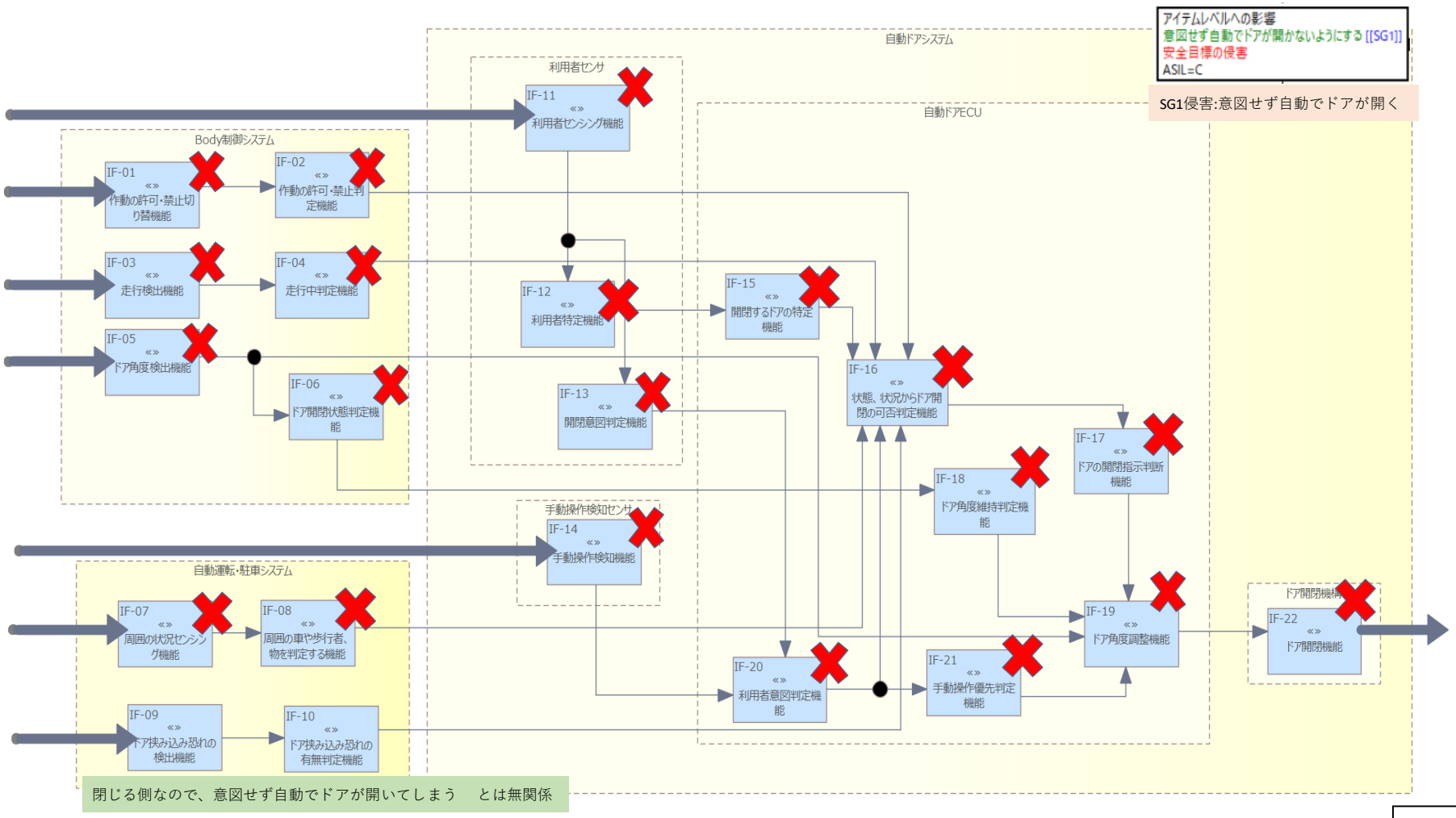
安全目標ID	安全目標	ハザードID	ハザード	最高ASIL
SG1	意図せず自動でドアが開かないようにする。	H1	意図せずドアが開く ※「人・車の進路にドアが開いている」を包含する	ASIL C
		H2	システムの作動許可条件外で作動する	
		H3	意図したよりドアの開くタイミングが遅い	
		H4	ドア付近の障害物の検知が途中で止まる	
		H5	走行中が判定できない	
		H6	ドアの開位置が維持できない	
		H7	ドアの開く速度が速い	
		H8	障害物の検出タイミングが遅い	
		H9	ドア付近の障害物を検知しない	
		H10	障害物の検出距離が実測より長い	
		H11	意図したのにドアが開かない	
SG2	意図せずドアが開かないことがないようにする。	H15	走行中と誤判定する	ASIL B
		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	



4.今回のスタディでの失敗や、気づき、所感、課題など

SG侵害に至る原因系（SG1）

SG2～SG7については、7章付録に添付



5.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。

6.参考文献、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

7.付録

SG2～SG7の安全目標について、各安全目標侵害に至る故障モードを洗い出し、安全関連の意図機能を特定した結果を×で示す。

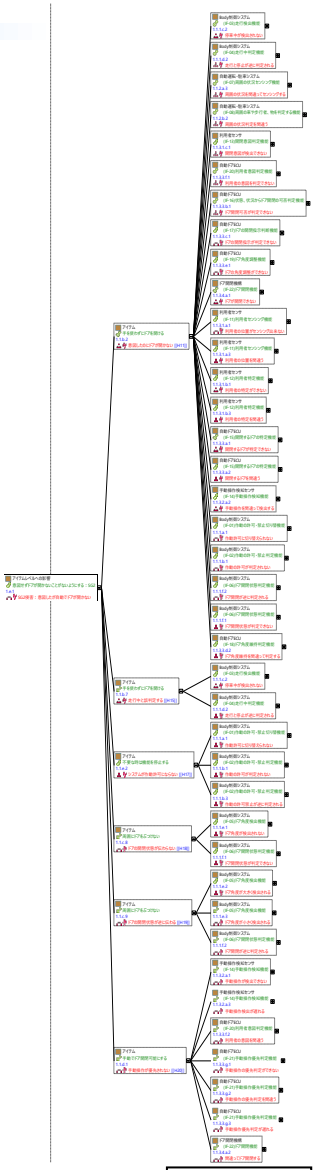
（一部DFMEAの結果から抽出された結果に対し、無関係と思われるものについては、修正を行っている）

7.付録

SG侵害に至る原因系（SG2）

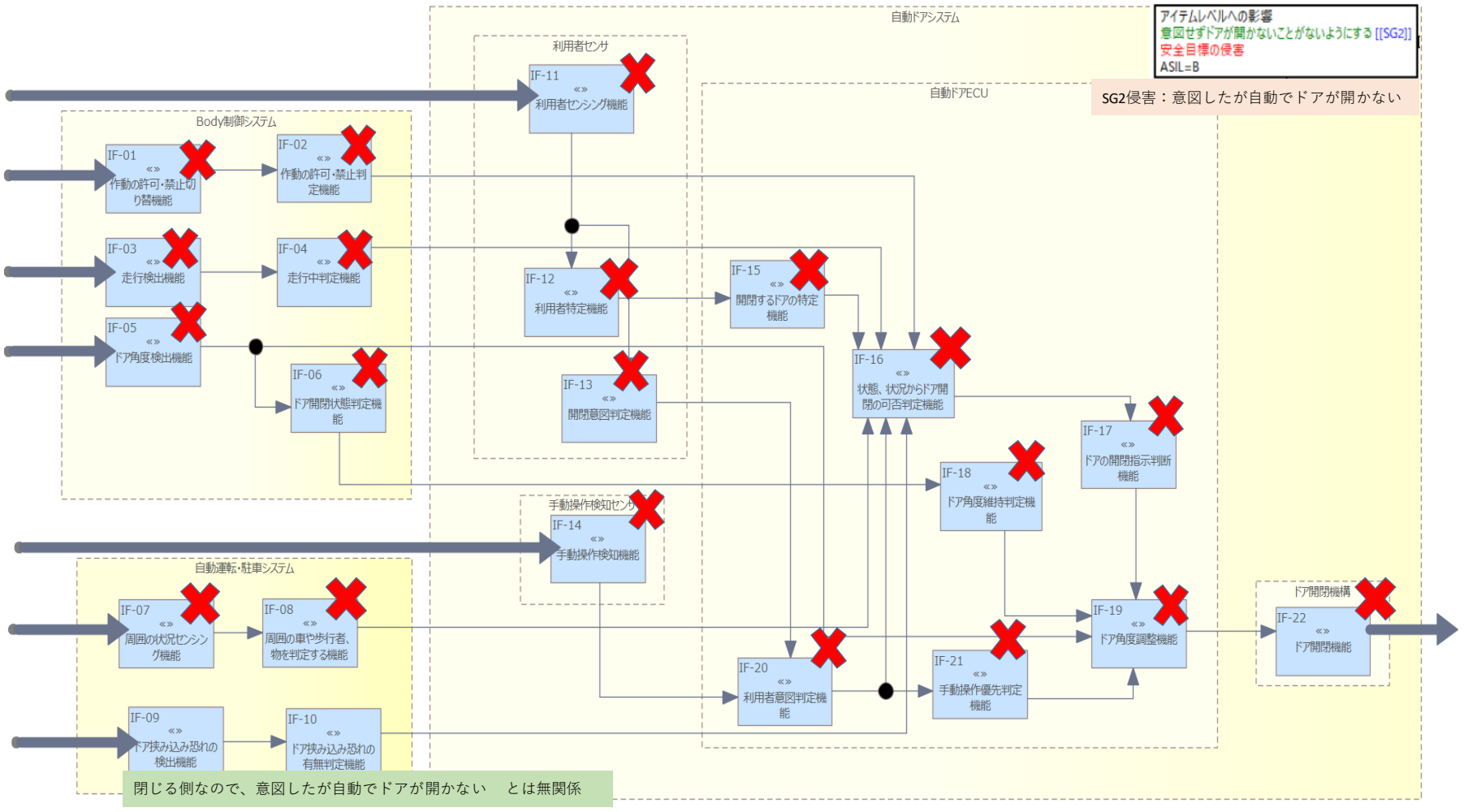
表11

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	



7.付録

SG侵害に至る原因系（SG2）

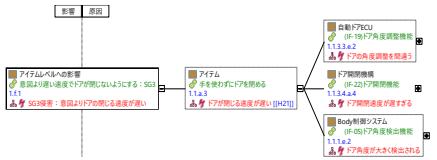


7.付録

SG侵害に至る原因系（SG3）

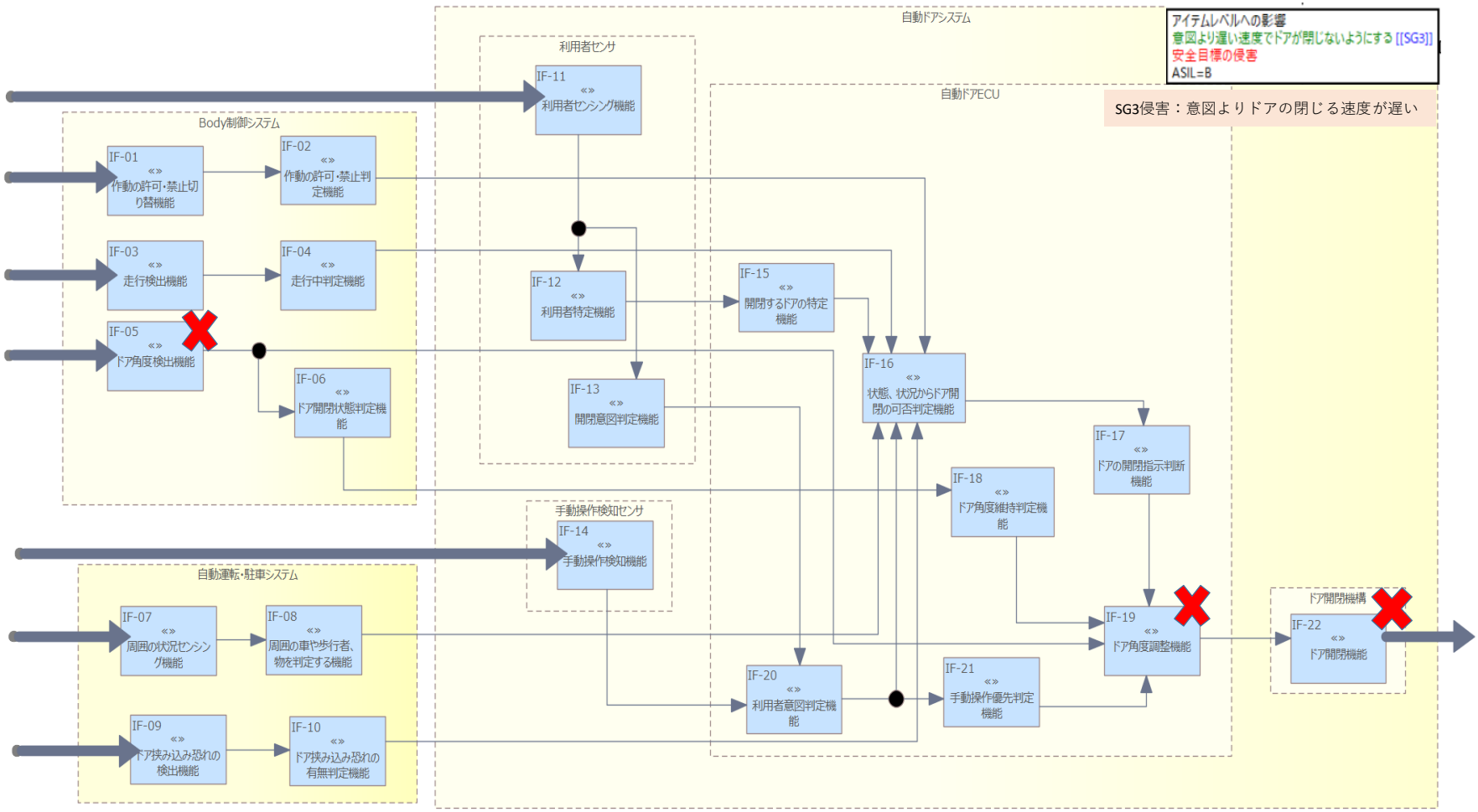
表11

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	



7.付録

SG侵害に至る原因系（SG3）

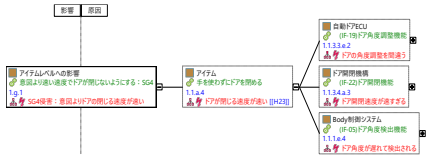


7.付録

SG侵害に至る原因系（SG4）

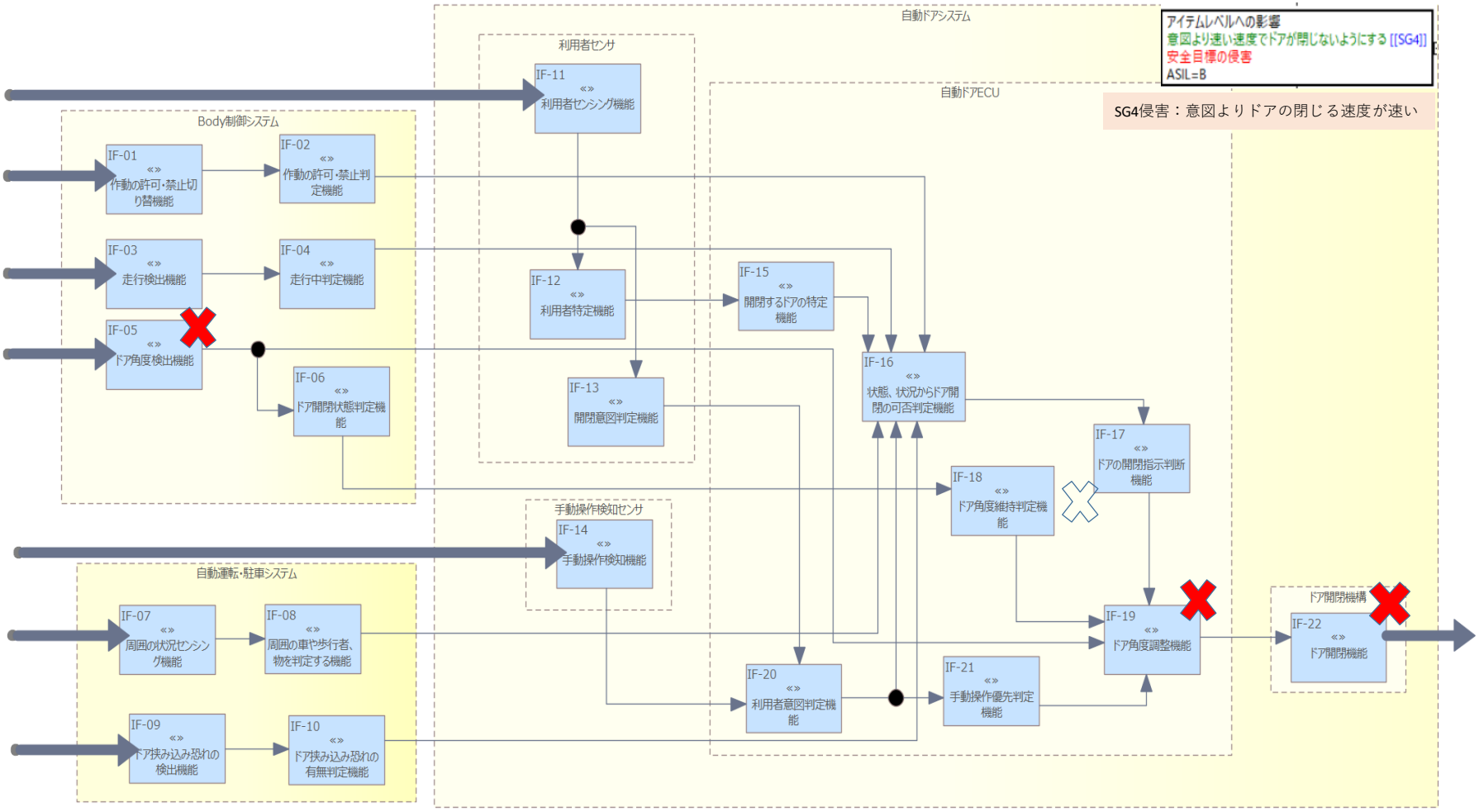
表11

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	



7.付録

SG侵害に至る原因系（SG4）

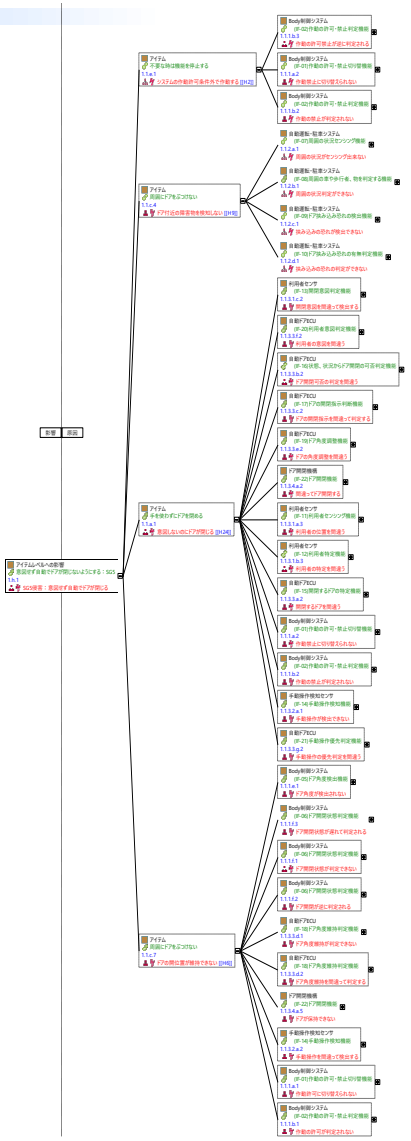


7.付録

SG侵害に至る原因系（SG5）

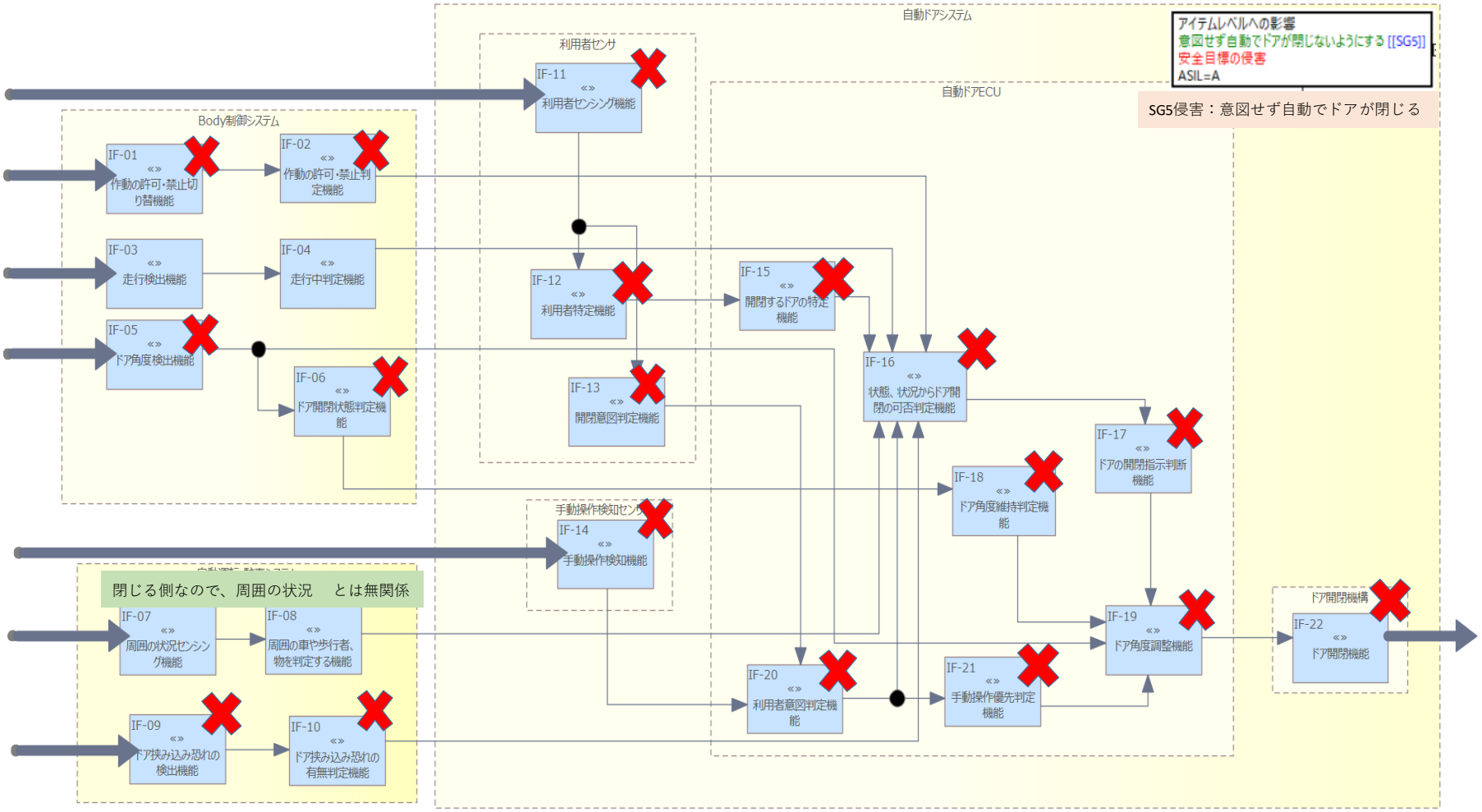
表11

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	
		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	ASIL A
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	



7.付録

SG侵害に至る原因系（SG5）

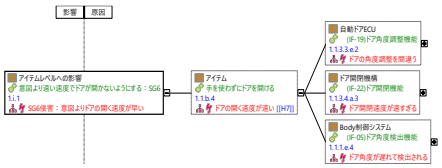


7.付録

SG侵害に至る原因系（SG6）

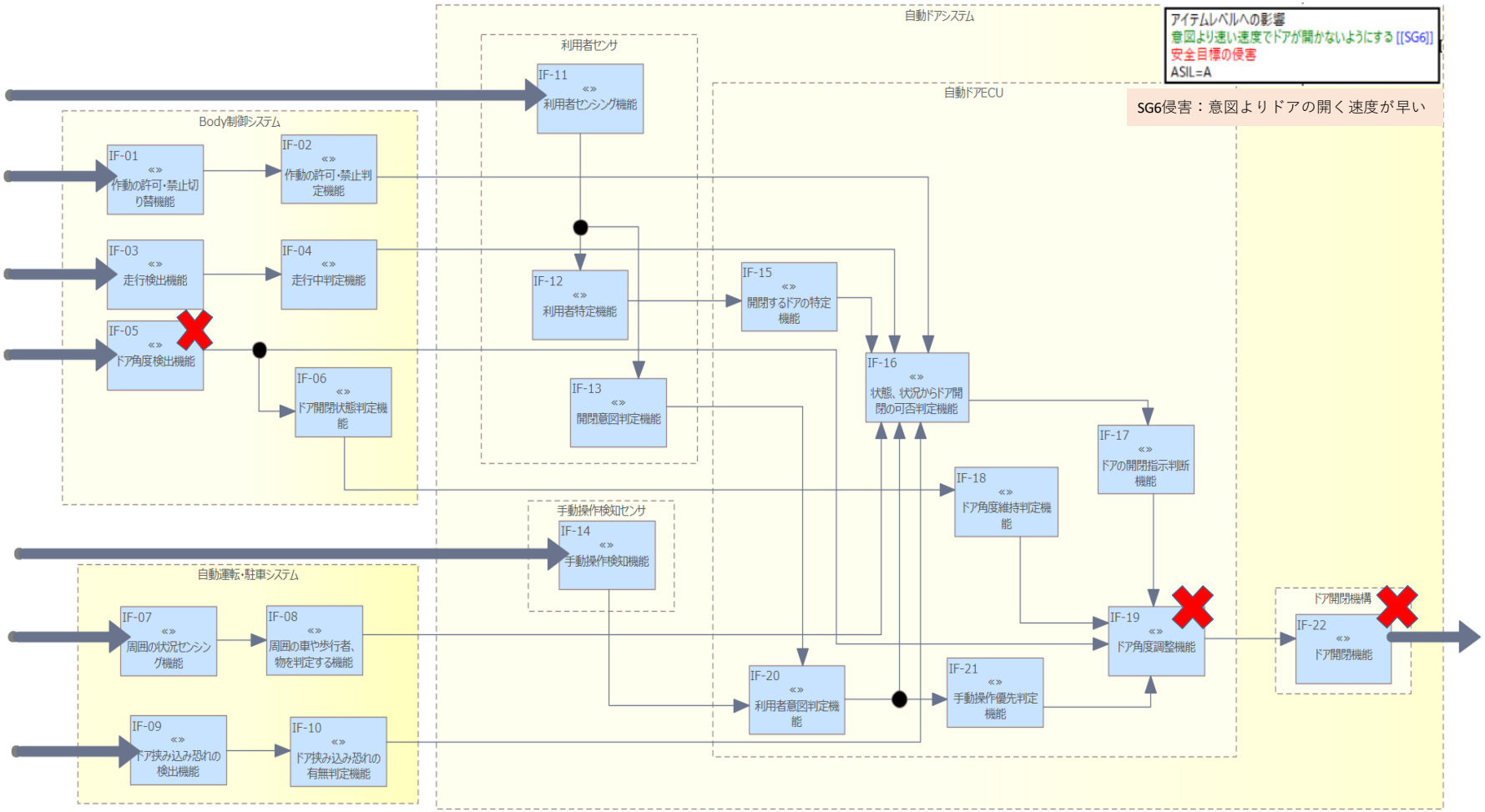
表11

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	



7.付録

SG侵害に至る原因系（SG6）

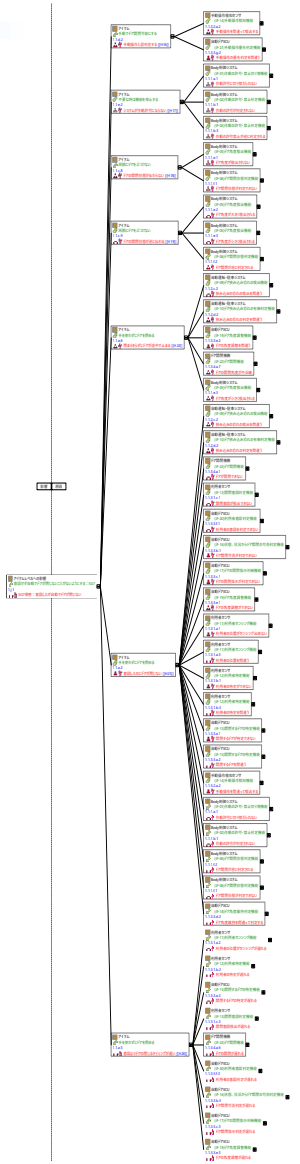


7.付録

SG侵害に至る原因系（SG7）

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	



7.付録

SG侵害に至る原因系（SG7）