SCDL ユースケース

～ 機能安全設計への適用 ～

SCDL ：Safety Concept Description Language

For Safety Evolution

2016年 10月 19日

株式会社 アドヴィックス
技術統括部　河野 文昭

自己紹介

- 氏名：　　河野 文昭　〔 技術士（総合技術監理・情報工学）〕
- 会社-所属：　株式会社アドヴィックス　技術統括部
- 職務：
  - 2009年より自動車制御ブレーキの機能安全開発業務に携わり、開発プロセス及び開発環境の整備、さらには機能安全監査及びアセスメントに尽力中。

- 社外活動：
  - ISO/IEC JTC1/SC7 WG10 アドバイザ
  - 独立行政法人 情報処理推進機構 ソフトウェア高信頼化センター(IPA/SEC)連携委員
  - 公益社団法人 自動車技術会 情報セキュリティ分科会委員
  - 一般社団法人 JASPAR 機能安全WG 副主査
  - 一般財団法人 日本自動車研究所 ISO 26262 運営委員会幹事
  - クリティカルソフトウェアワークショップ(WOCS^2)プログラム委員
  - SCN-SG ステアリングコミッティ委員
  - 日本SPICEネットワーク代表

はじめに

- 本講演でお伝えしたいこと
  - ISO 26262：2011の安全活動においてKEYとなるのは「要求」「アーキテクチャ」「分析」である
  - SCDLは、「要求」を「アーキテクチャ」に配置したアーキテクチャ視点の安全設計をビジュアルに表現できるため、「分析」にも有用である
  - SCDLは、製品開発に携わる設計者や検証者だけでなく、機能安全アセスメント実施者にとっても有益な表記法といえる

注）本講演の記載例に基づく如何なる損害等の責任も負えません

アジェンダ

- 会社紹介
- 安全論証
  - ISO 26262の肝は安全論証
  - 安全コンセプトの段階的詳細化
  - 機能安全設計階層モデル
  - SCDLによる安全設計アプローチ
- ユースケース
- まとめ

SCN：Safety Concept Notation

会社紹介

本社：愛知県刈谷市

Brake Booster

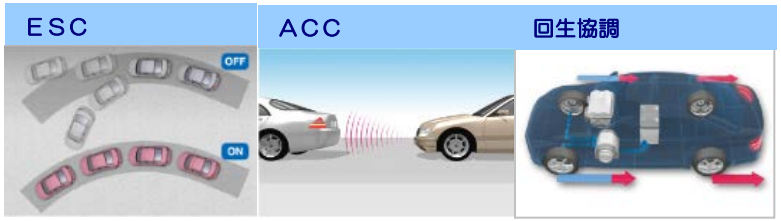
Master Cylinder

ESC Modulator

Pad

Parking Brake

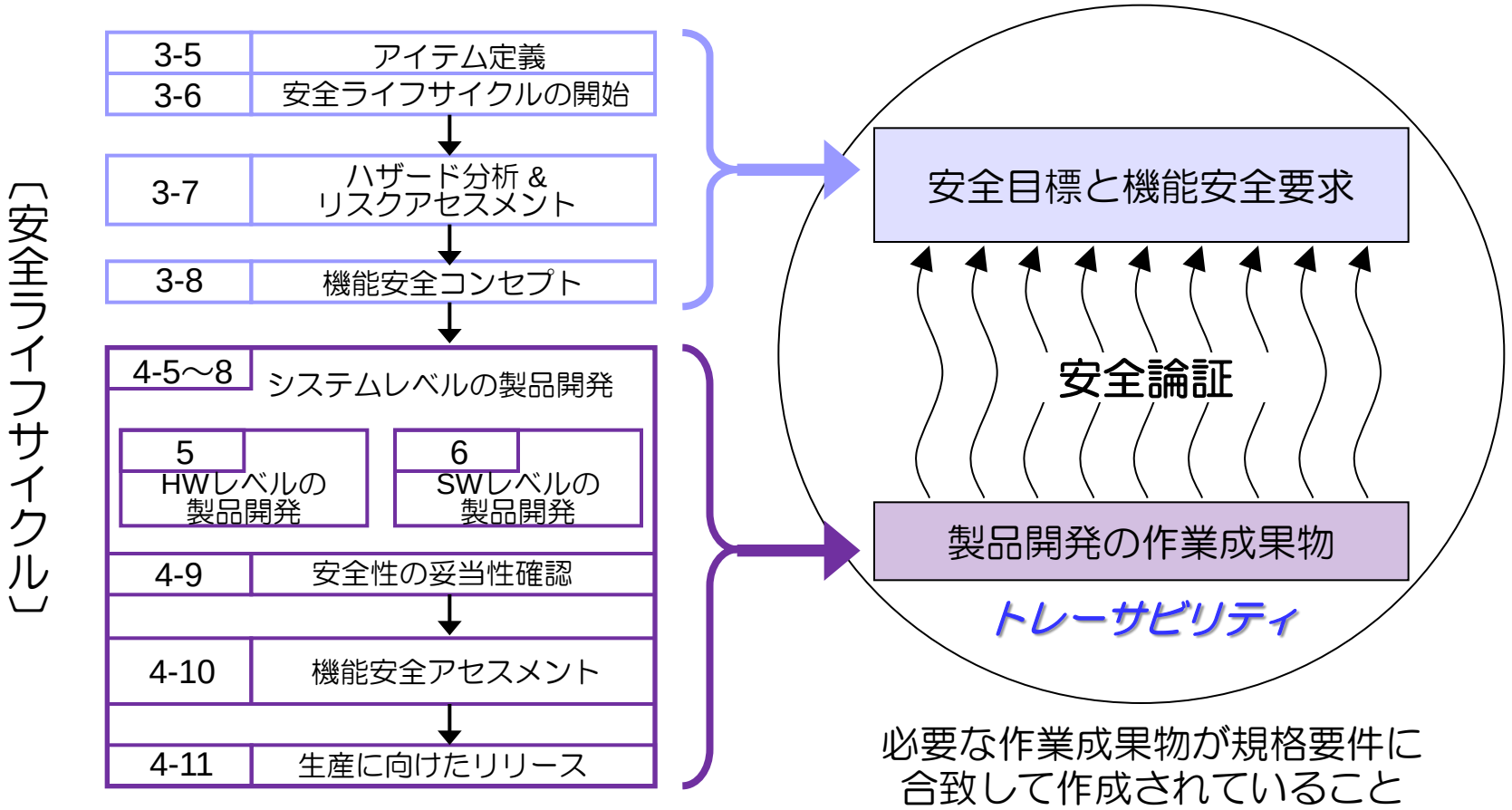
Disc Brake



【社名】	株式会社アドヴィックス
【設立】	2001年 7月 3日
【事業内容】	自動車用ﾌﾞﾚｰｷｼｽﾃﾑ 及び ｼｽﾃﾑを 構成する部品の開発・生産・販売
【資本金】	70.4 億円（2016年3月31日現在）
【売上高】	5,512 億円（2015年度 連結）
【従業員数】	7,420 名（2016年3月31日現在 連結）
【主要品目】	ESC、ABS、ﾌﾞﾚｰｷﾌﾞｰｽﾀ、ﾏｽﾀｰｼﾘﾝﾀﾞ ﾃﾞｨｽｸﾌﾞﾚｰｷ、ﾄﾞﾗﾑﾌﾞﾚｰｷ 電動ﾊﾟｰｷﾝｸﾞﾌﾞﾚｰｷ、その他関連部品

ISO 26262の肝は安全論証

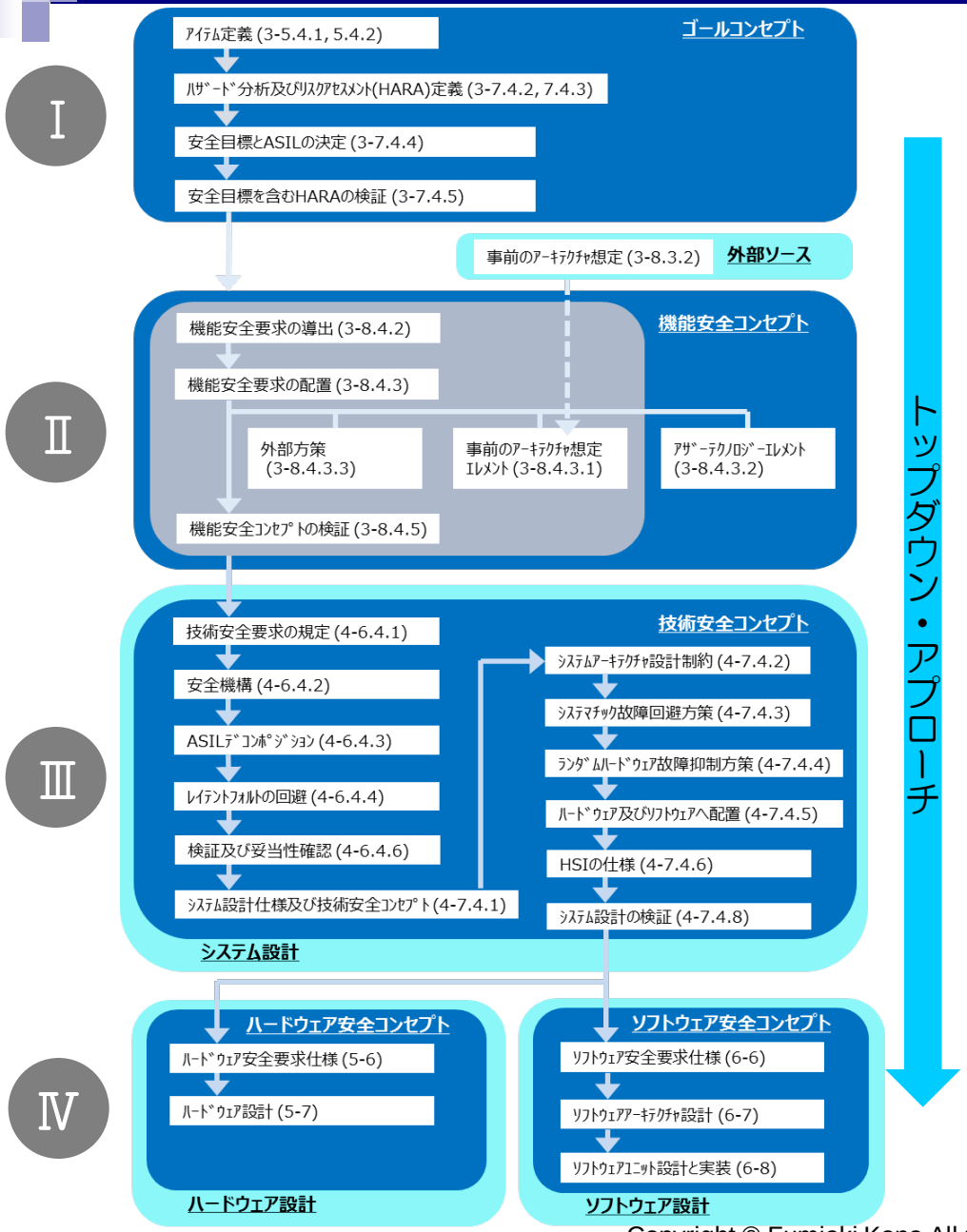
- Part 10
  - 5.3.1 セーフティケース



出典）ISO 26262-10：2011 図6

安全論証は、必要かつ適切な作業成果物を積み上げる必要がある

安全コンセプトの段階的詳細化



I. ゴールコンセプト*1

II. 機能安全コンセプト

III. 技術安全コンセプト

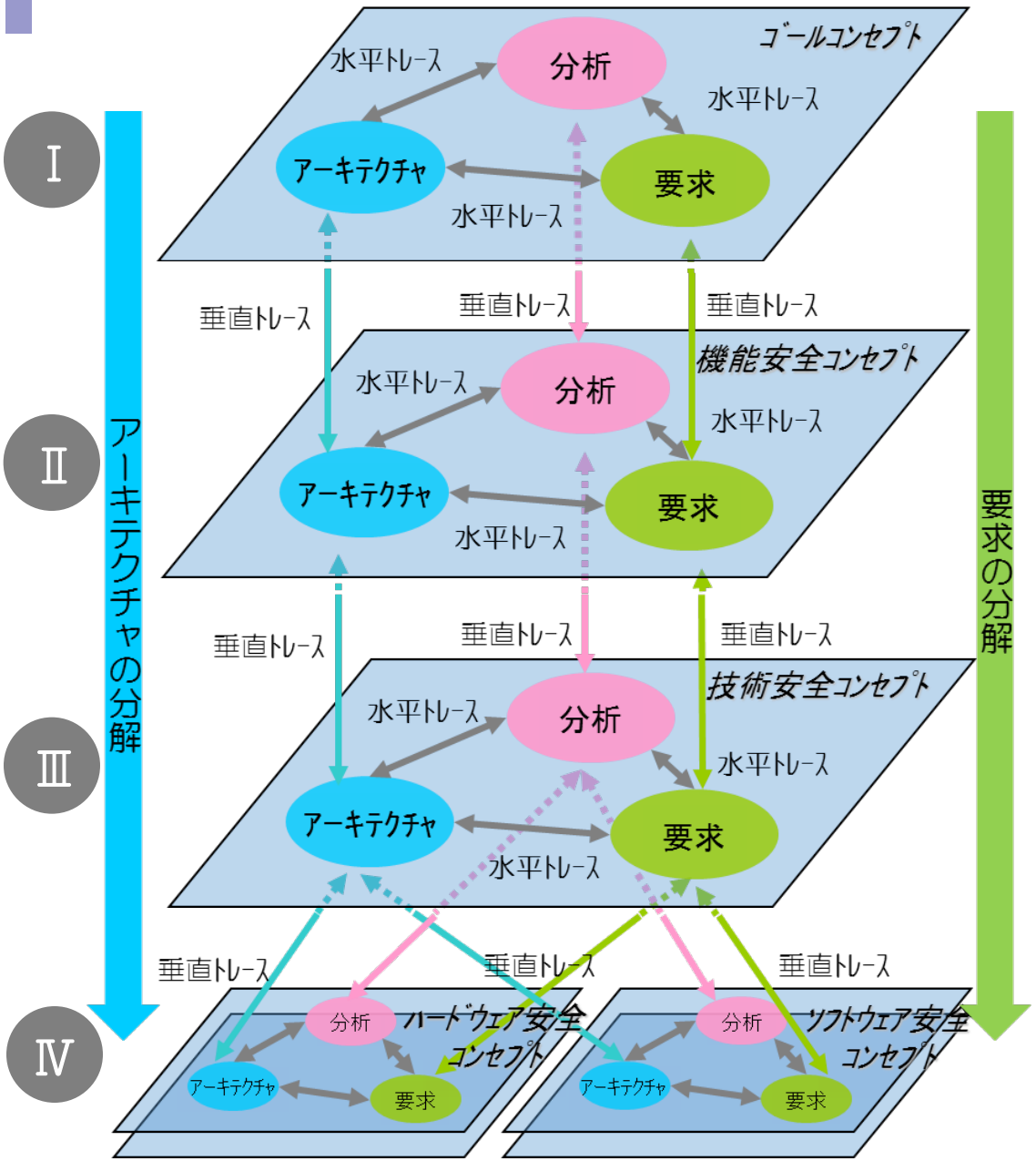
IV. ハードウェア安全コンセプト*1
ソフトウェア安全コンセプト*1

Ⅰ～Ⅳ全階層の安全アーキテクチャを描き、段階的に詳細化される各階層の要求とアーキテクチャ構成要素の関係を明確に表現することで、安全設計の論証に役立てる。

Safety Concept Description Language

＊1：
ISO 26262:2011に定義されている用語ではなく、本講演における説明のための名称

安全設計階層モデル



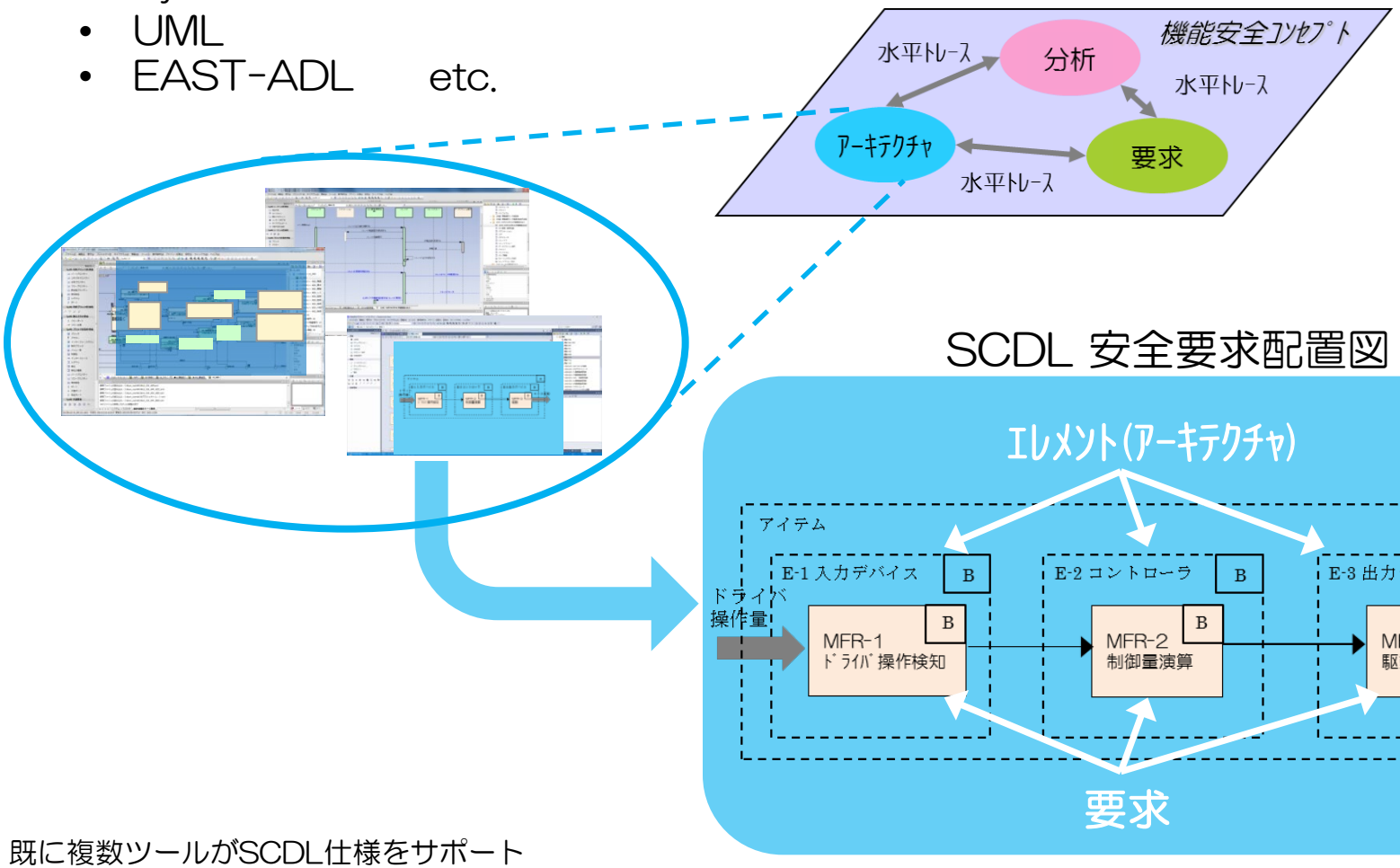
- ISO 26262のプロセスで特に重要となるのが、
  「要求」
  「アーキテクチャ」
  「分析」
  の3軸である。
- 3つの軸を相互に関連させながらゴールコンセプト※1の安全目標を起点としたトップダウンアプローチで段階的に実装レベルにまで落とし込む。
- トップからボトムまでの三次元トレーサビリティと一貫性を確保する
- これにより、安全目標の確実な実装が可能となる。

＊1：
ISO 26262:2011に定義されている用語ではなく、安全設計階層モデルを説明するための名称

SCDLによる安全ｺﾝｾﾌﾟﾄの説明性向上

◇ 準形式記法でアーキテクチャを描く

- SCDL
- SysML
- UML
- EAST-ADL　　etc.

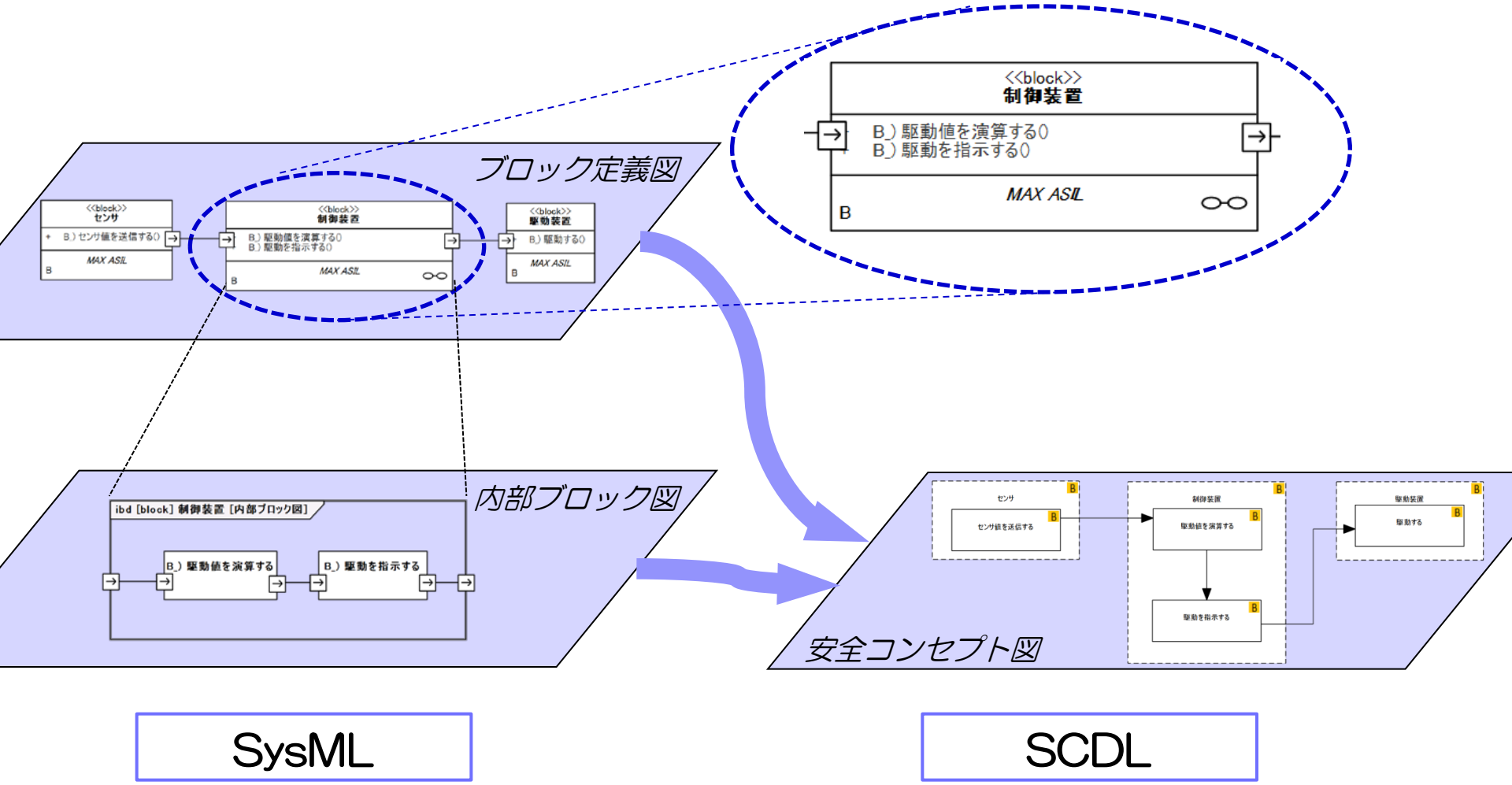


※ 既に複数ツールがSCDL仕様をサポート

要求の繋がりや処理の流れがﾋﾞｼﾞｭｱﾙに伝わる形で要求をｱｰｷﾃｸﾁｬへ配置

SysMLとSCDLの違い

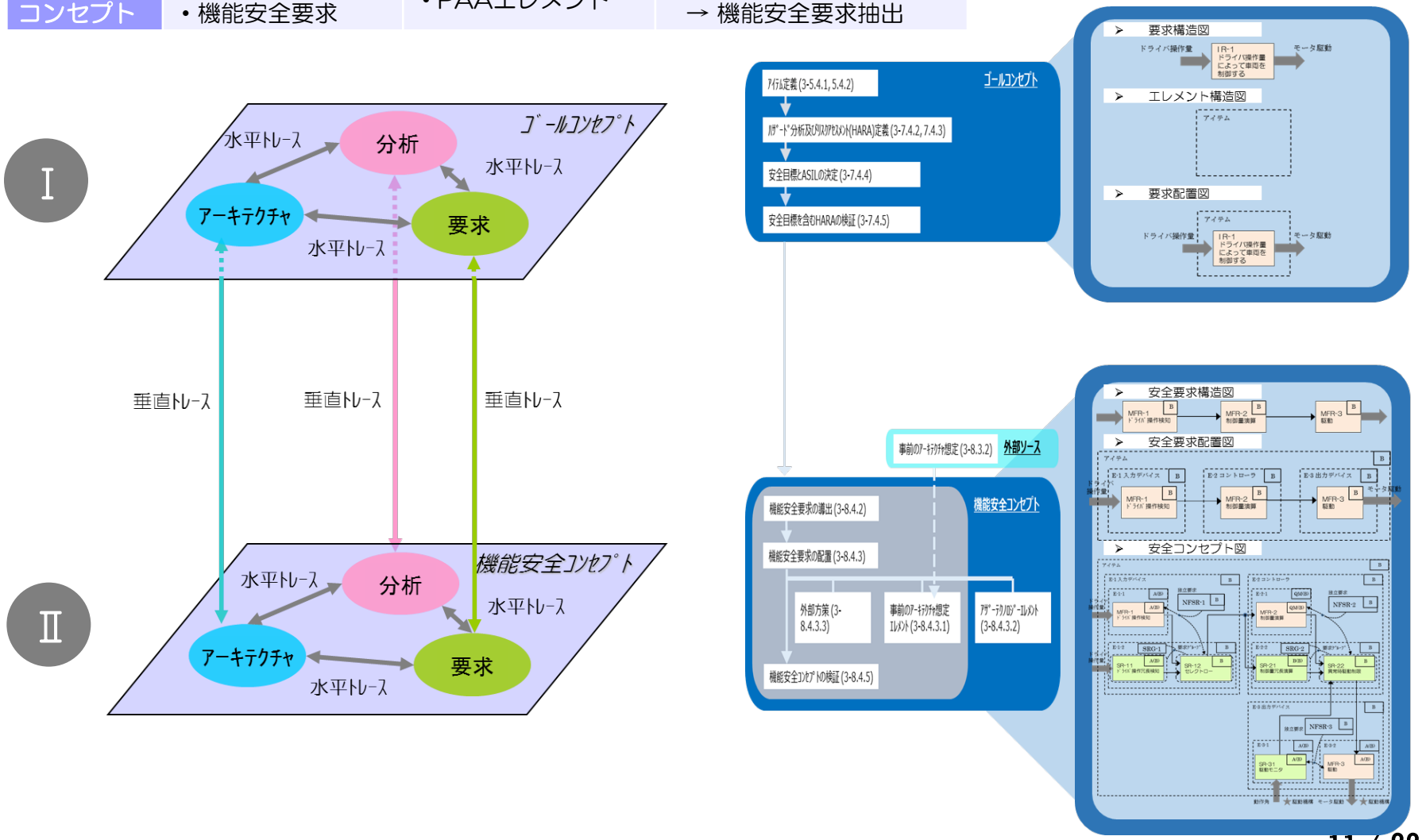
- SysMLの2階層表記が、SCDLなら1階層表記となる



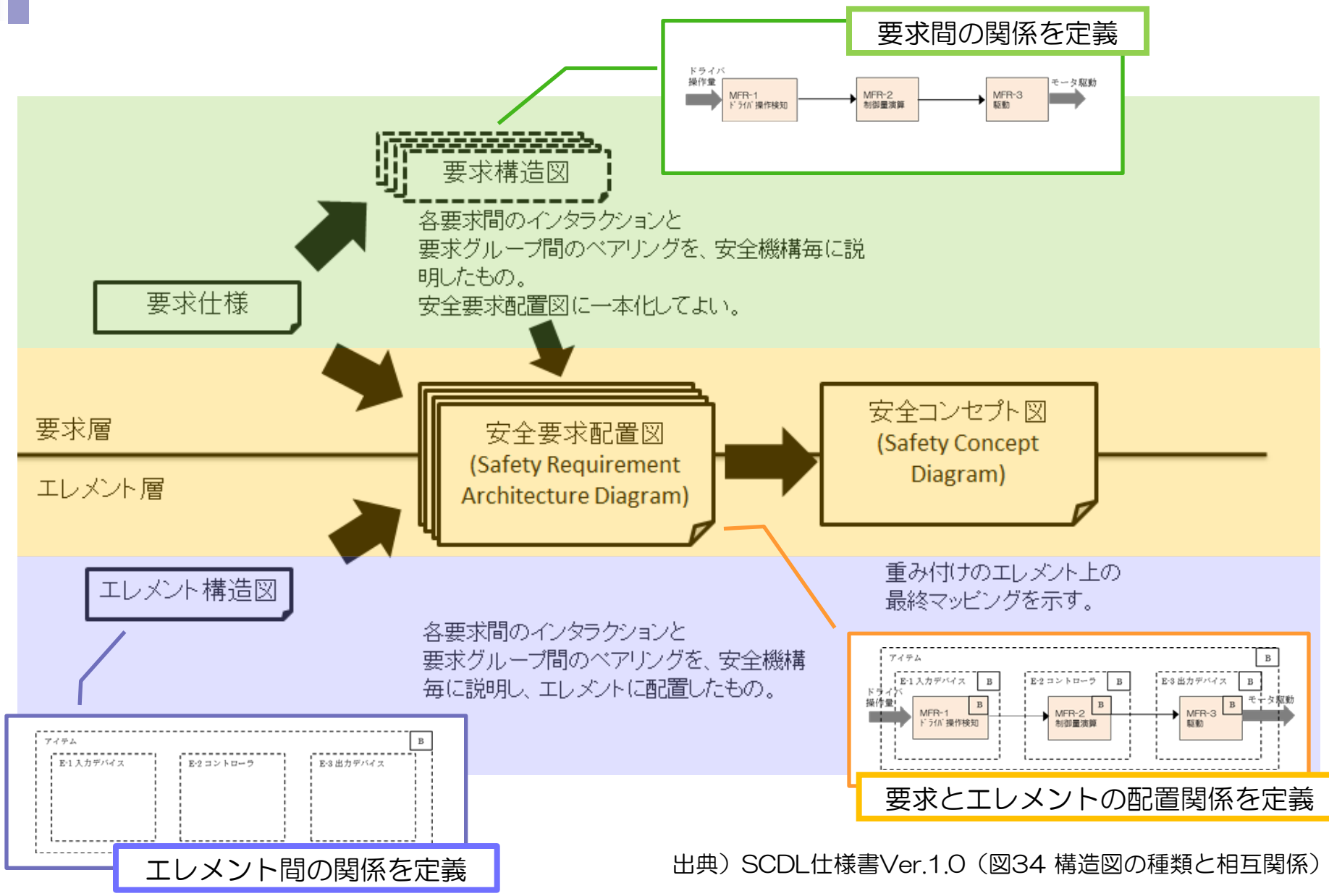
ISO 26262へのSCN適用イメージ

階層	要求	アーキテクチャ	分析
ゴール コンセプト	• アイテムへの要求 • 安全目標	• アイテム	• ハザード分析 → 安全目標導出
機能安全 コンセプト	• 意図した機能要求 • 機能安全要求	• PAAエレメント	• 安全分析＆従属故障分析 → 機能安全要求抽出

PAA：Preliminary Architecture Assumption



安全コンセプト図作成までの流れ



出典）SCDL仕様書Ver.1.0（図34 構造図の種類と相互関係）

ユースケース（1）

- アイテム定義
  - ドライバ操作量によって車両を制御するための車両制御システム

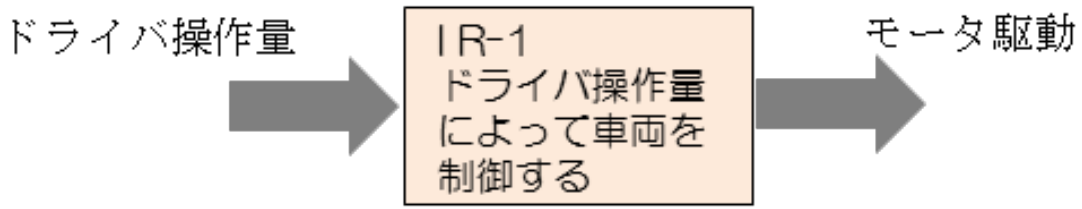


図 UC1．アイテムの要求図

- アイテム構成

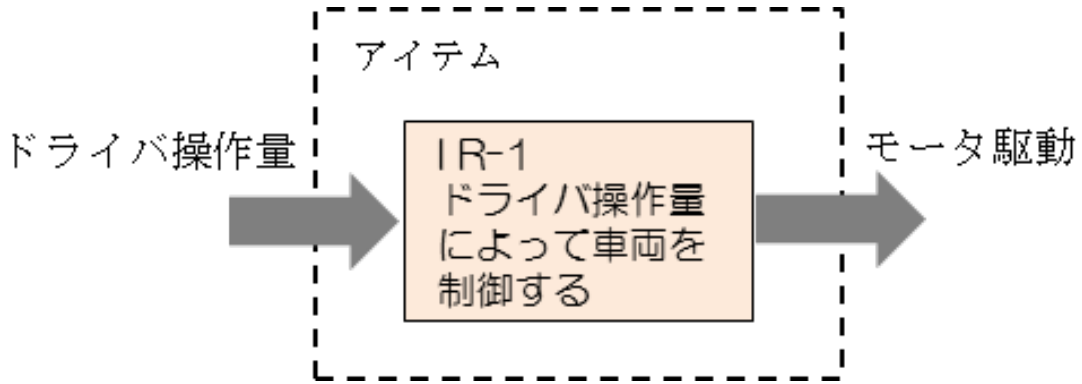


図 UC2．アイテムの要求配置図

ユースケース（2）

- ハザード分析 & リスクアセスメント

ハザード	車両が意図せず大きく偏向する
安全目標	車両が意図せず大きく偏向するような過大な出力を発生させない
安全状態	車両の意図しない偏向が、3deg/s以下
時間的制約	安全状態に500ms以内で移行すること
ASIL	B

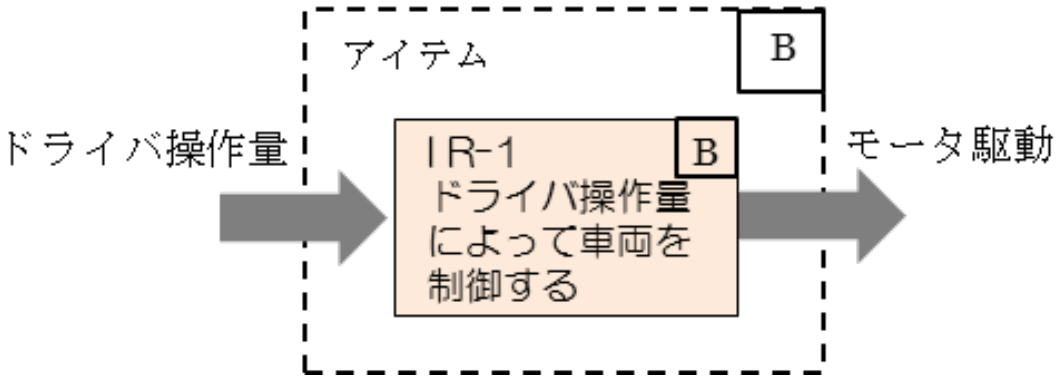


図 UC3．アイテムの安全要求配置図（安全目標配置図）

ユースケース（3）

- 意図した機能要求（主機能）

ID	名称	意図した機能要求
MFR-1	ドライバ操作検知	ドライバの操作量を検知してコントローラへ送る
MFR-2	制御量演算	ドライバの操作量に従った制御量を演算し、演算値を出力デバイスへ送る
MFR-3	駆動	演算値に応じて駆動をおこなう

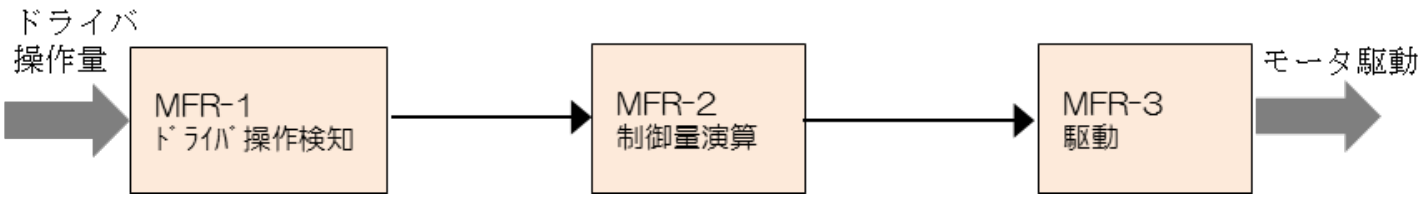


図 UC4．要求構造図

- 事前アーキテクチャ想定

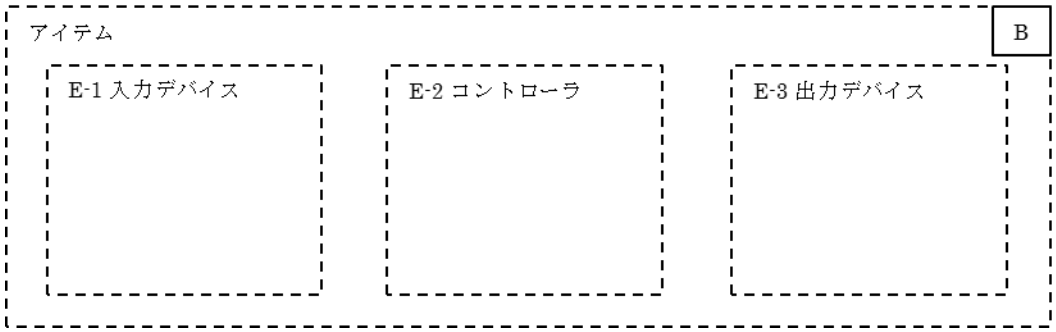


図 UC5．エレメント構造図

ユースケース（3）

- 機能安全コンセプトにおける安全分析

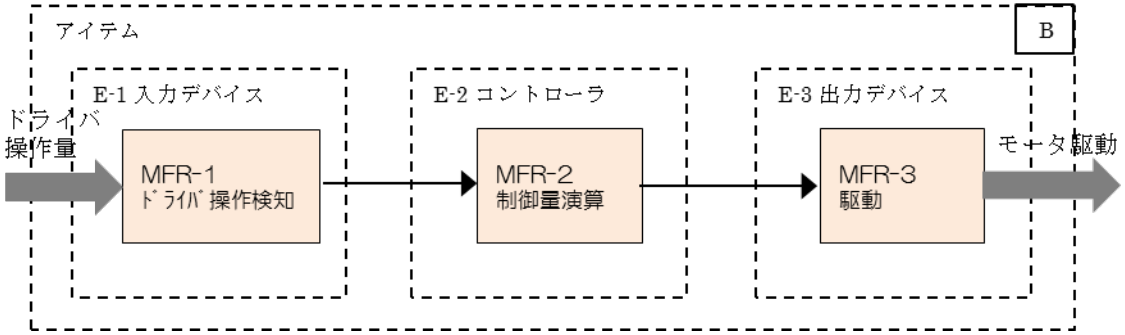


図 UC6. 要求配置図

ID	名称	安全目標侵害の可能性がある機能不全
MFR-1	ドライバ操作検知	過大側に入力値を誤る
MFR-2	制御量演算	過大側に演算値を誤る
MFR-3	駆動	過大な駆動をおこなう

ユースケース（4）

- 機能安全コンセプトにおける安全要求抽出

ID	名称	意図した機能要求に由来する安全要求
MFR-1	ドライバ操作検知	ドライバの操作量を(安全要求を侵害しないように正しく)検知してコントローラへ(安全要求を侵害しないように正しく)送る
MFR-2	制御量演算	ドライバの操作量に従った制御量を(安全要求を侵害しないように正しく)演算し、演算値を出力デバイスへ(安全要求を侵害しないように正しく)送る
MFR-3	駆動	演算値に応じて(安全要求を侵害しないように正しく)駆動をおこなう

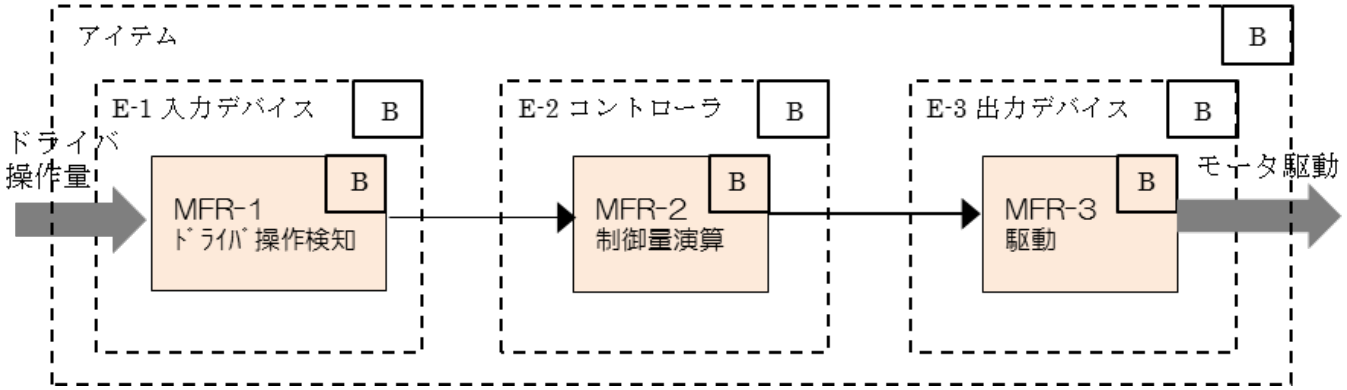


図 UC7．安全要求配置図

ユースケース（5）

- 機能安全コンセプトにおける安全要求（機能安全要求）のデコンポジションの結果、追加される安全要求や独立要求を示す

ID	名称	要求グループ	安全要求（安全目標侵害なきよう要求を満たす）
SR-11	ドライバ操作冗長検知	SRG-1	ドライバの操作量を検知する
SR-12	セレクトロー		2つのドライバ操作量を比較し、ロー側を選択する
SR-21	制御量冗長演算	SRG-2	ドライバの操作量に従った制御量を演算する
SR-22	異常時駆動制限		2つの演算値比較や駆動モニタSR-31からの異常通知時に駆動を制限する
SR-31	駆動モニタ	ー	駆動量を監視して、SR-22に異常を通知する

ID	独立要求
NFSR-1	MFR-1とSRG-1は従属故障を持たないこと
NFSR-2	MFR-2とSRG-2は従属故障を持たないこと
NFSR-3	MFR-3とSR-31は従属故障を持たないこと

ユースケース（6）

- 機能安全要求のデコンポジション
  - 前頁のSR-11, SR-12, NFSR-1からなる安全要求構造図とエレメント構造図から安全要求配置図を作成する

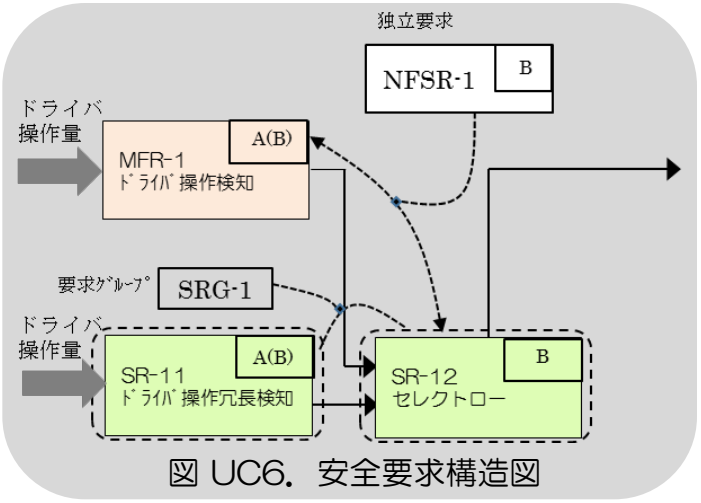


図 UC6. 安全要求構造図

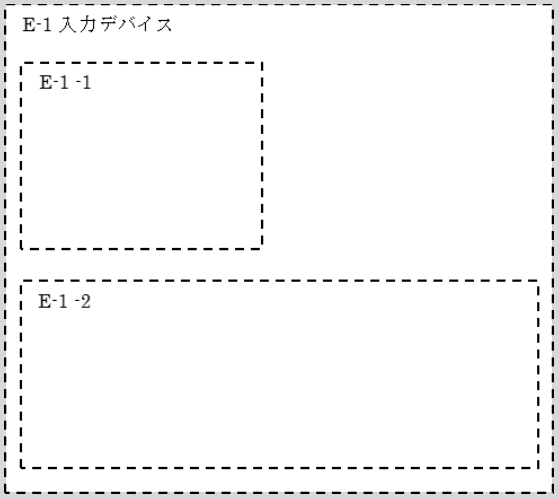


図 UC7. エレメント構造図

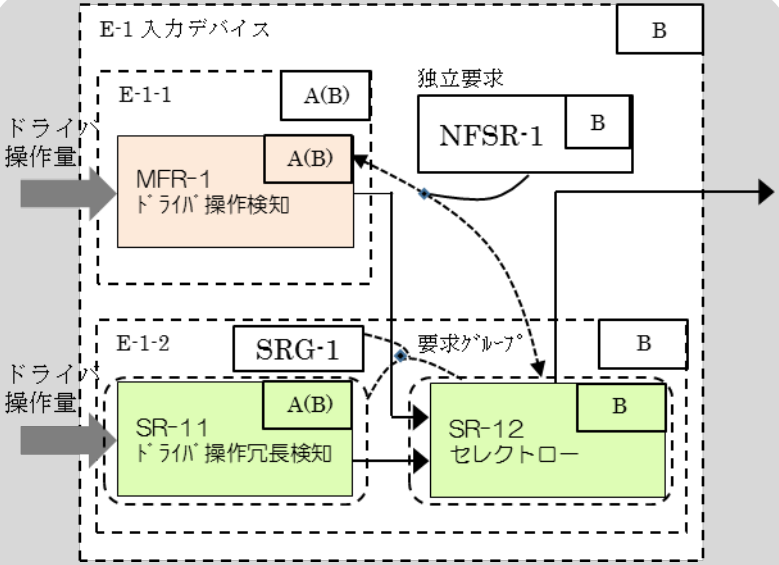


図 UC8. 安全要求配置図

ユースケース（7）

- 機能安全要求のデコンポジション
  - E-1エレメントのMFR-1だけでなく、E-2エレメントのMFR-2やE-3エレメントのMFR-3に対しても順次、安全要求配置図を作成して最終的に安全コンセプト図として統合する

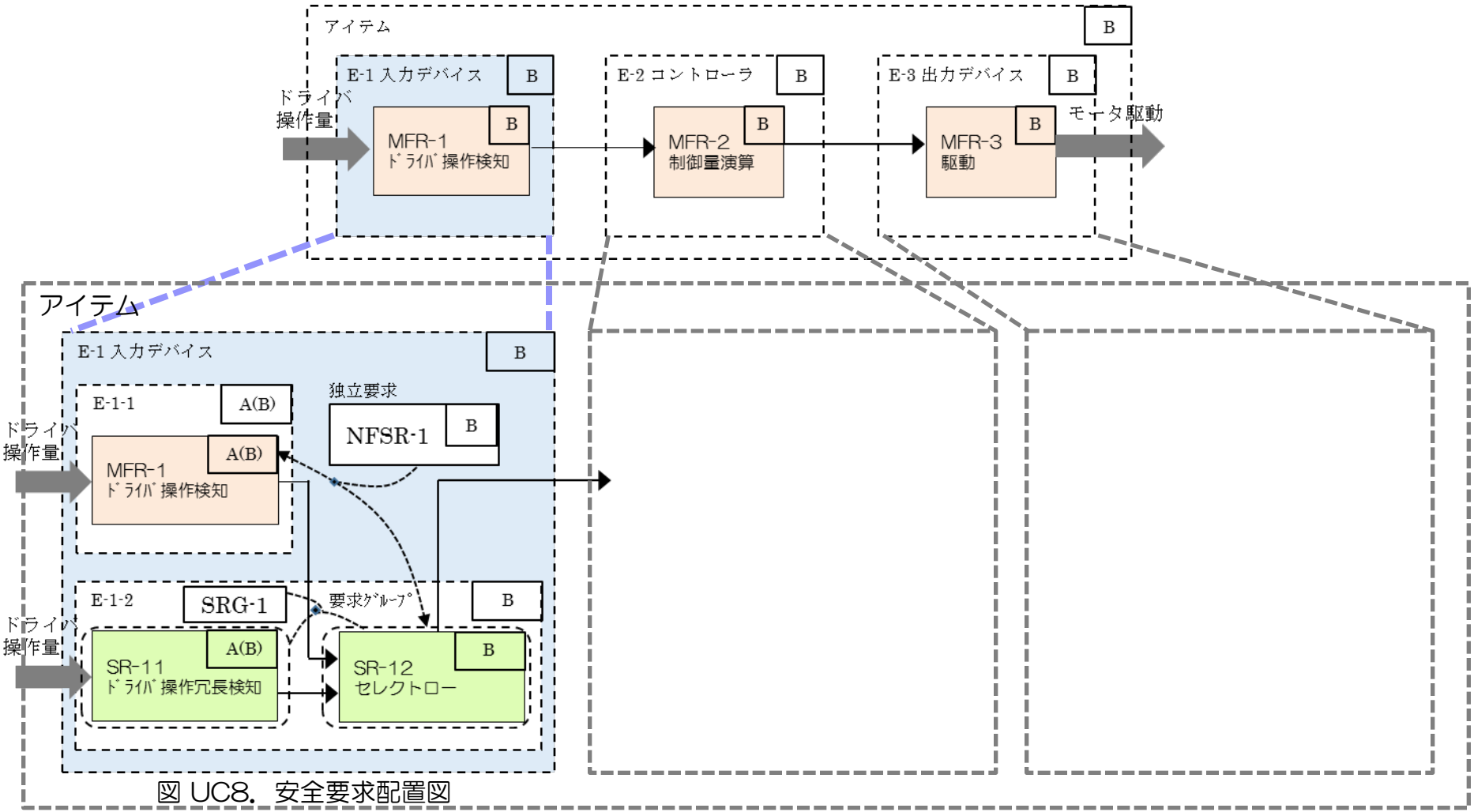


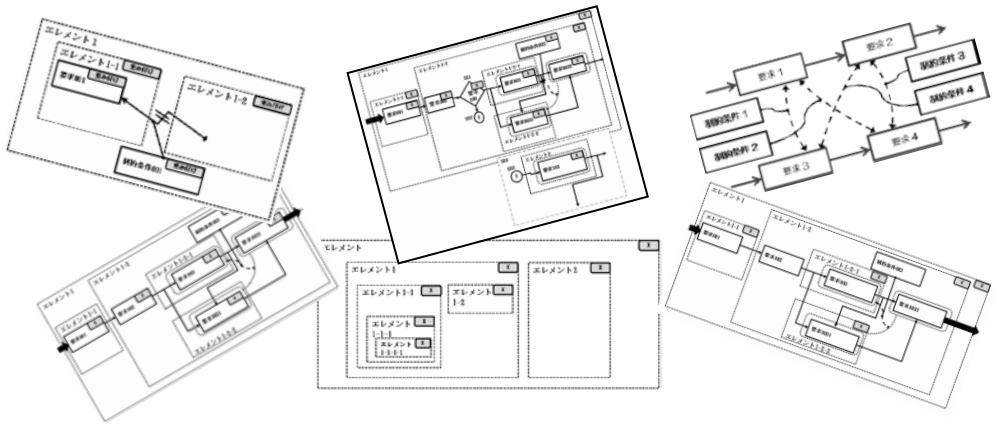
図 UC8. 安全要求配置図

図 UC9. 安全コンセプト図

まとめ

◇ 安全論証にSCDL表記法を活用すると･･･

- 要求とアーキテクチャのエレメントとの関係を明確に表現できる
- 独立要求をアーキテクチャ上に表現しやすい
- アーキテクチャのエレメントに配置された要求をビジュアルに捉えることができるため、設計レビューや安全分析がし易くなる
- アーキテクチャの階層をコンパクトにできる



ご清聴ありがとうございました