
SCN-OC 2020

『SCDL活用のための手法連携の試み』

2020/11/25

おおた開発効率化プロジェクト

小笠原 豊和

自己紹介

- 小笠原 豊和(おがさわら とよかず)
- おおた開発効率化プロジェクト 代表
- 2001年～2020年 大手自動車OEMに勤務
 - ー 自動運転／ADASの先行および量産開発
 - ー 自動運転／ADAS領域における社内機能安全対応推進リーダー
 - ー 新型車種の実験統括、プロジェクトマネジメント
- 2020年8月 おおた開発効率化プロジェクトを開業
 - ー 開発効率化支援、コンサルティング
 - ー エンジニア育成、講演、セミナー
 - ー 標準化活動(SCN-SG)
 - ー 他業界との交流活動(Field Robotics Japan, 日本うんこ学会)
 - ー 公式HP <https://www.ota-develop-efficiency-project.com/>
- 公益社団法人 自動車技術会 正会員
- SCN-SGコミッティメンバー(2015年～現在)

Agenda

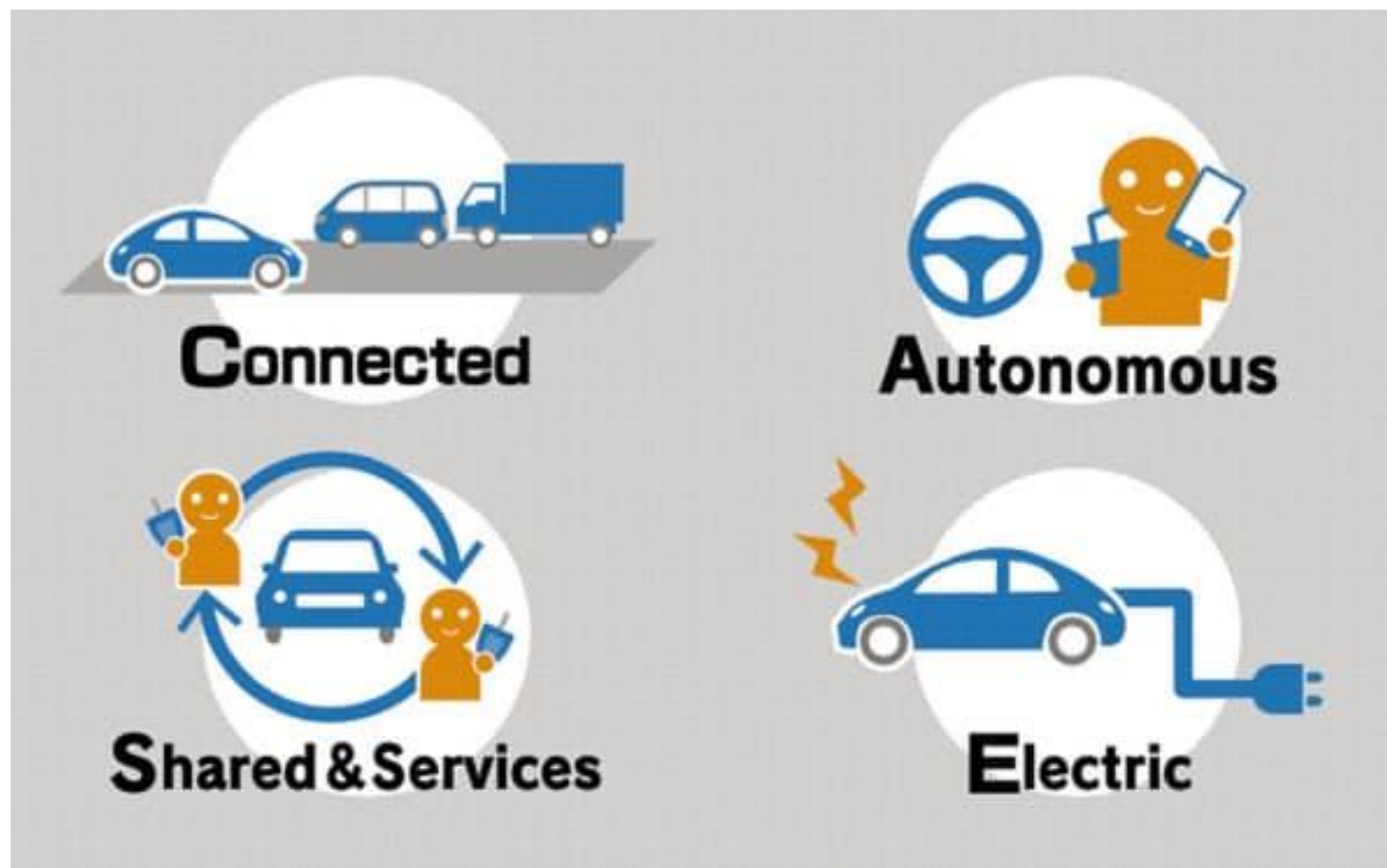
- 本発表の目的
- 自動車を取り巻く環境
- 自動車の安全に対する要求の変化
- 自動車の安全開発の現状
- 自動車の安全開発の課題
- 手法連携の狙いと課題
- 手法連携における課題の対策例
- SCDLと他開発手法との手法連携の検討
- まとめ

本発表の目的

- 自動車の安全開発（要求、アーキテクチャ、分析）を包括的に行う手法を検討し、開発の高効率化、高精度化を図る。
- 安全開発の現状と課題を明らかにする。
- 複数の安全開発手法の強みを生かした手法連携の考え方および課題について述べる。
- SCDLと他開発手法との手法連携の検討について述べる。

自動車を取り巻く環境

- 社会情勢の変化、ユーザーニーズの多様化に伴い、自動車の使われ方が大きく変化している。

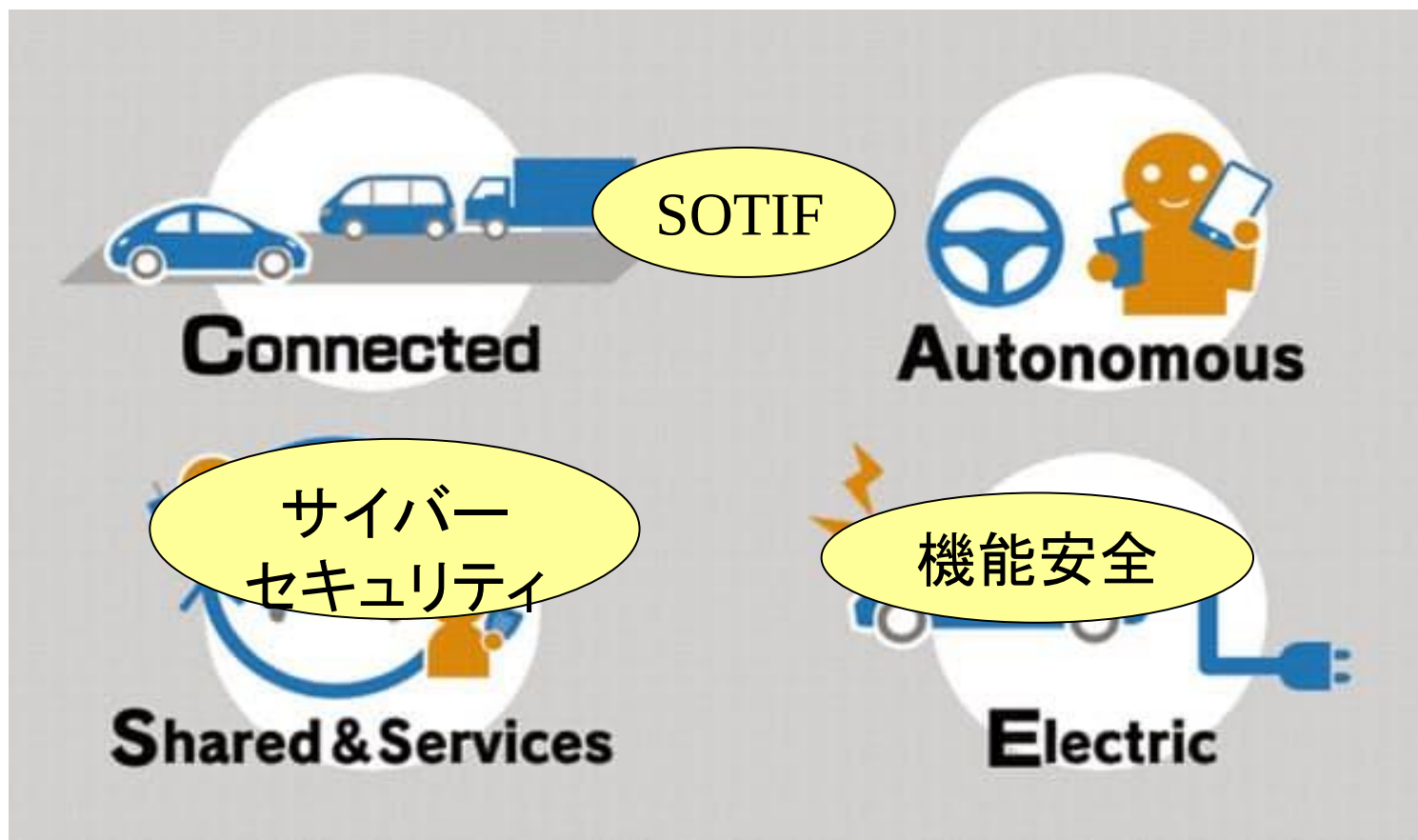


出典: 日本経済新聞Webサイト

<https://www.nikkei.com/article/DGXXKZO51931240X01C19A1EA2000/>

自動車の安全に対する要求の変化

- 自動車のユースケースの変化に伴い、担保すべき安全の要求、アーキ、分析の精度、開発効率の向上が求められている。



自動車の安全開発の現状

- 安全に対する要求の量、複雑度が増す中、それに対応した開発手法が多く提唱されている。

＜主な開発手法＞

- AIAG & VDA-FMEA
- DRBFM
- FMEDA
- HAZOP
- STAMP/STPA
- UML
- DFD
- East-ADL
- FTA
- SCDL
- SysML
- USDM

など

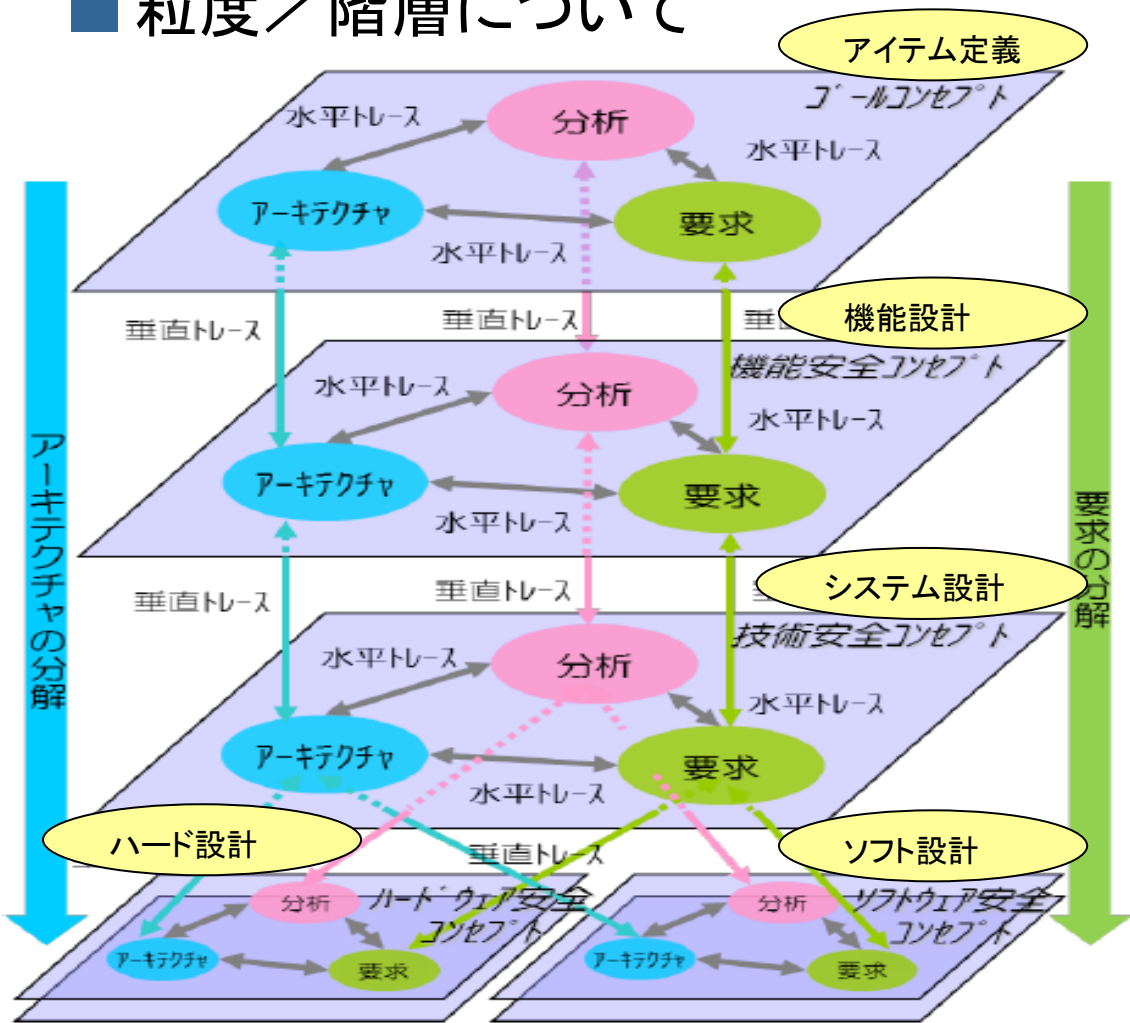
自動車の安全開発の課題

- 安全担保の手法こそ多様化されているが、手法選択、手法連携など、俯瞰した手法や統一指針が明確でない。
- ⇒ 開発者間の理解齟齬が生じ、安全担保の阻害要因となる。

活動・成果物	課題
要求	・ 粒度／階層が開発者間で共有されていない ・ (要求の) 目的が共有されていない ・ (要求に対する) 目標が共有されていない
アーキテクチャ	・ 粒度／階層が開発者間で共有されていない ・ (アーキテクチャという) 言葉の定義・解釈が共有されていない
分析	・ 目的／用途に合わせた分析手法の適用が必要 ・ 最も効果的な分析手法の適用手段が不明

自動車の安全開発の課題

■ 粒度／階層について



安全設計の活動(要求、アーキテクチャ、分析)において、階層毎における作業内容、成果物を明確にしなければならない。

- ※着眼点
- ・設計階層
 - ・活動の目的
 - ・活動の対象
 - ・活動の手段
 - ・検証の手段
 - ・階層毎に要求される成果物
 - ・次工程への引継ぎ
- など

自動車の安全開発の課題

■ 言葉の定義／解釈について

☆「構造」の解釈について

ー アーキテクチャ(architecture)

(情報システムの)設計方法、**設計思想**、およびその**設計思想に基づいて構築された**システムの構造などのこと。

ー ストラクチャ(structure)

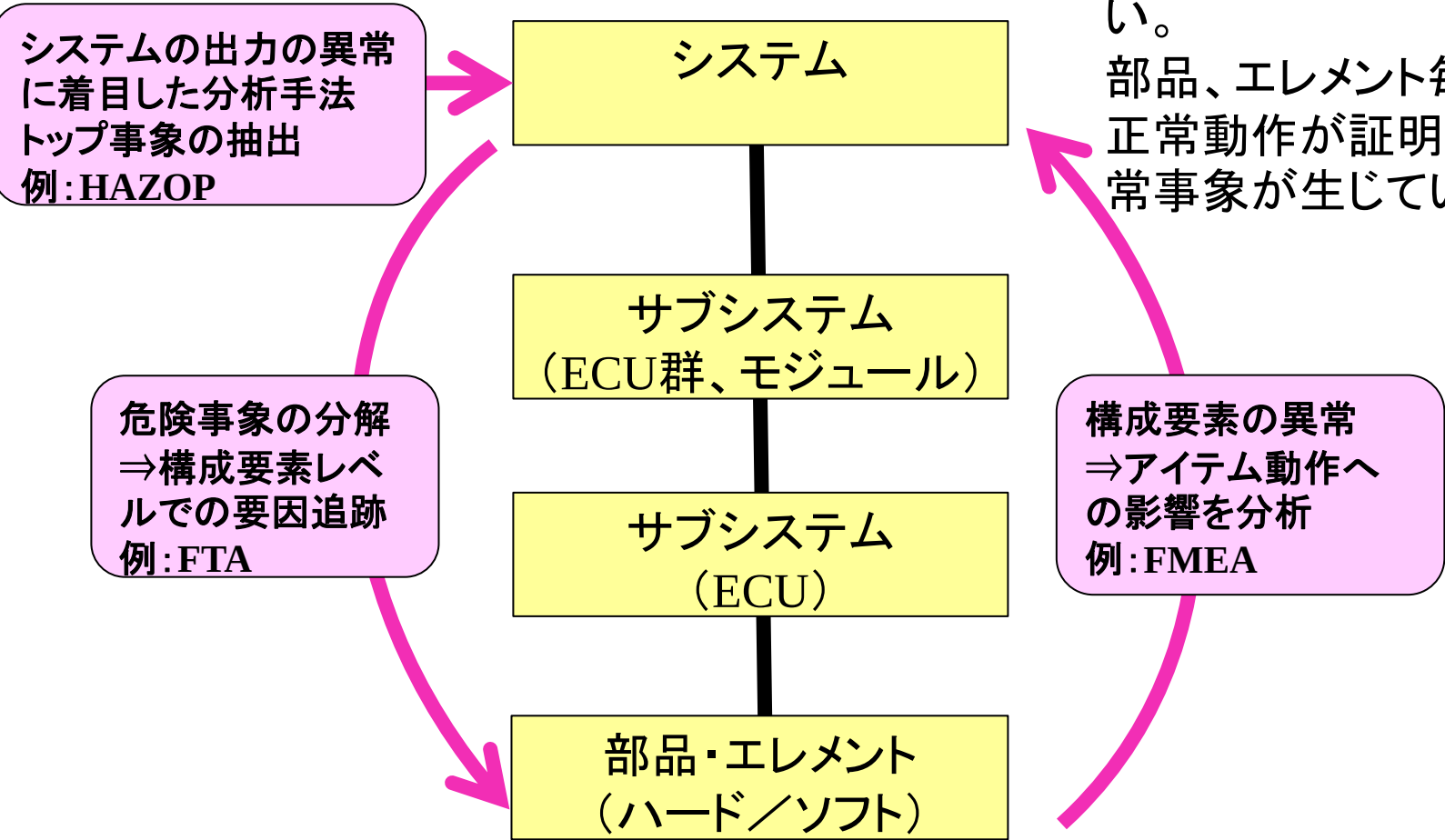
構造、機構(**そのもの**)。

アーキテクチャは構造、機構に加え、目的や設計思想を含む。

※出典: weblio英和辞典、和英辞典より(<https://ejje.weblio.jp/>)

自動車の安全開発の課題

■ 従来の安全分析の例



エレメントの異常やオペレーションミスに着目している。

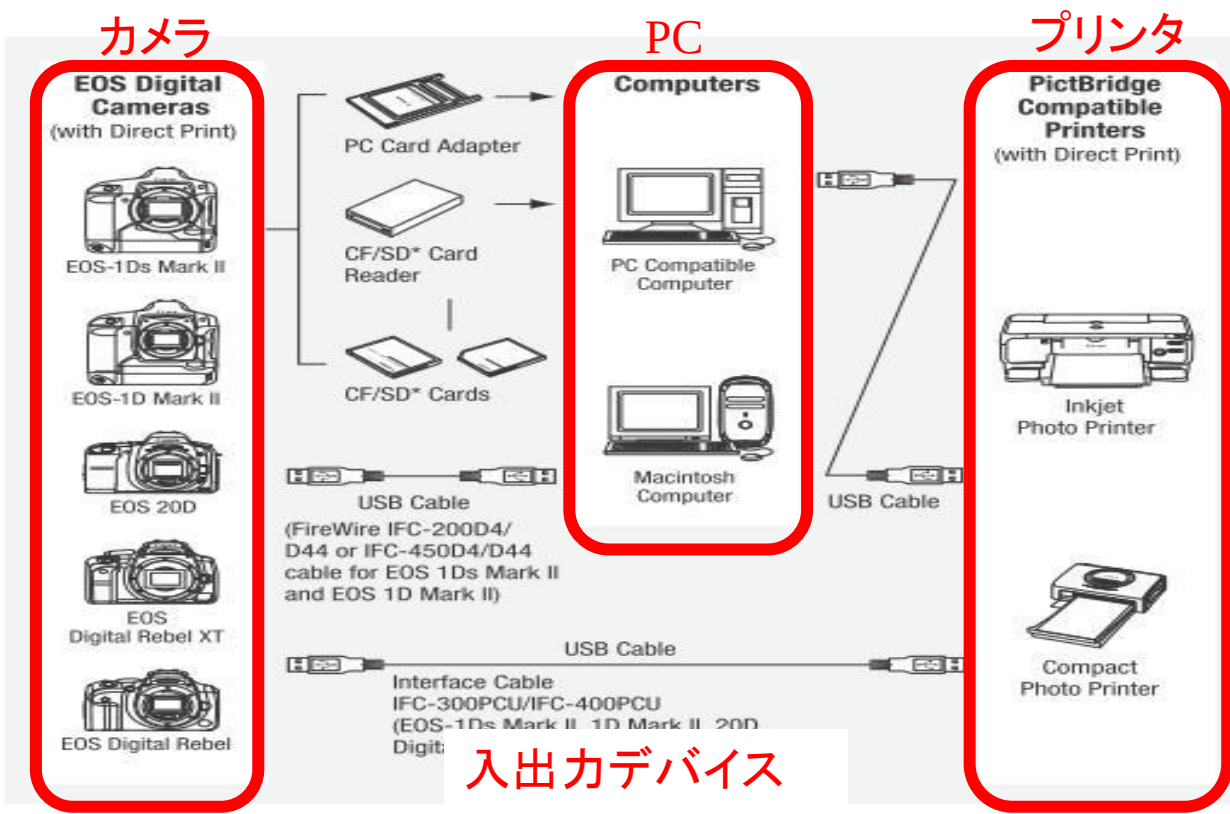
課題: 部品点数の増大、ソフトウェアの複雑化に対応できない。

部品、エレメント毎の安全や正常動作が証明されても、異常事象が生じている。

自動車の安全開発の課題

System of Systems

例：カメラで撮影した画像を印刷する。



＜現象＞

構成要素(カメラ、PC、プリンタ、入出力デバイス)毎の正常動作を確認できているが、画像を印刷できない。

＜想定要因＞

- ・ドライバソフトの互換性
 - ・対応可能な画像フォーマット
 - ・対応可能なI/F規格
 - ーハードウェア形状
 - ー入出力信号
- など

⇒ 構成要素間の相互作用にも異常の要因が潜んでいる

自動車の安全開発の課題

- 自動車のニーズ多様化に伴い、安全思想もより多岐にわたると推測。
運転シナリオやユースケースを俯瞰した安全分析の整理手法の確立が必要。

例：STAMP (Systems-Theoretic Accident Model and Processes)
/STPA (System-Theoretic Process Analysis)

＜考え方＞

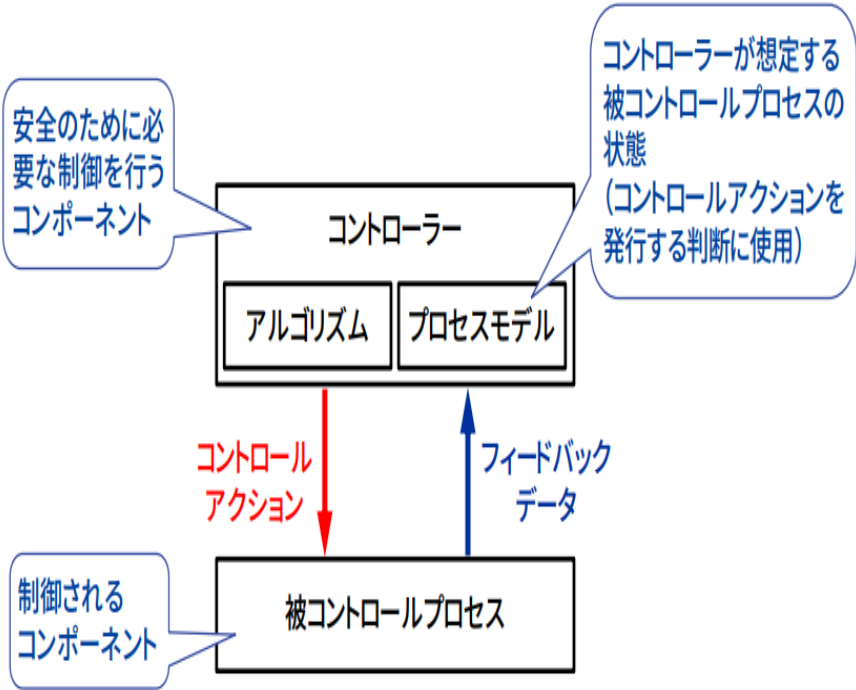
システムはソフトウェアや人間・組織を含む
サブシステムやコンポーネントで構成。



コンポーネントに不具合がなくとも
サブシステム やコンポーネントの相互作用
によってハザードが発生する。



『相互作用に着目した安全分析手法』



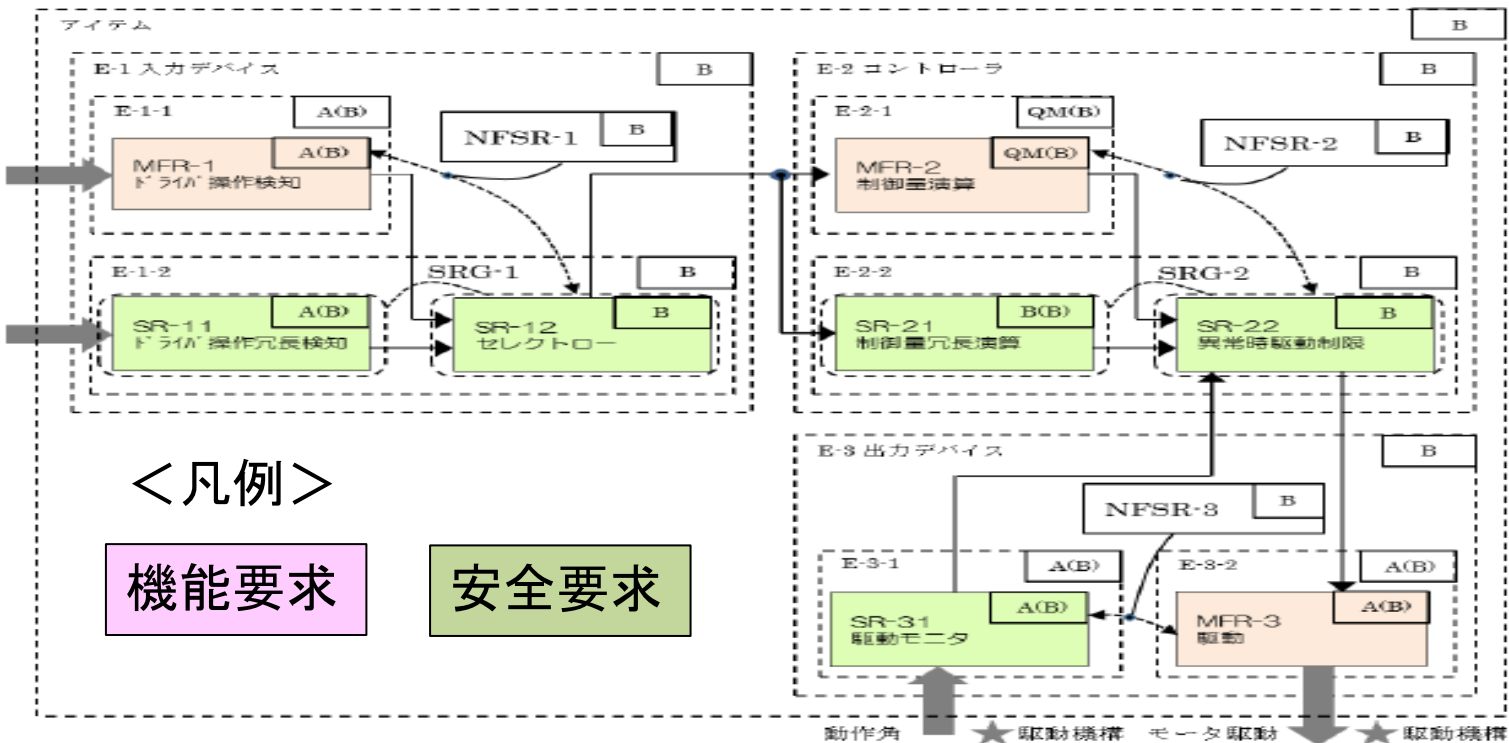
自動車の安全開発の課題

SCDLにおける課題

メリット： 機能要求と安全要求をアーキテクチャレベルで俯瞰している。

課題： アイテムの「目的」に触れていない。

「ふるまい」における記述が不明瞭。



手法連携の狙いと課題

■ 手法連携の狙い

開発手法 ⇒ メリット、デメリットが必ず存在



各々の開発手法のメリットを活用 ⇒ 開発高精度化、高効率化

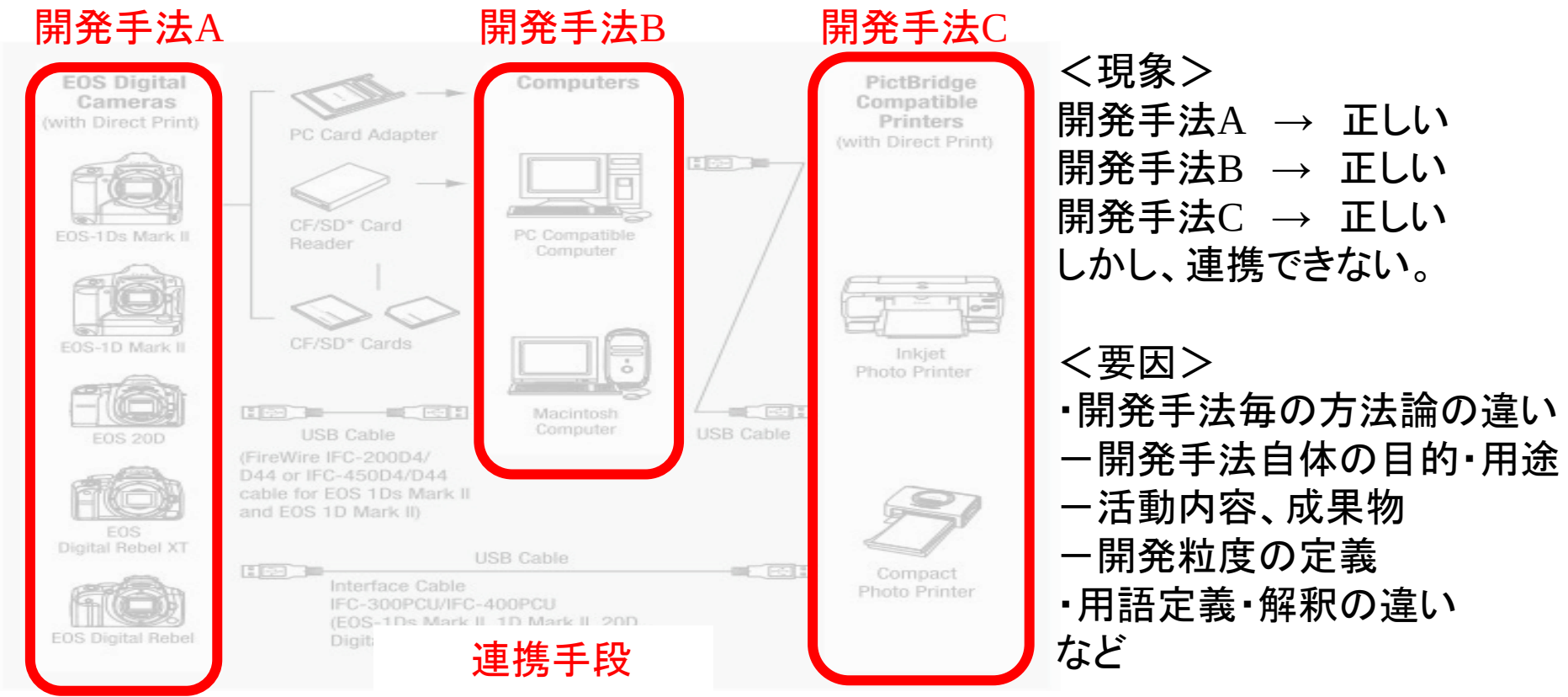
■ 手法連携を実現するための課題

- 各々の開発手法における方法論の違い
 - 開発手法自体の目的・用途
 - 活動・成果物の分類、開発の階層・粒度の分類
 - 開発手法で用いられる用語の定義および解釈の違い
- 理解齟齬なく連携するためのフレームワークづくりが必須

手法連携の狙いと課題

■ 手法連携にはSystem of Systemsと同様の課題が存在。

☆12ページの図の「構成要素」を「開発手法」に置き換えて表現。



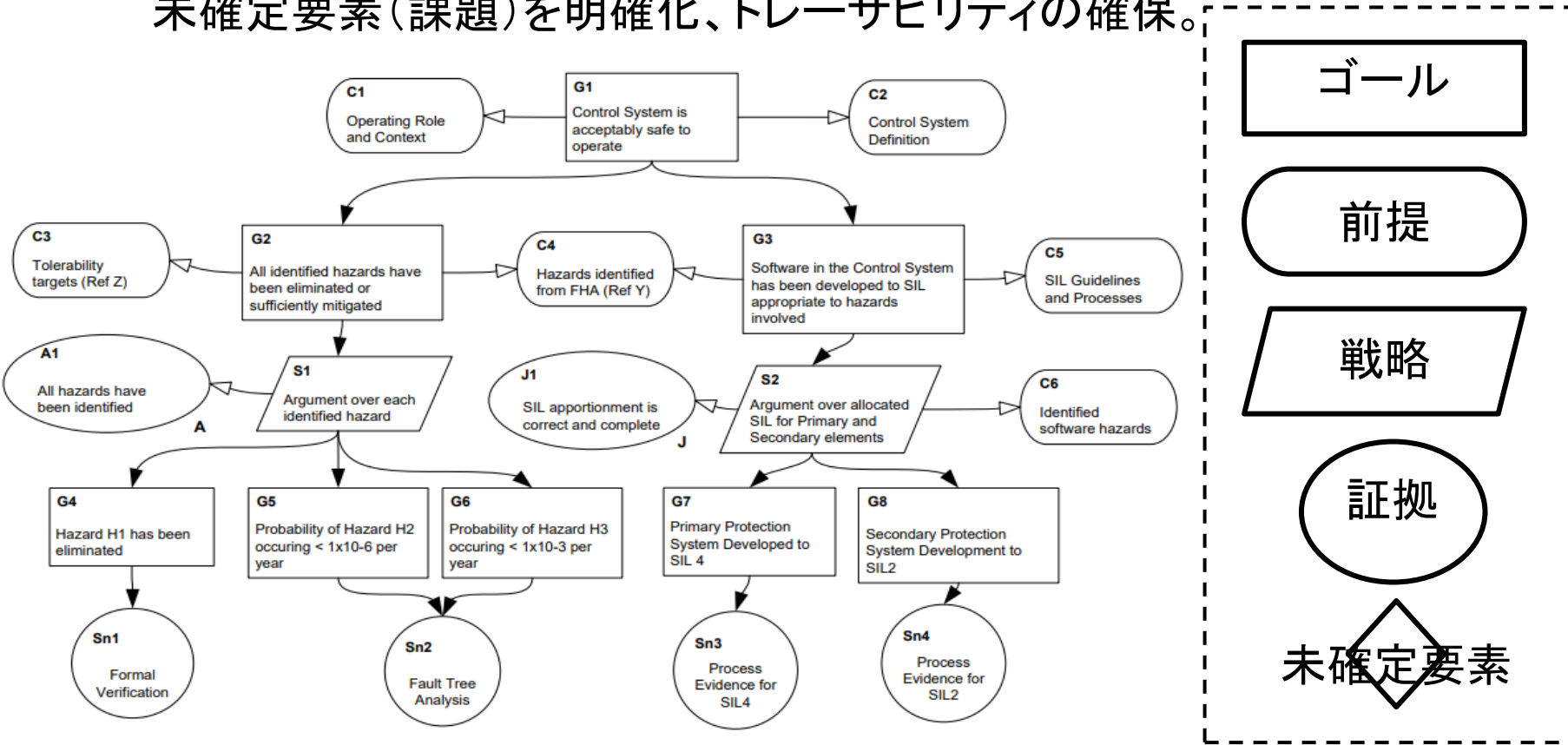
手法連携の狙いと課題

■ 手法連携を行う上での課題と方策

活動・成果物	課題	方策
要求	・粒度／階層が開発者間で共有されていない	・開発の全体像（粒度、階層）の明確化
	・（要求の）目的が共有されていない	・ユースケース、マーケット分析結果の明示
	・（要求に対する）目標が共有されていない	・目標を策定した根拠の明示
アーキテクチャ	・粒度／階層が開発者間で共有されていない	・開発の全体像（粒度、階層）の明確化
	・（アーキテクチャの）定義・解釈が不明確	・用語の定義および明確化
分析	・目的／用途に合わせた分析手法の適用が必要 ・最も効果的な分析手法の適用が不明	・分析対象の明確化

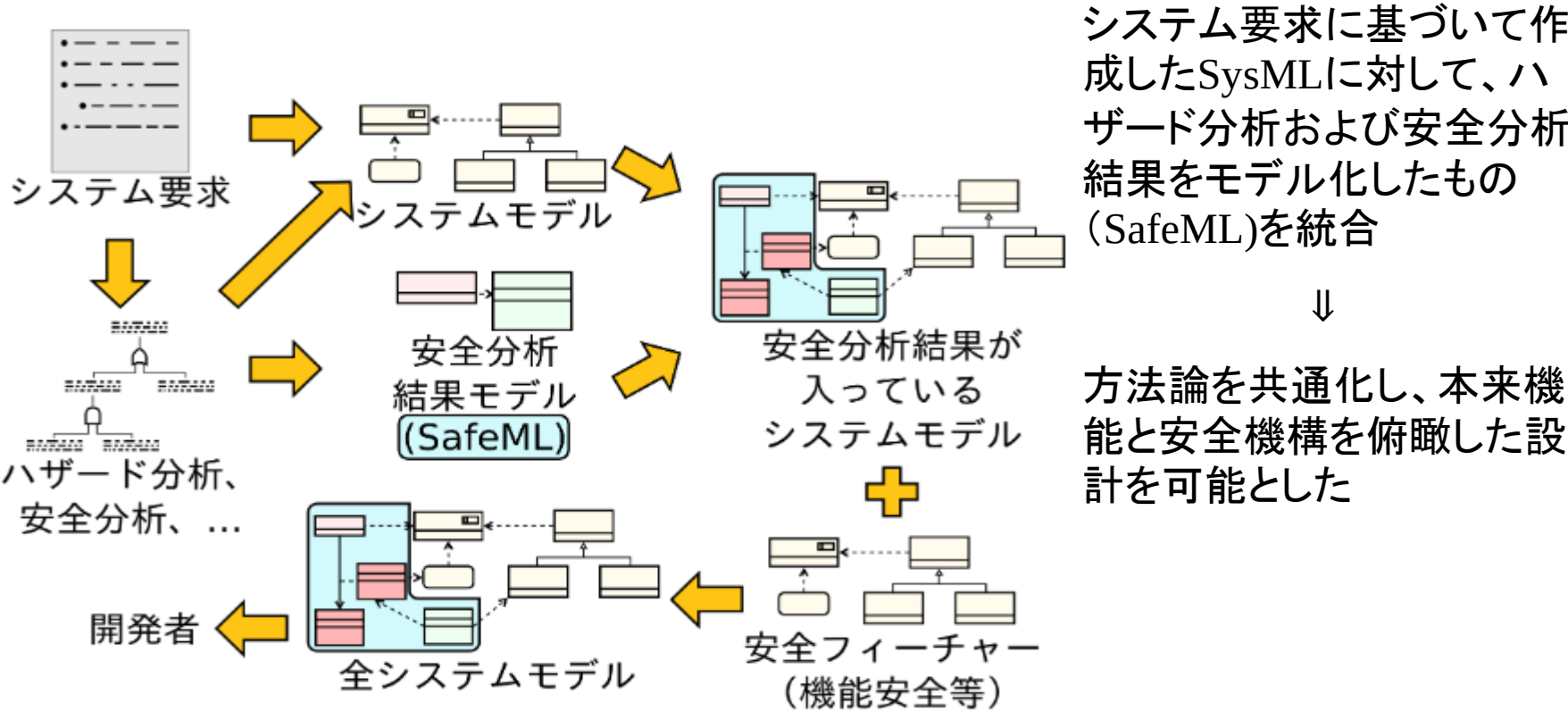
手法連携における課題の対策例

■ GSN (Goal Structuring Notation): 議論を可視化するための表現手法
メリット: ゴール(目的)、戦略(方針)、前提(制約)、証拠(分析手段)、
未確定要素(課題)を明確化、トレーサビリティの確保。



手法連携における課題の対策例

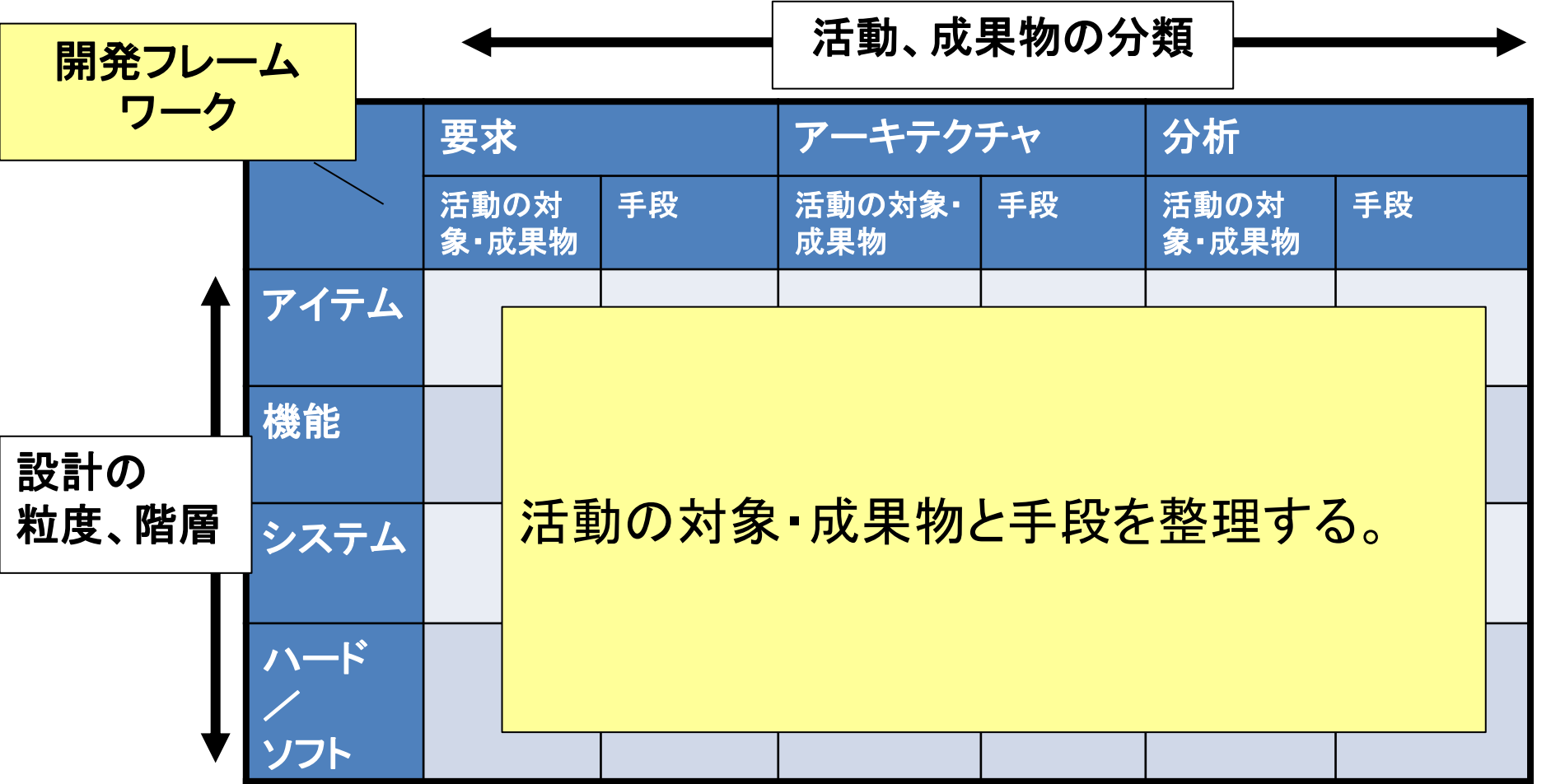
■ SafeML



出典：『SysMLを拡張したSafeMLで、システムの安全性をモデル化・設計しよう』 Geoffrey Biggs 著
※SafeMLは『機械学習システム (Machine Learning) の安全』の意味として使われている
ケースが実在するので注意。

手法連携における課題の対策例

■ マトリックスを用いた開発フレームワークの表現例



SCDLと他開発手法との手法連携

■ SCDLとSysMLの手法連携を検討

☆開発手法としてよく用いられているSysMLとアーキテクチャ表現に強いSCDLとの連携を検討。

＜SysMLの強み＞

- ・多数の使用実績、認知度
- ・アイテム定義
 - ー上位要求
 - ーアイテム外環境
 - ーユースケース
- ・ふるまいに対する記述

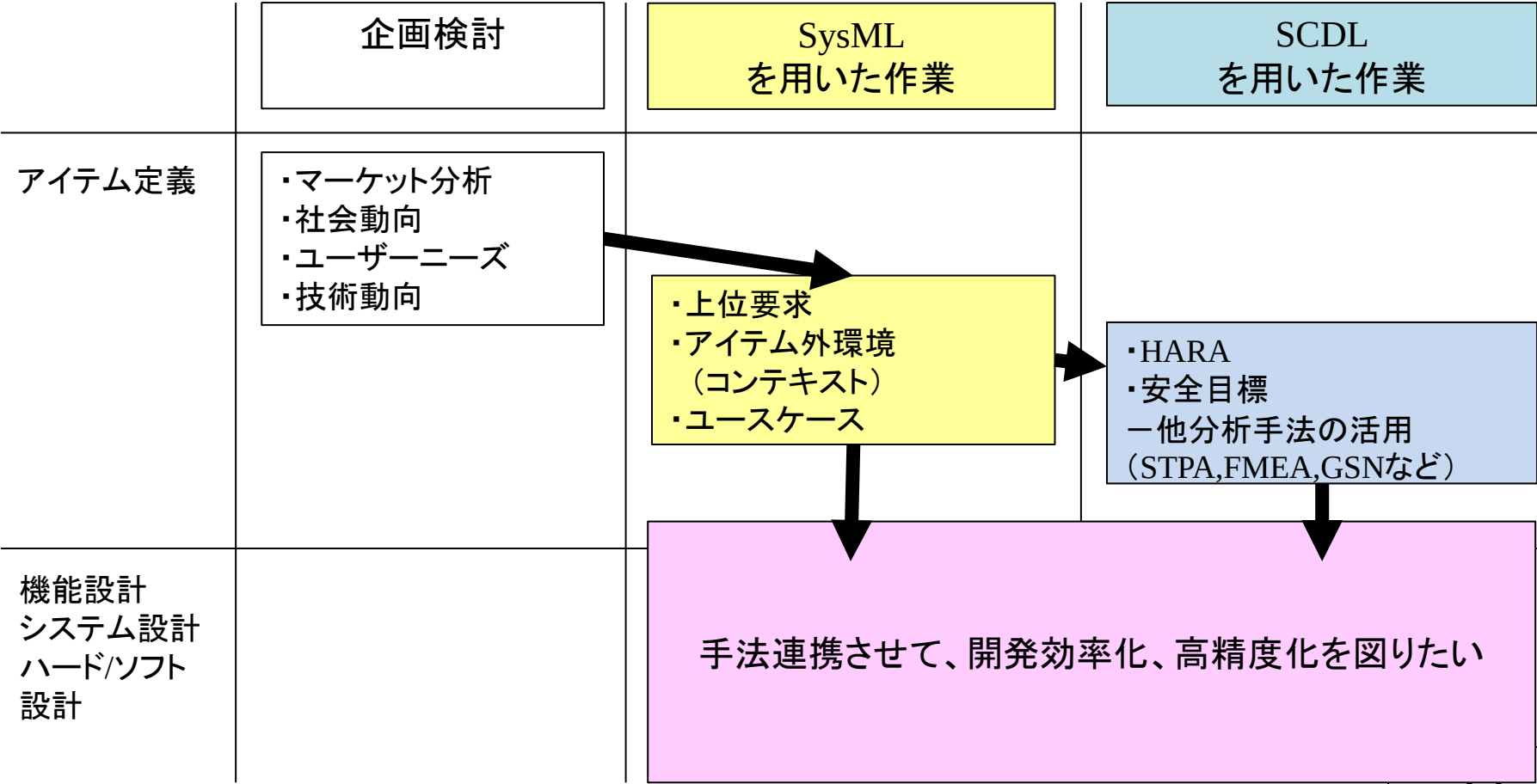
＜SCDLの強み＞

- ・機能要求と安全要求を俯瞰
- ・アーキテクチャ表現に強い
 - ー要求構造
 - ーエレメント構造
 - ー要求配置
- ・ASIL付与、デコンポジション

手法連携して、
両手法の強みを生かす

SCDLと他開発手法との手法連携

■ SCN-SGではSysMLにおける開発方法論(MagicGrid)を用いて、SCDLとの連携検討・課題抽出を行っている。



SCDLと他開発手法との手法連携

■ MagicGridを活用して、手法連携を検討。

	Pillar					
Layer of Abstraction			Requirements	Behavior	Structure	Parametrics
	Problem	Black Box	Stakeholder Needs	Use Cases	System Context	Measurements of Effectiveness
		White Box	System Requirements	Functional Analysis	Logical Subsystems Communication	MoEs for Subsystems
	Solution		Component Requirements	Component Behavior	Component Assembly	Component Parameters

出典:ダッソーシステム社HP(<https://www.3ds.com/ja/>)より

SCDLと他開発手法との手法連携

■ MagicGridと安全設計階層モデルにおける方法論の考察と課題

ー 活動・成果物の分類に関して

- ・MagicGrid: 「要求」「ふるまい」「ストラクチャ」「パラメトリックス」
- ・安全設計階層モデル: 「要求」「アーキテクチャ」「分析」

☆課題: 両手法の活動・成果物分類の相関どりが必要

ー 階層の分類に関して

- ・MagicGrid: 「Problem」「Black Box」「White Box」「Solution」
⇒ 活動の粒度とステータスを包含
- ・安全設計階層モデル: 「アイテム」「機能」「システム」「ハード／ソフト」
⇒ 活動の粒度

☆課題: 「粒度」と「ステータス」を別々に管理すべきか？

ー 論理、物理の解釈に関して

- ・MagicGrid: 「論理 (Problem)」 「物理 (Solution)」
- ・安全設計階層モデルの中ではどのように解釈すべきか？

☆課題: 理解齟齬が発生しない手段の構築が必要

まとめ

- 社会情勢の変化やユーザーニーズの多様化により、自動車を取り巻く状況が大きく変化している。
- 自動車を取り巻く状況の変化に伴い、自動車の安全に対する要求の質・量が高まっている。
- 安全要求の変化に伴い、要求、アーキテクチャ、分析といった安全開発の手法が多様化している。
- 安全開発の手法にはメリット・デメリットが存在すること、各開発手法のメリットを生かす手法連携について述べた。
- 手法連携を行う上で、各開発手法の方法論や解釈の違いが存在し、開発者はこれらを理解する必要がある。
- 手法連携の課題に対する方策と実施例について紹介した。
- SCDLと他開発手法の手法連携の検討について述べた。

ご清聴ありがとうございました。

Thank you for your attention.



ODEP

AFSP
by SGS-TÜV Saar

おおた開発効率化プロジェクト
Ota Development Efficiency Project

代表

小笠原 豊和
Ogasawara, Toyokazu

〒373-0821 群馬県太田市下浜田町1085-79
090-2207-1899 (携帯電話)
0276-52-8915 (固定電話、FAX)
ogatoyocla@mountain.ocn.ne.jp
<https://www.ota-develop-efficiency-project.com/>