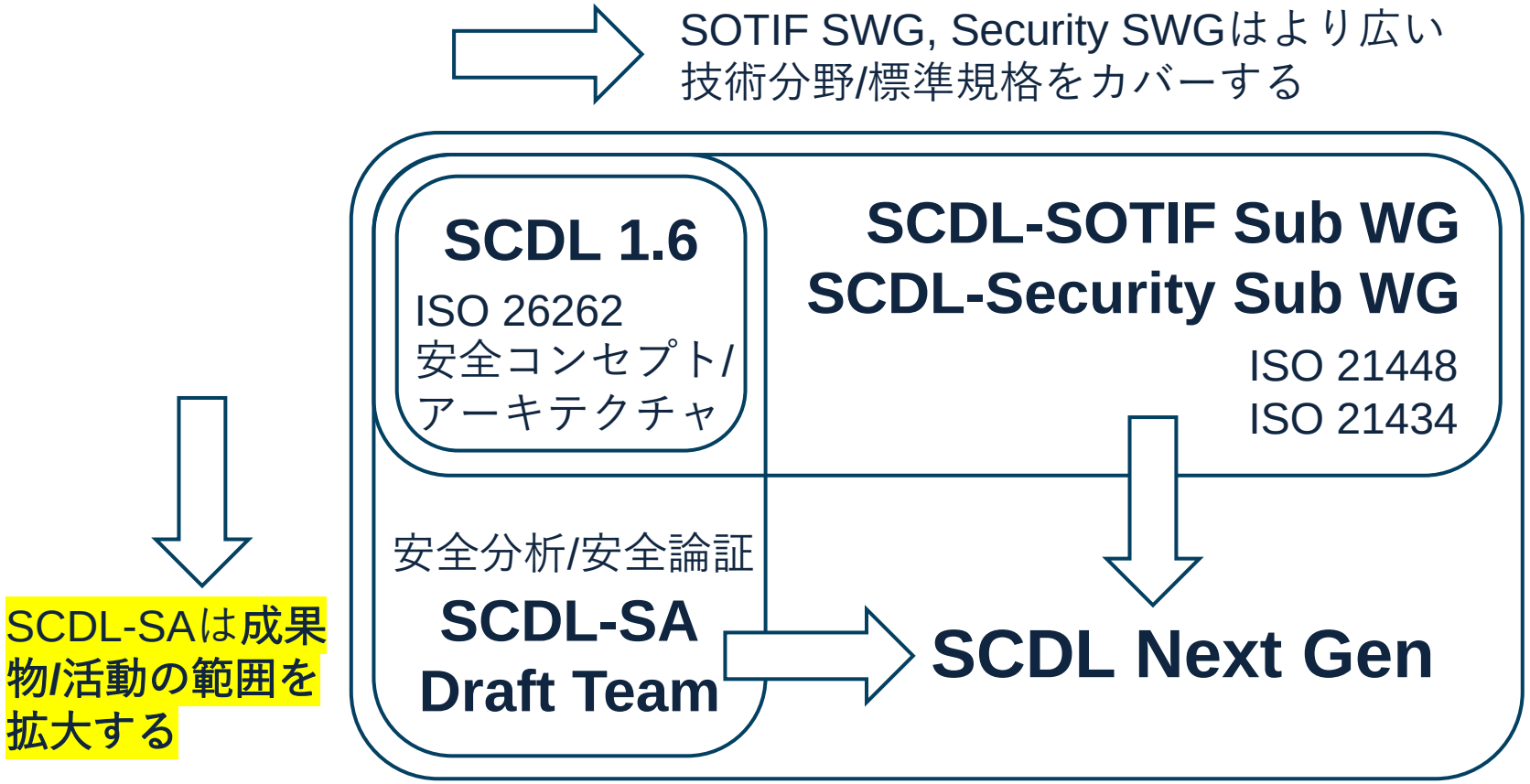
SCDL Next Genに向けたSCDL-SAの検討状況

SCN-SG SCDL-SA Draft Team/SOTIF Sub WG
田中伸明/株式会社 OTSL

目次、概要

1. SCDL NextGenにおけるSCDL-SAの位置付け: ASAM WS (Sep./2023)

- SCDL-SA は安全分析/安全論証をカバーします
  - WG開始当初は安全分析の準形式化を意図して議論開始
  - 安全アーキ＋安全分析＝安全論証とみなして論証にも範囲を拡大



2. SCDL NextGenに向けた検討項目

2.1 SCDL-SAの特徴：故障がモデルに入る

SCDL-SAへの要求事項

新規の要求事項

1. **要求侵害(故障等)**と安全機構の関係の表現
2. 安全分析の階層化
3. 演繹的分析/帰納的分析への対応

SCDL1.6の改善

1. 安全要求間の独立性の効率的な表現

	情報交換、議論から抽出したニーズ
1	安全目標侵害の観点で、どの要求侵害(故障等)をどこの安全機構(SM)で対処するかの表現を整理する
2	コンポーネント単位の分析結果を組み合わせてシステム全体の分析結果を構築できる
3	安全要求間の独立性を効率的に表現できる
4	要求を詳細化した時に、トップダウン、ボトムアップの分析を矛盾なく整合させることができる（整合させる仕掛けがある）
5	主機能故障と安全機構故障の分離のパターン化を表現できる

故障の表現方式

- 図中に表現
  - 例：SafeDeML (次ページ)
- 表として表現
  - 先例：FMEAシート
- ダイナミックドキュメント
  - 例：STATURE (機能安全ツール)
  - 単純な故障-影響以外の独立性、故障伝搬の表現もカバー

SafeDeMLの故障表現

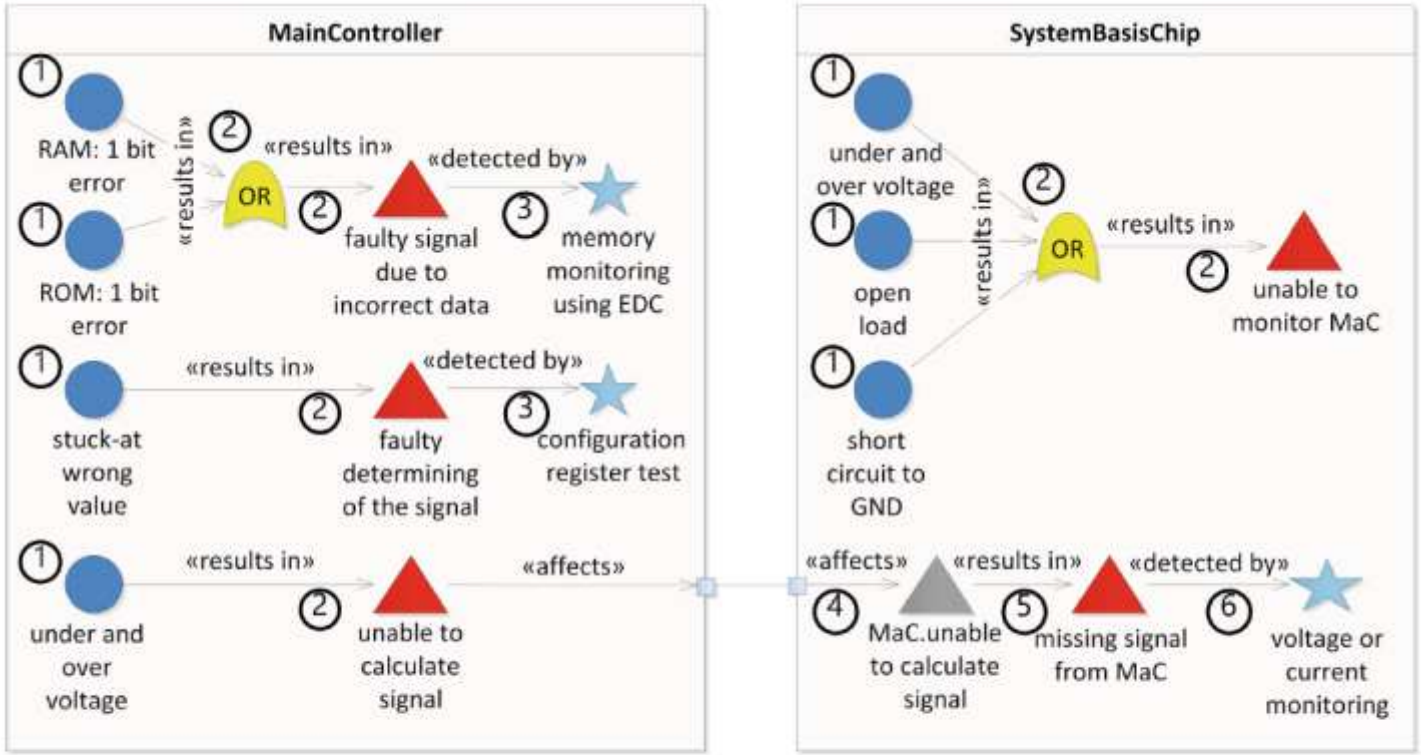


Fig. 8. Excerpt of the brake light system used to validate our modeling methodology. It contains the failure definitions for the *MainController (MaC)* and the *SystemBasisChip (SBC)* The numbers assigned to the elements indicate the different steps in which these elements are added to the fault modeling.

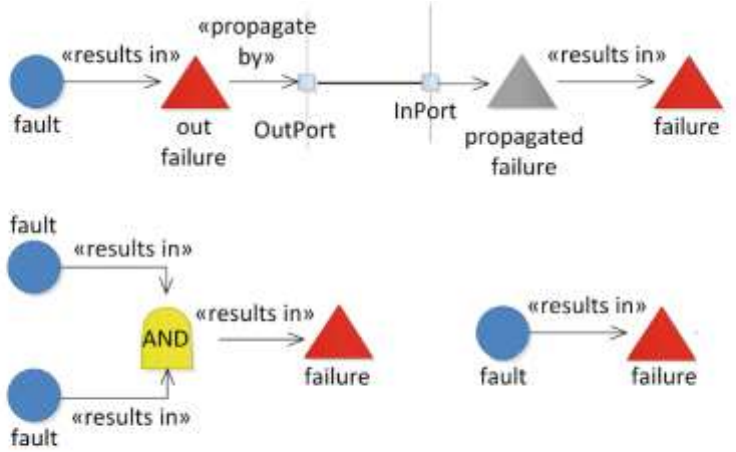


Fig. 4. Possible representations of the SafeDeML::Failure modeling. It shows a horizontal propagation (top), a SafeDeML::Failure with more than one correlated SafeDeML::Fault (left) and a single SafeDeML::Fault leading to a failure.

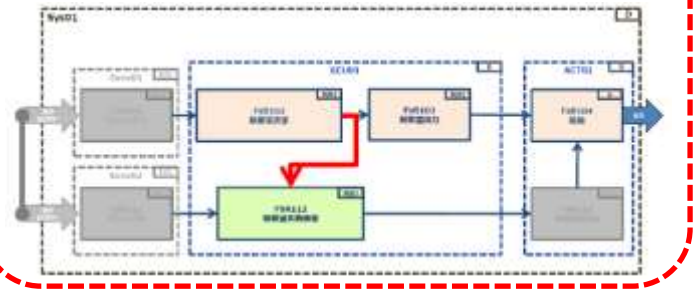
2.2 SRVAのモデル化(SRVA : Safety Req. Violation Analysis)

安全
コンセプト

安全分析

安全要求

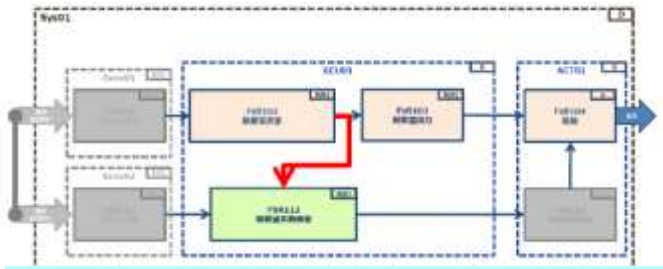
SCDL 1.6



FMEA,
FTA,
SRVA,
etc

ID	名称	内容
TsR101-1-1	センシング 1	Sens01 は車両単動にしたがって正しく静電容量を変化させ、TsR101-1-2 へ正しく送信すること
TsR101-1-2	変換 1	Sens01 は信号変換部を設けて、静電容量を正しく電圧に変換し、TsR101-1-3 へ正しく送信すること
TsR101-1-3	デジタイズ 1	Sens01 は A/D 変換により、正しくデジタル量に変換し、TsR101-1-4 へ正しく送信すること
TsR101-1-4	コミュニケーション 1	Sens01 はデジタル量をシリアル通信によって TsR101-1-5 へ正しく送信すること

SCDL NextGen



SCDLと相性の良いSRVAを
組合せて安全アーキの一部と
することを議論中

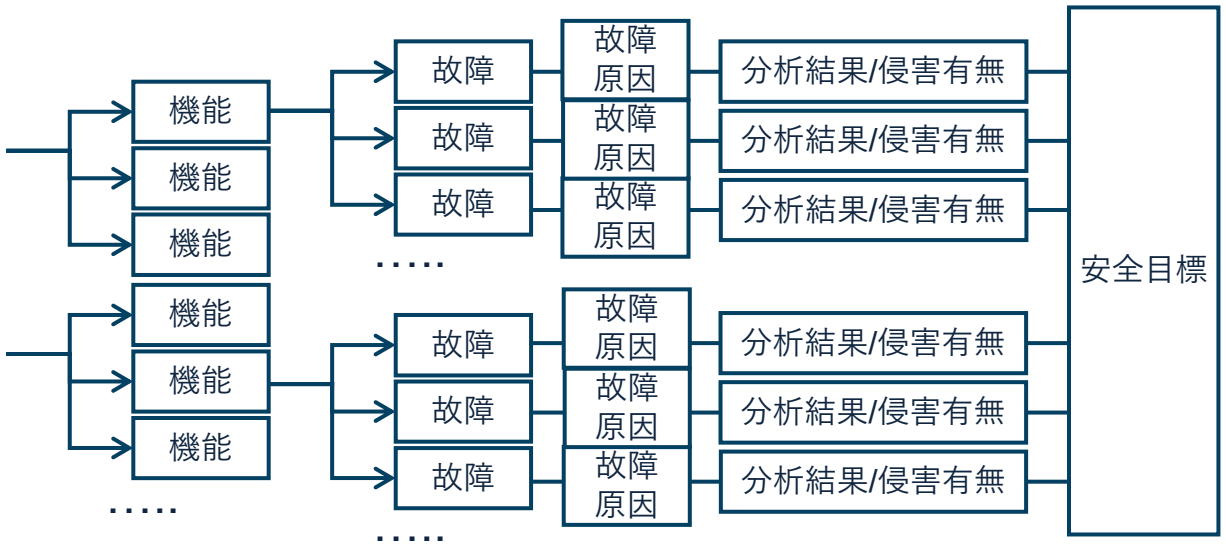
SRVAのメタモデル作成、
他の安全分析手法との
比較をトライ

FMEAとSRVAの考え方

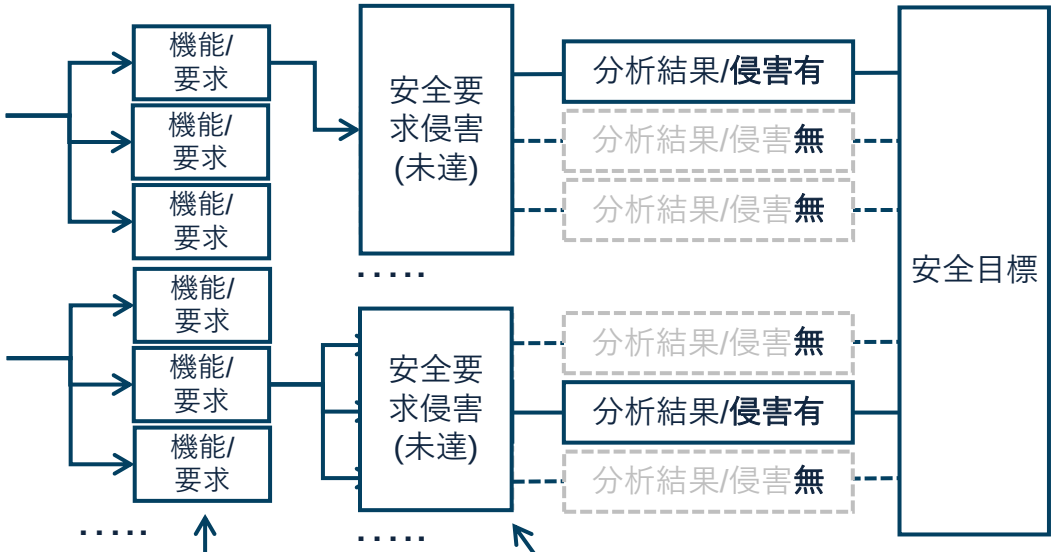
故障の影響を考え、
原因側の信頼性を高めるのがFMEA。

安全目標侵害の影響と対策を考えるのがSRVA。

FMEA



SRVA



AIAG/VDAの機能≒ SRVAの要求

安全目標を侵害する事象＝SGVモード

図A.3 SRVAとFMEAの考え方

FMEAでは機能の故障、故障原因、影響を分析する。

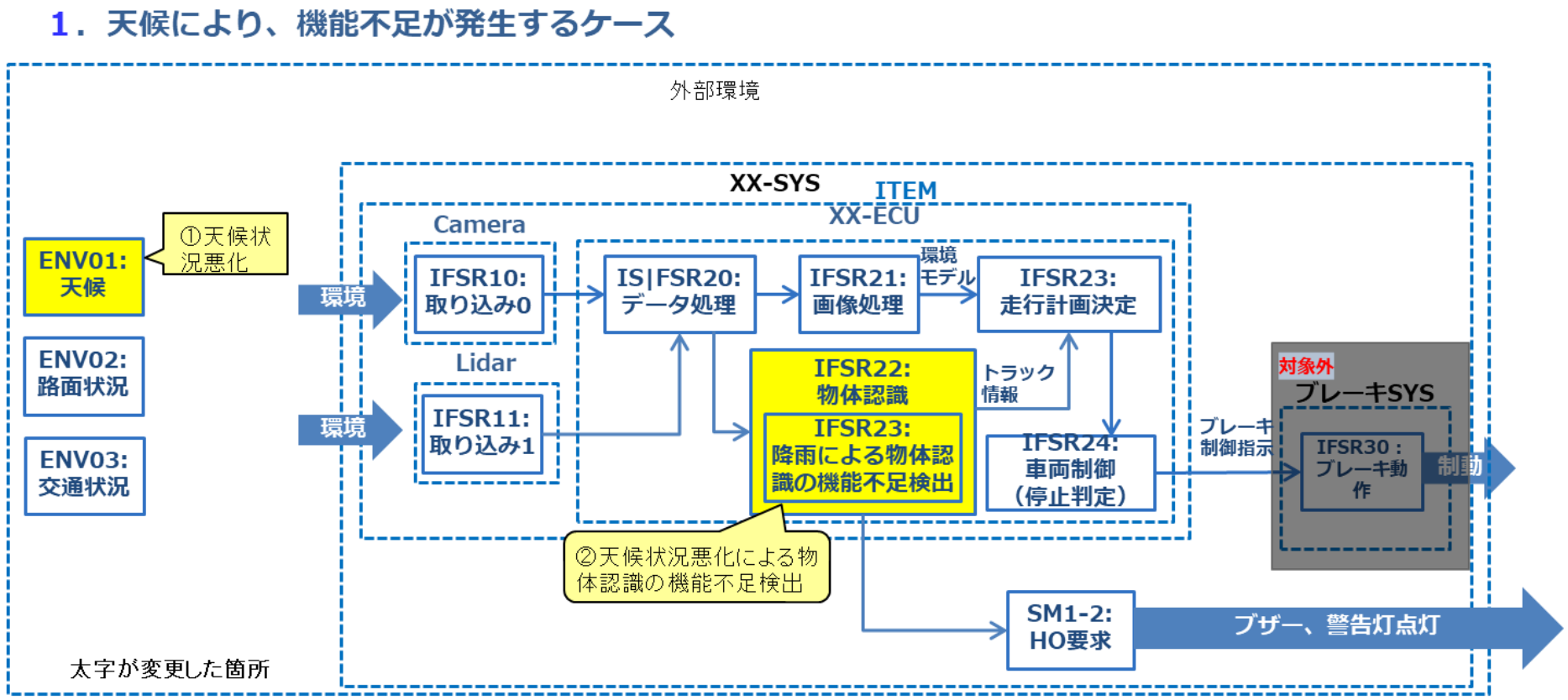
SRVAでは、安全目標侵害が発生する事象(SRVモード)を抽出する。
安全目標侵害の影響と対策を考える。

表A.2 SRVAとFMEAのメリット

	AIAG/VDA FMEA	SRVA
メリット	部品レベルの故障に対する網羅性が高い。 故障抽出の難易度低。	高い抽象度での分析が行えるため、作業効率が良い。

2.3 SOTIF SWGのHLRとの関係

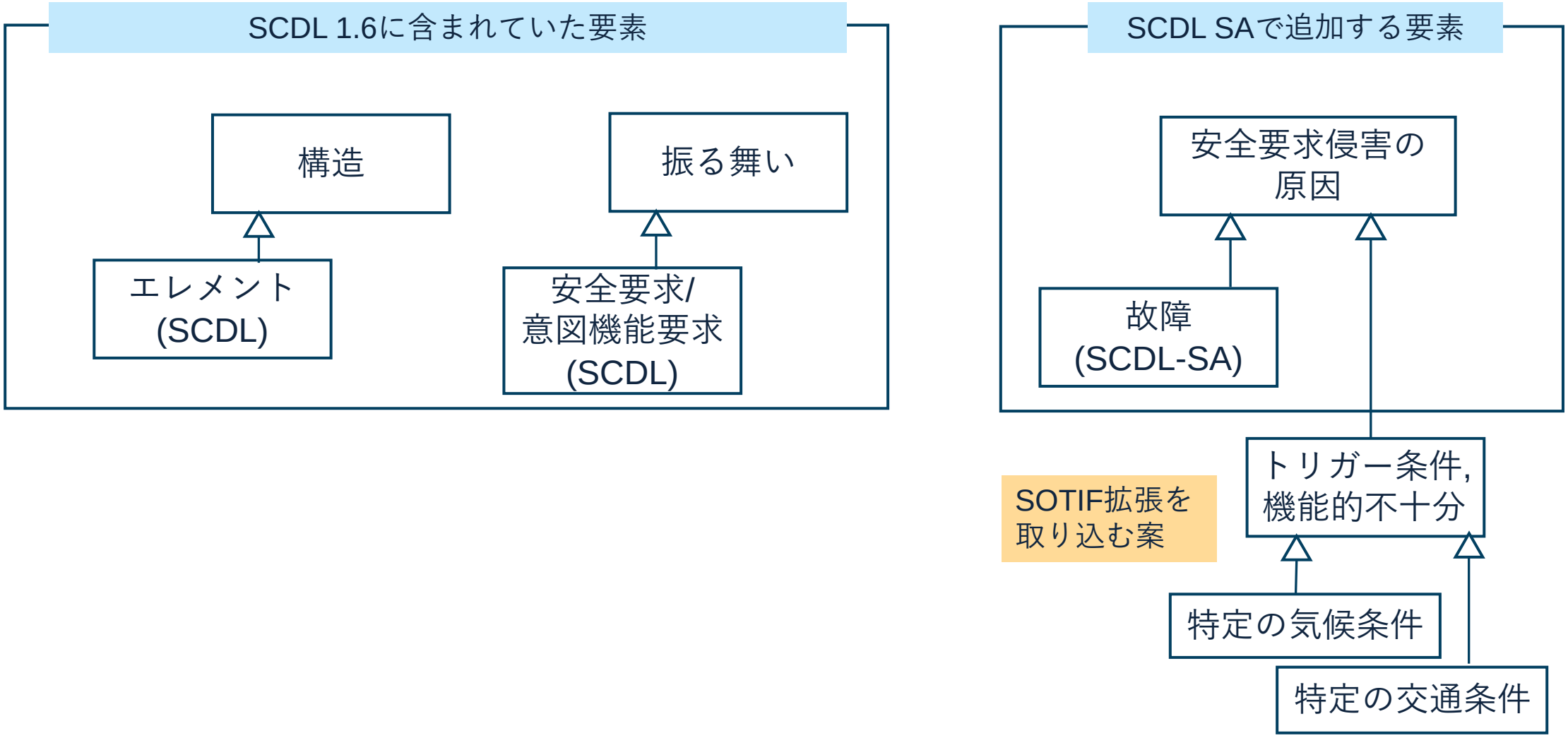
SOTIF SWGの課題：
トリガー条件、機能的不十分性をSCDLの中にどのように取り込むべきか。



SR	SRV mode	誘発条件例（SOTIF）	SMr / SM	
IFSR21: 周辺環境モデルを生成する	停止標識を誤って環境モデルとして生成する	ML学習不足により看板と標識を誤って認識してしまう	-	SMr1：MLの再学習による性能向上
IFSR20：周囲の物体を認識する(認識処理する)	周囲の物体を誤って認識する	**天候状況悪化により物体を誤って認識する**	**SM1：天候状況悪化を検出した際にハンドオーバーを要求する**	~~SMr2：MLの再学習による性能向上~~

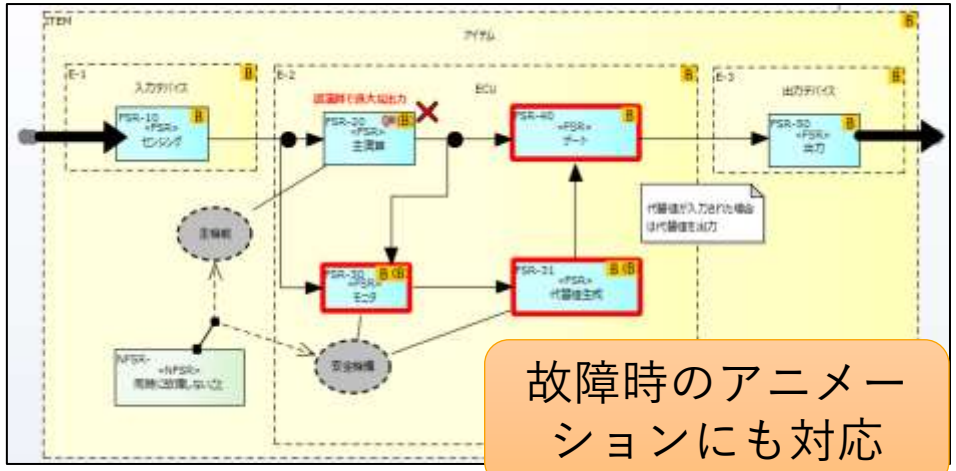
SOTIF SWGのHLRとの関係(続き)

- トリガー条件、機能的不十分性を安全要求侵害の一種とみなすことを検討



2.4 ダイナミックドキュメント

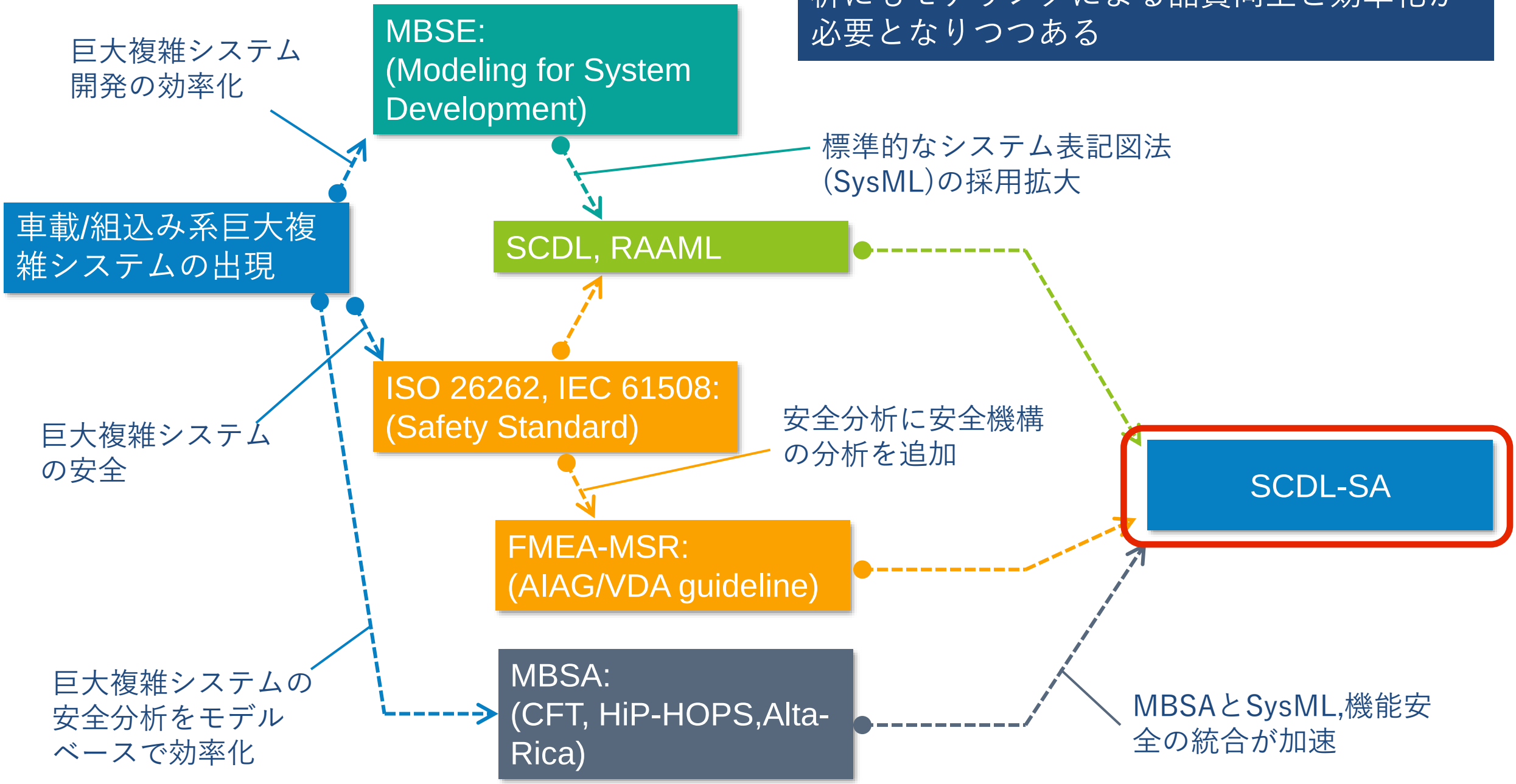
- 静的な図の限界
  - 例：モデルが大きくなると独立性の表現が煩雑に
  - 例：故障が伝搬する様子を表現できない/表現が煩雑に
- 独立性、故障の伝搬を表示するソフトウェアツールは存在する
  - ⇒表現方法をSCDLの一部とできないか？



既存製品の例

なぜSCDL-SAが必要なのか?

車載系巨大複雑システムの出現により安全分析にもモデリングによる品質向上と効率化が必要となりつつある

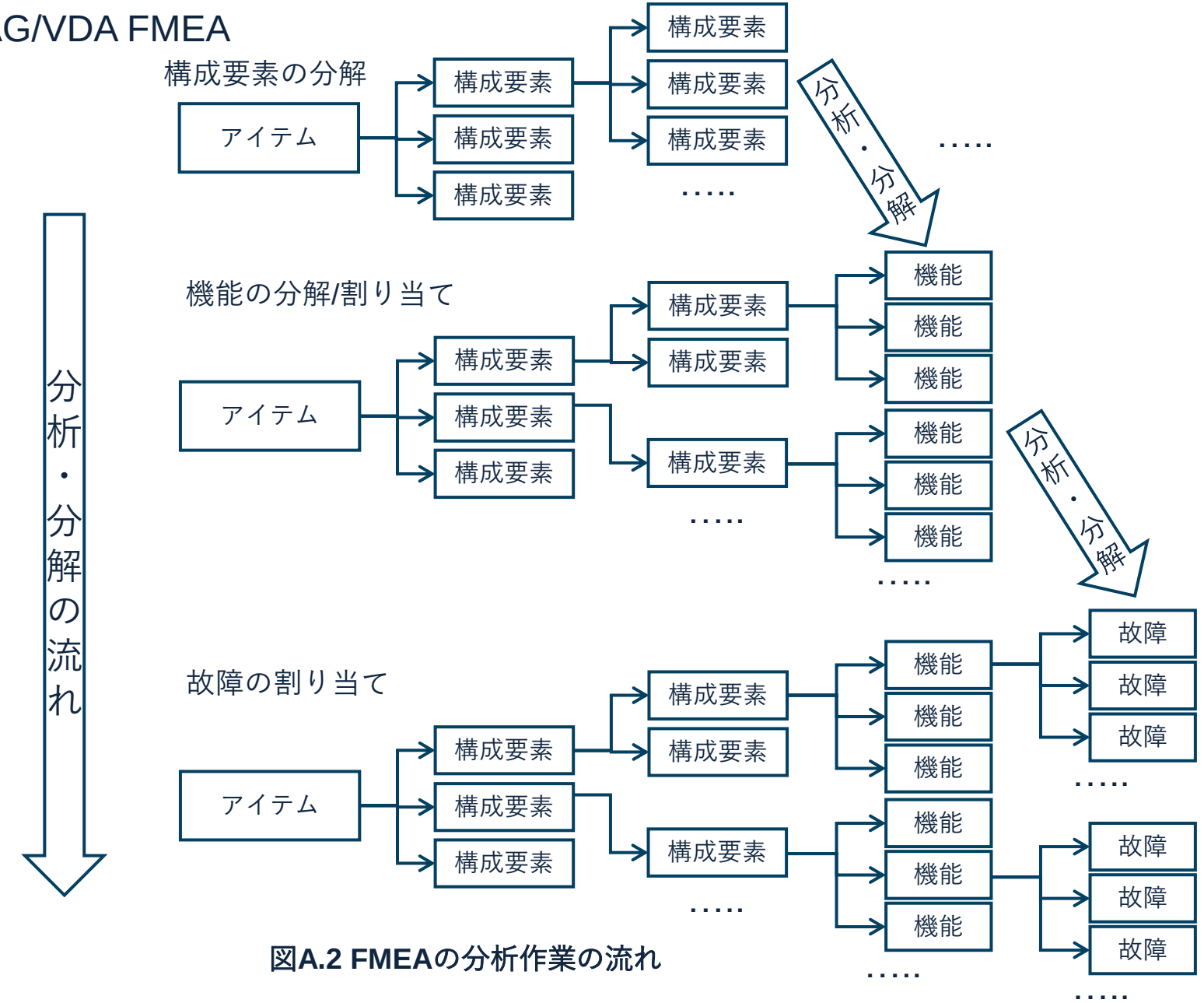


おわりに

- SCDL NextGenに向けた検討状況をご紹介しました
  - 故障がモデルに入る
  - SRVAのモデル化
  - SOTIFのHLRとの連携
  - ダイナミックドキュメント
- SCDL NextGenの重要な軸としてSCDL-SAの技術開発を進めます

予備スライド

AIAG/VDA FMEA



図A.2 FMEAの分析作業の流れ

AIAG/VDA FMEA ver.4参照