モデルベース安全分析(MBSA)とSCDL-SA

SCN-SG SCDL-SAドラフトチーム
ガイオ・テクノロジー株式会社　田中伸明

自己紹介

- 田中伸明
  - 所属：ガイオ・テクノロジー株式会社
    - サービス＆ツール事業本部 開発2部 AWPグループ
  - 技術分野：
    - 機能安全＋モデリング(SCDL/UML/SysML)：
      - DECSoS (Safecomp) 2020、自技会春季大会2020でMBSAの技術発表(名古屋市工業研究所、東芝と共同発表)
      - 機能安全デザインパターン(JASPAR機能安全WG : 2016年)
      - エンジニアリングサービス、技術調査/技術開発を担当
    - プロセス：
      - JISX 33000シリーズ原案作成委員会
      - Automotive SPICE provisional assessor
      - 現在、出向先にてプロセス監査業務に従事

講演の主旨：

- 安全コンセプト以外の安全分析、安全論証などもSCDLで記述したいというニーズに応え、SCDL-SA(Safety Analysis/Assessment/Argument/Assurance)ドラフト作成チームが2022年4月に発足しました
- 本講演ではSCDL-SAに関連する技術分野であるMBSA (Model-Based Safety Analysis/Assessment)の概要と、SCDL-SAとの関係についてご紹介します

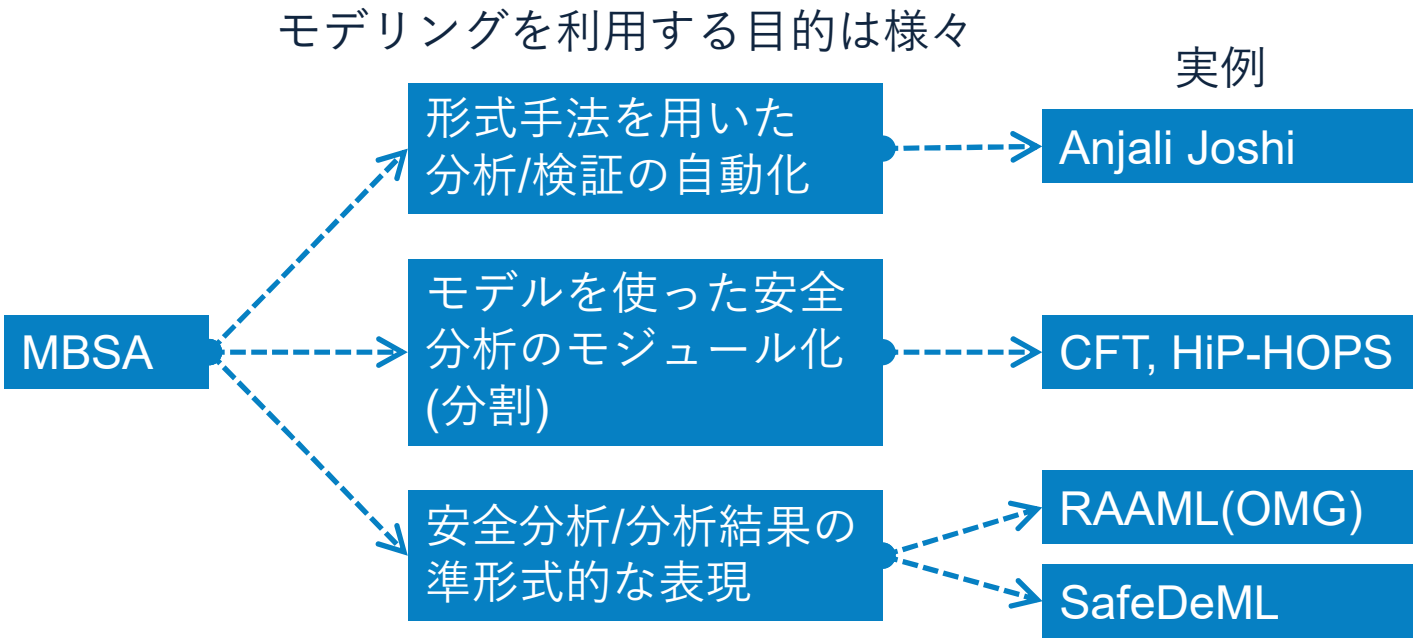
アジェンダ

- 1. MBSAとは
- 2. なぜMBSAが必要なのか
- 3. MBSAにはどんな技術が含まれているのか
- 4. SCN-SGの取り組み
- 5. MBSAの難しさ、今後の課題
- 6. 今後の取り組み

1. MBSAとは

- MBSA (Model-Based Safety Analysis/ Assessment : モデリング技術を安全分析に利用する技術

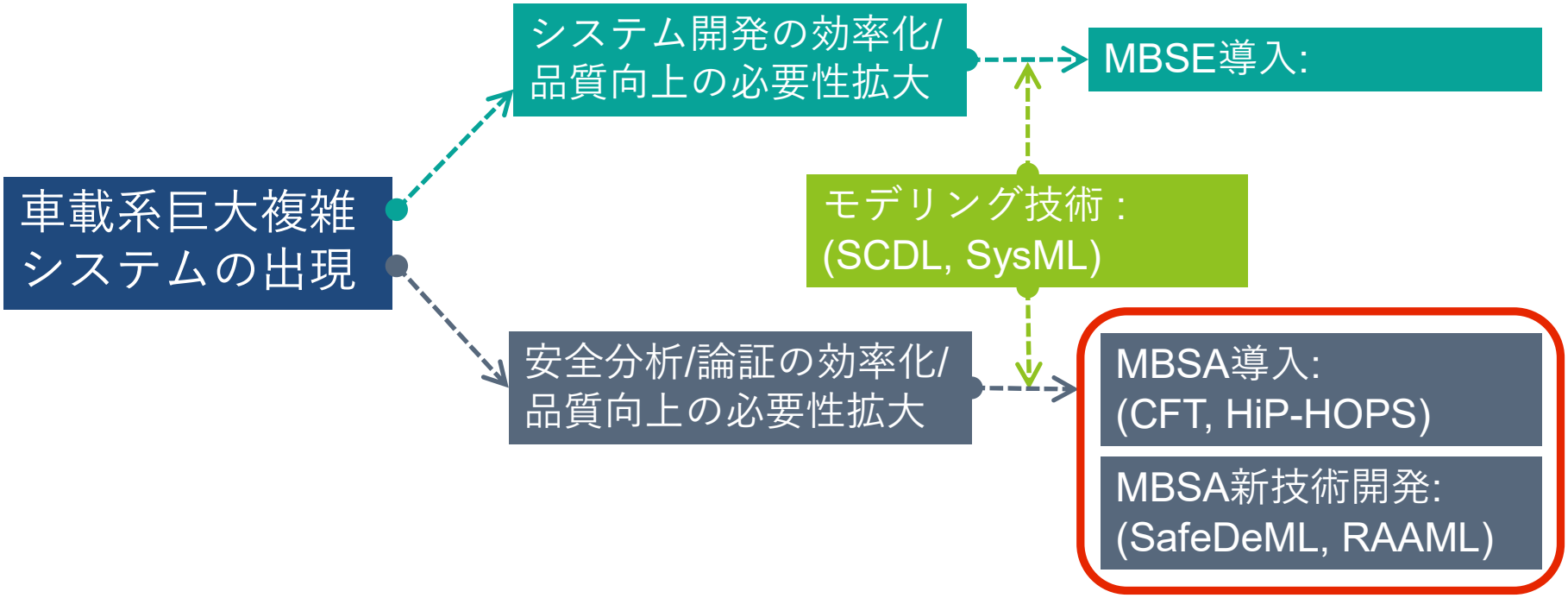
MBSA=安全分析+モデリング



主な情報源：IMBSA(International Symposium on Model-Based Safety Assessment)

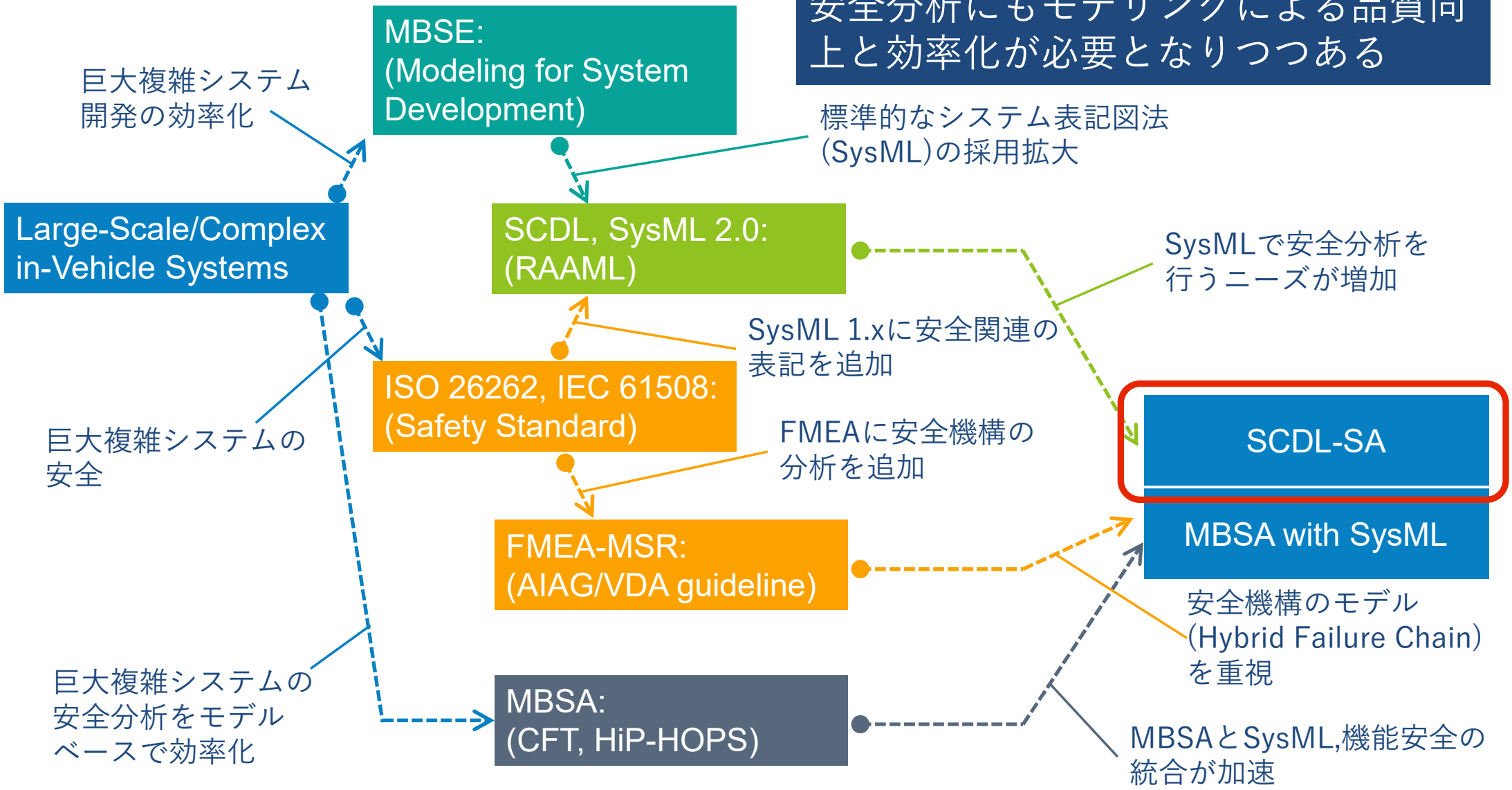
2. なぜMBSAが必要なのか

- 車載系巨大複雑システムの出現により、MBSEが対象としてきた設計、要求だけでなく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

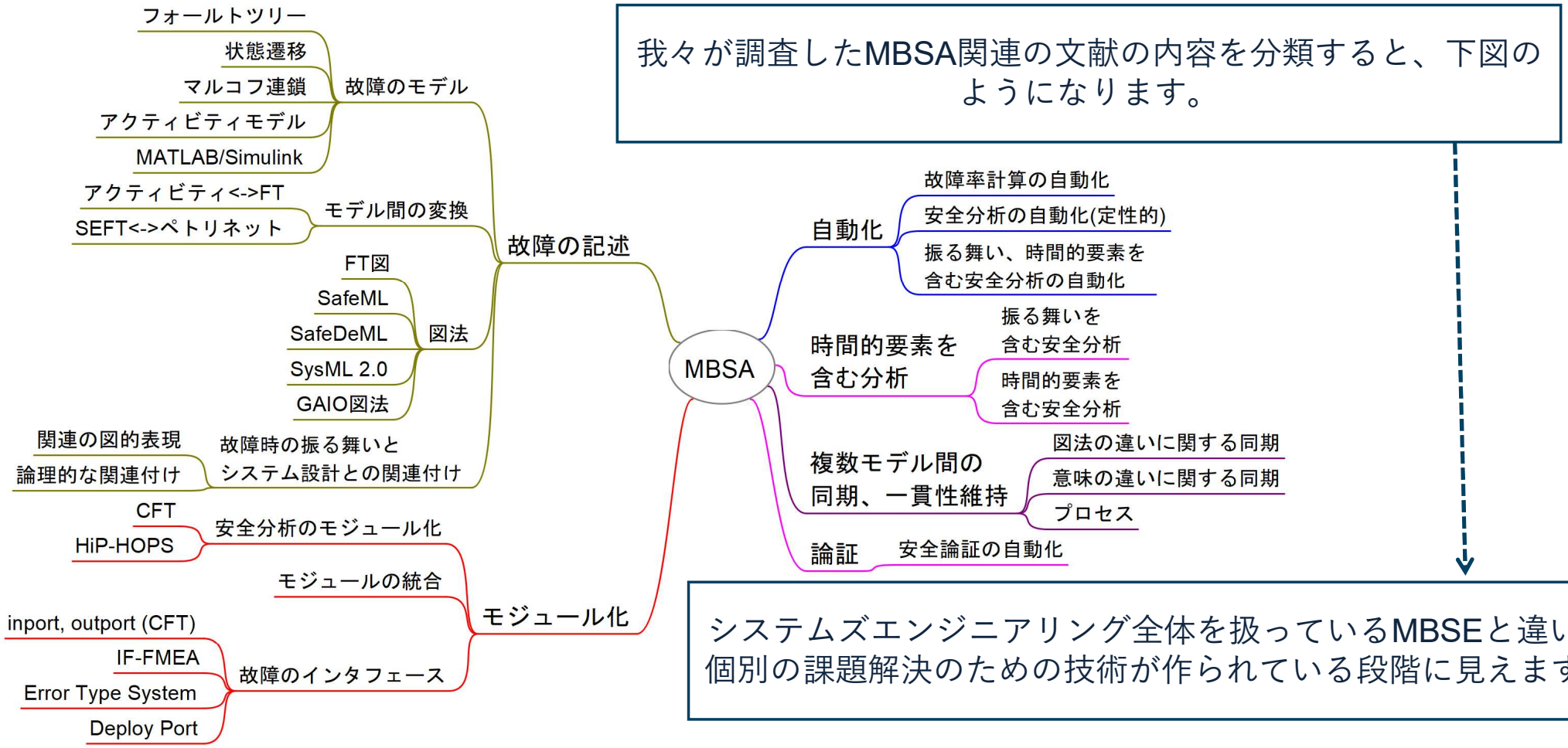


2. なぜMBSAが必要なのか(詳細)：

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



3. MBSAにはどんな技術が含まれているのか

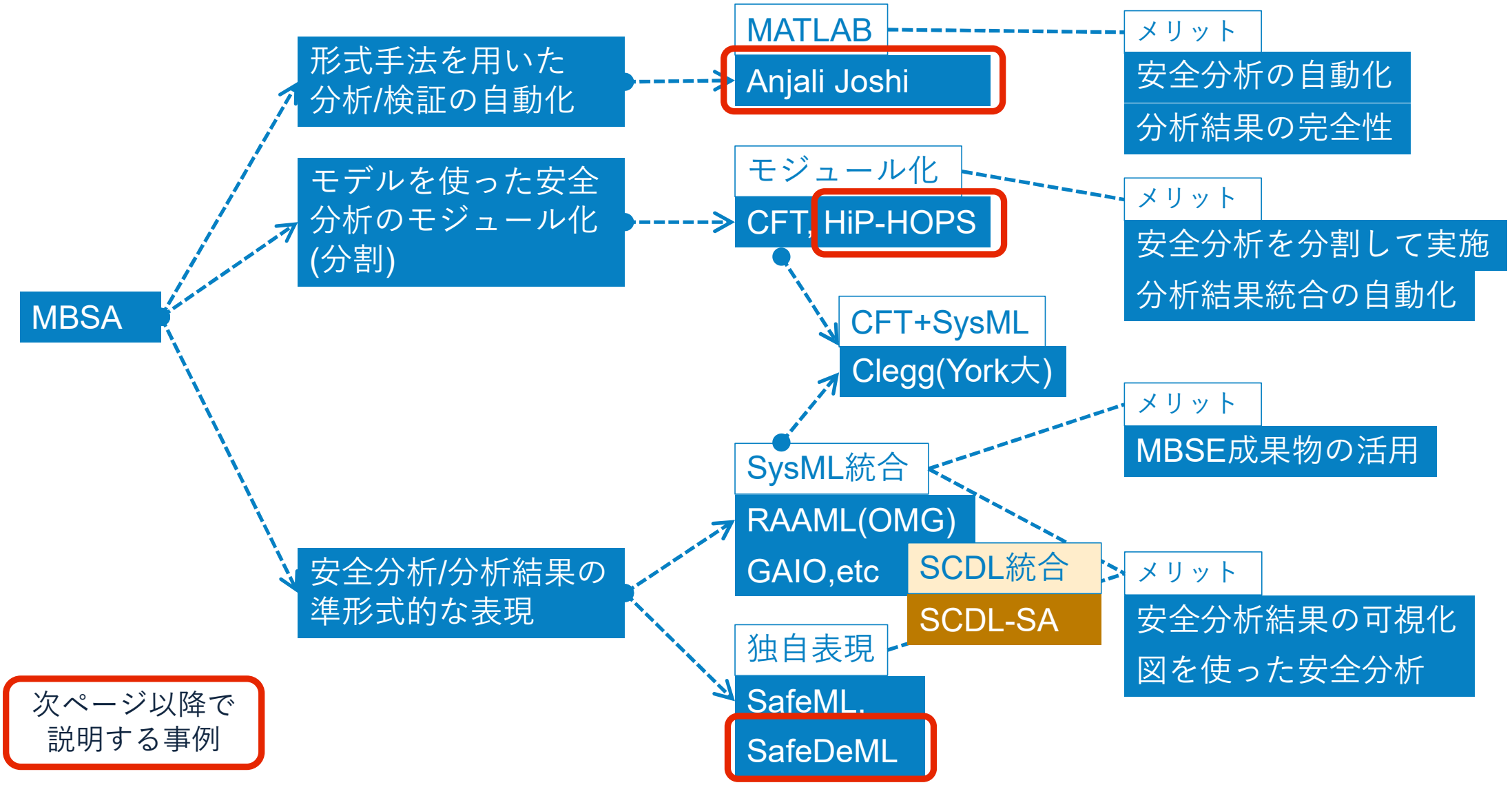


我々が調査したMBSA関連の文献の内容を分類すると、下図のようになります。

システムズエンジニアリング全体を扱っているMBSEと違い、個別の課題解決のための技術が作られている段階に見えます。

本ページの技術分類は弊社で独自に検討したものです。一般的な定義、分類は見つかっていません。

3. MBSAにはどんな技術が含まれているのか(主な例)



事例１：Joshi et al.の研究

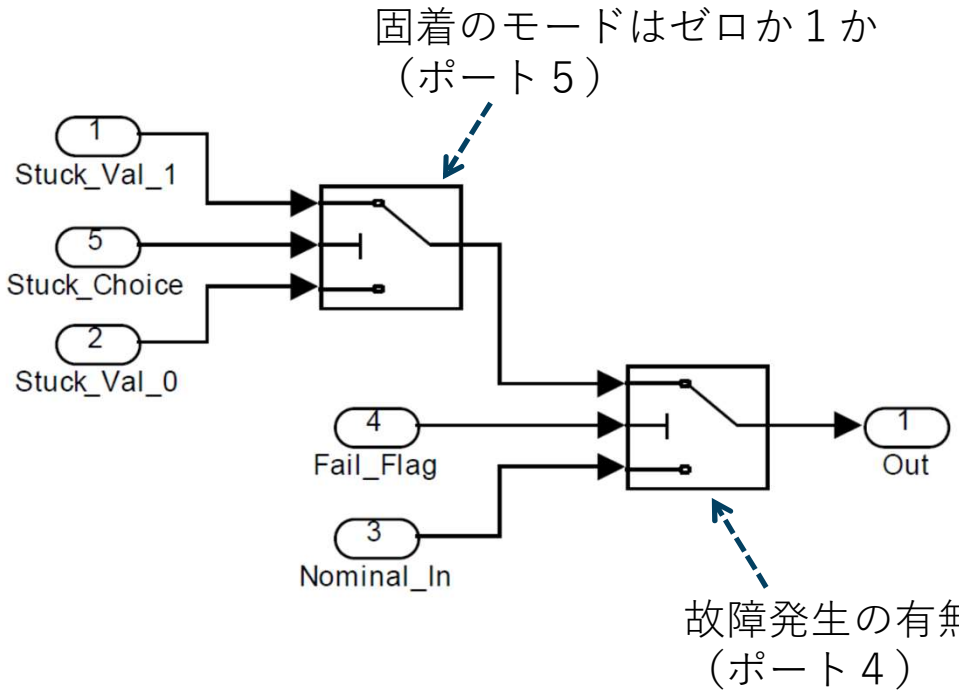


Figure 6 : Binary_Stuck_at

MATLABモデルで故障時の振る舞いを記述し、故障時の特性(いくつのマルチプルポイントフォールトで安全目標侵害が発生するかなど)を形式的に解析する。

故障がゼロか１の固着のみの場合、その振る舞いはこのMATLABモデルですべて表現できる＝形式的に解析できる。
形式検証にはNuSMVモデルチェッカーを使用。
ただし、システムのすべての故障事象をモデルとして表現することは現実的には不可能。

事例２：HiP-HOPS

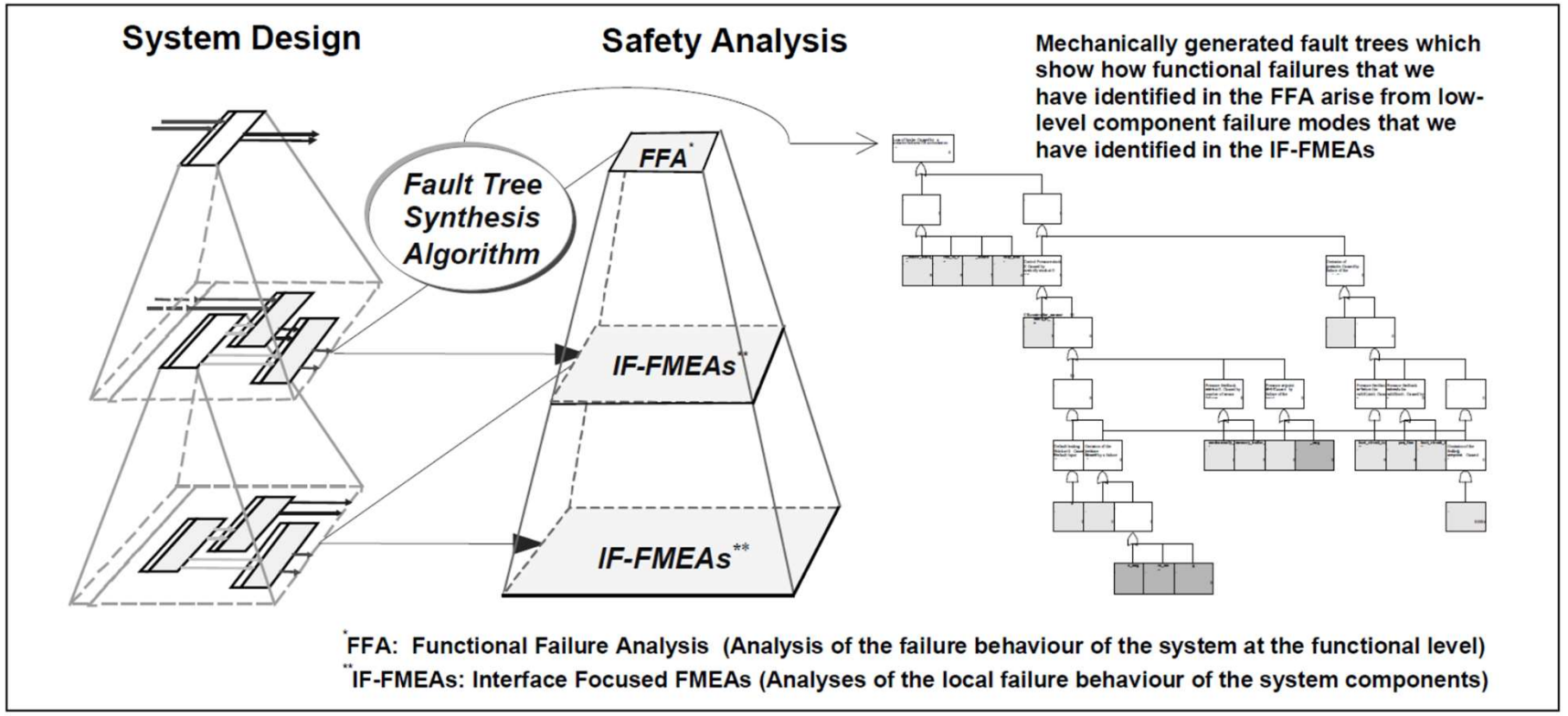


Fig. 1. Overview of Design and Safety Analysis in HiP-HOPS

階層化されたコンポーネントごとにFT(Fault Tree)を作り、コンポーネント間の故障のインターフェースを厳密に決めてシステム全体のFTを構築する手法

事例３：SafeDeML(1)

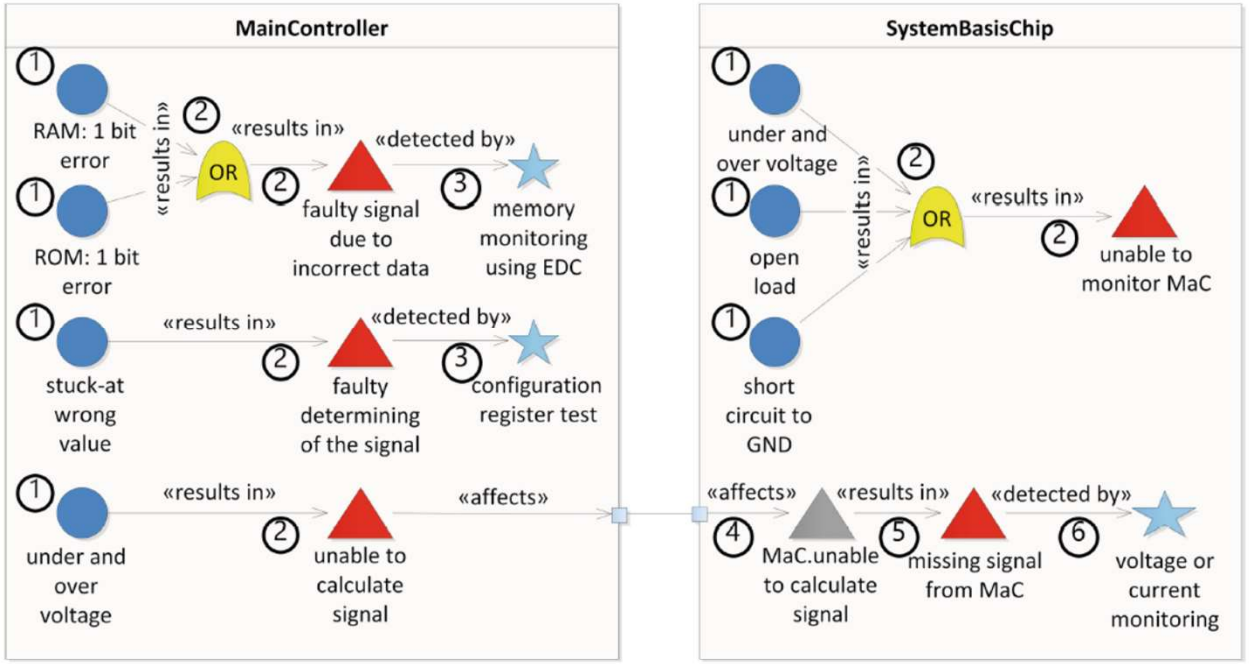


Fig. 8. Excerpt of the brake light system used to validate our modeling methodology. It contains the failure definitions for the *MainController (MaC)* and the *SystemBasisChip (SBC)* The numbers assigned to the elements indicate the different steps in which these elements are added to the fault modeling.

SafeMLを設計、実装の領域にも使えるように拡張した図法というイメージ。
(SafeComp2019で発表)

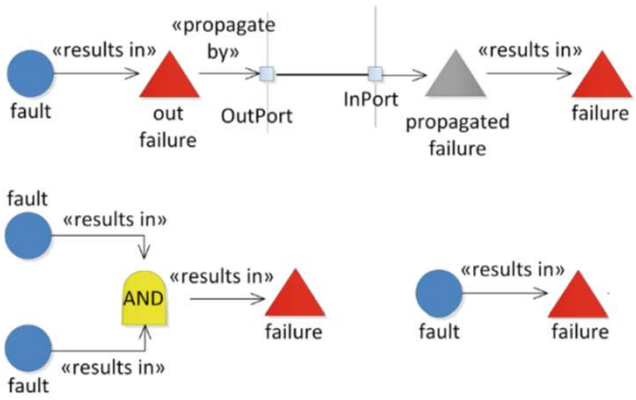
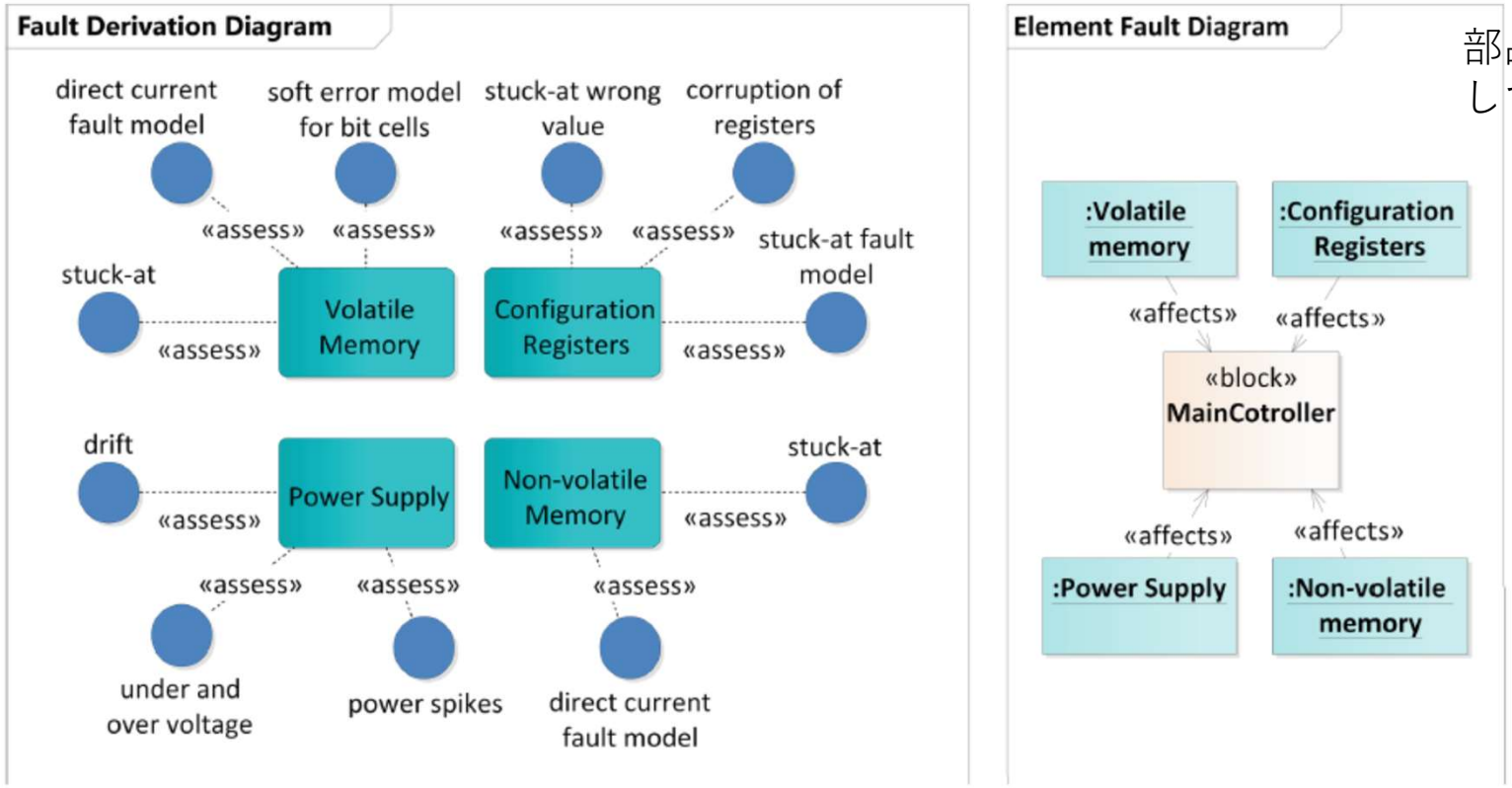


Fig. 4. Possible representations of the SafeDeML::Failure modeling. It shows a horizontal propagation (top), a SafeDeML::Failure with more than one correlated SafeDeML::Fault (left) and a single SafeDeML::Fault leading to a failure.

事例３：SafeDeML(2)



部品の故障モードもモデルとして定義する。

Fig. 9. Fault definitions of the MainController component. On the left side the associations of the faults to the ISO HWParts is shown and on the right side, instances of the HWElements are associated with the MainController block.

SafeDeMLの作図例

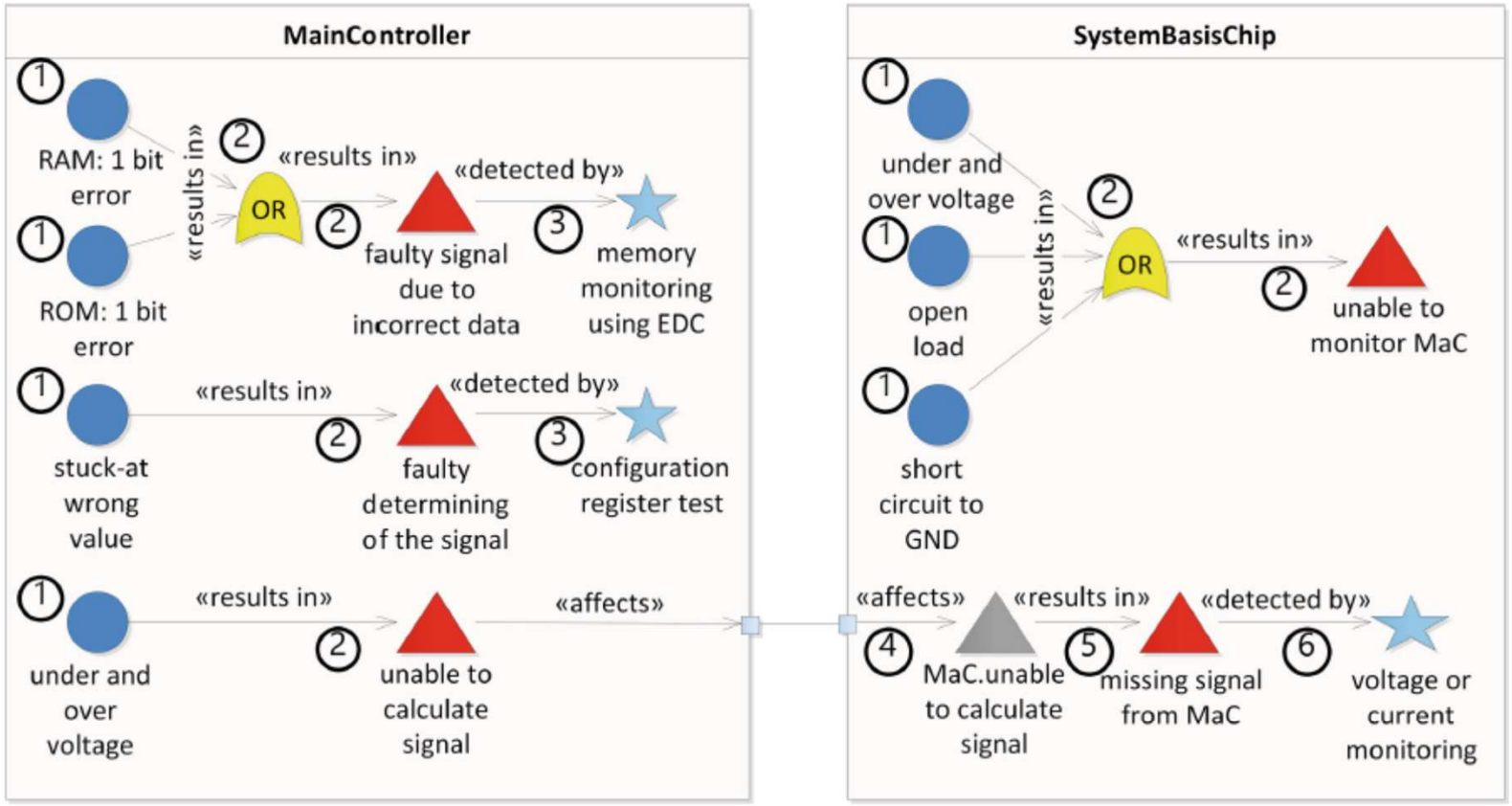
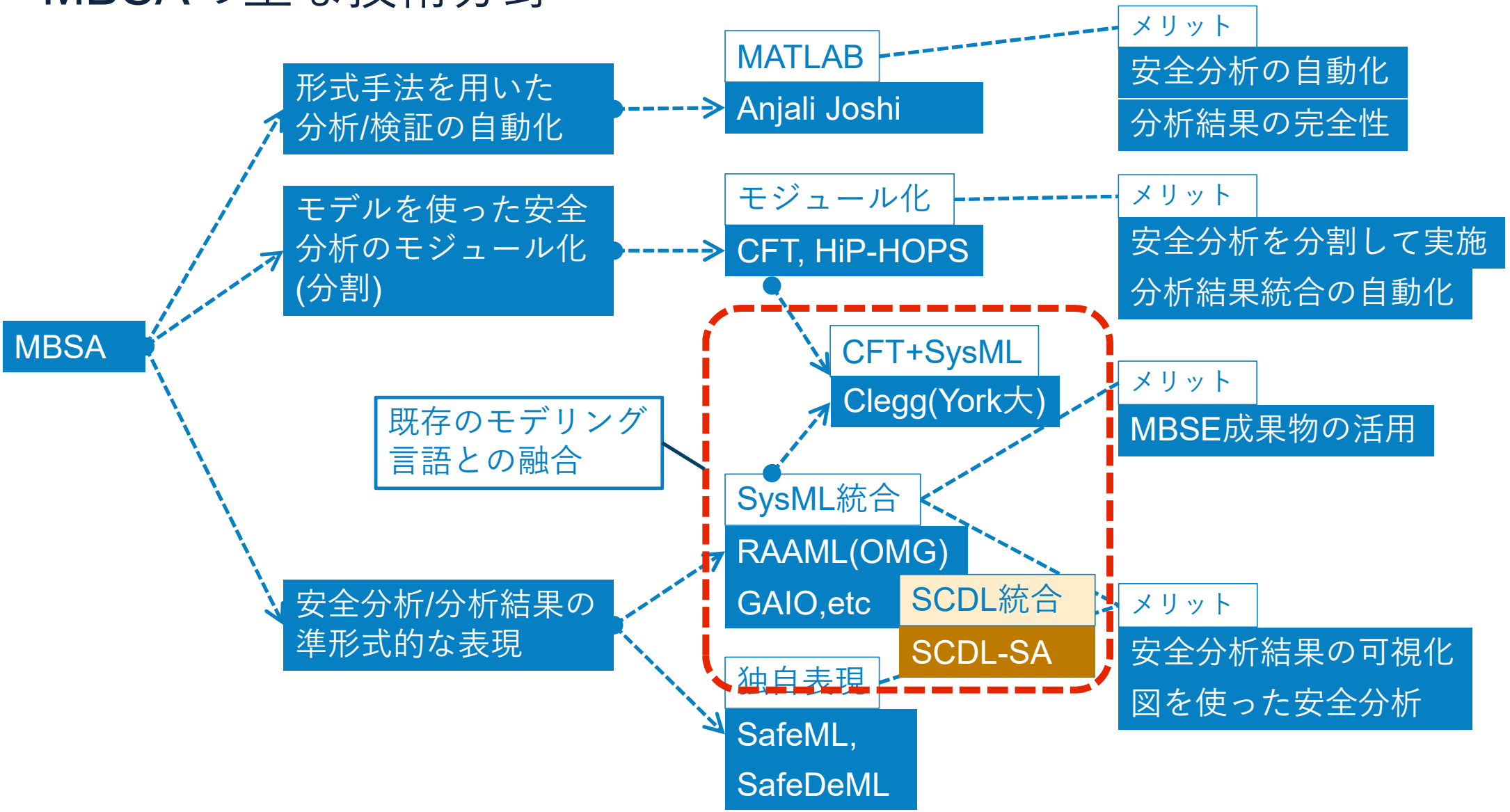


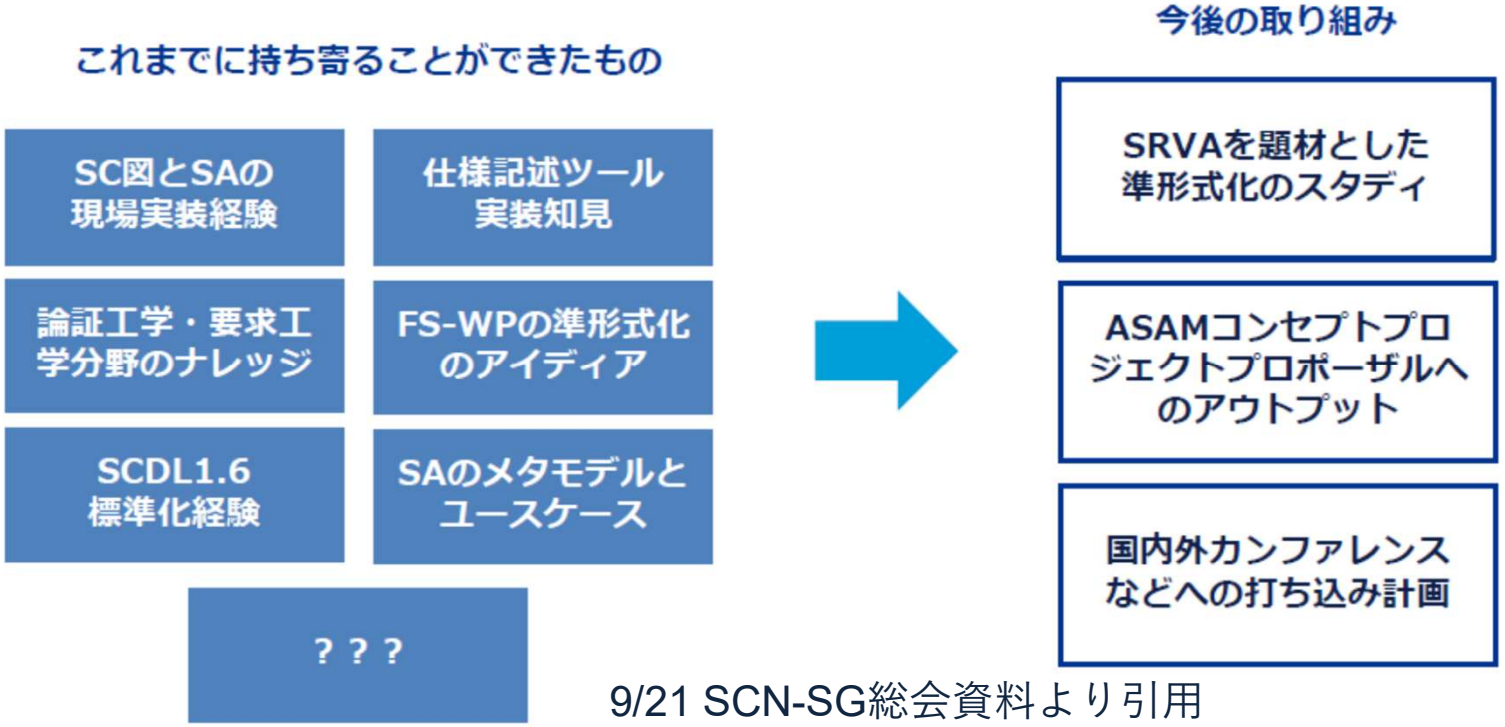
Fig. 8. Excerpt of the brake light system used to validate our modeling methodology. It contains the failure definitions for the *MainController (MaC)* and the *SystemBasis-Chip (SBC)* The numbers assigned to the elements indicate the different steps in which these elements are added to the fault modeling.

MBSAの主な技術分野



4. SCN-SGの取り組み：SCDL-SAの検討状況

- SCDL-SAとは
  - SA = Safety Analysis/Assessment/Argument/Assurance
  - 目標：機能安全の成果物全般を準形式化することによる共通化と理解共有による品質向上/生産性向上。(安全分析(MBSA)に閉じた活動ではない)



9/21 SCN-SG総会資料より引用

SCDL 1.6 ➡ SCDL 1.7案

SCDL1.6では

・SC図の文法を定義した

・SR表の併用を前提としていた

・SAの展開はユーザにおまかせだった

➡

SCDL1.7では

・SC-Diagram

・SR-spec.

・SRVA

の三点セットか・・・

SCDL1.6 WP	項目	SCDL 1.7 WP		
		SC-Diagram	SR-spec.	SRVA
SC図	SR構造	✓		
	エレメント構造	✓		
	SR配置	✓		
	ASIL	✓		
	要求グループ		✓	✓
	グループ間ペアリング		✓	✓
	独立要求	(✓)	✓	✓
	FFI		✓	✓
	FFI要求	(✓)	✓	✓
	I/F	(✓)	✓	
(SR表)	要求ID・ラベル		✓	✓
	自然言語表現		✓	
	タイプ（IF/SM…）		✓	(✓)
	入出力		✓	
	ASIL		✓	
	status		✓	
	トレサビ（上位要求ID）		✓	
(SA)	SRID			✓
	SR			✓
	タイプ			✓
	SRVモード			✓
	SRV影響（incl.SGV）			✓
	SMr（incl.SM）			✓

9/21 SCN-SG総会資料より引用

5. MBSAの難しさ、今後の課題

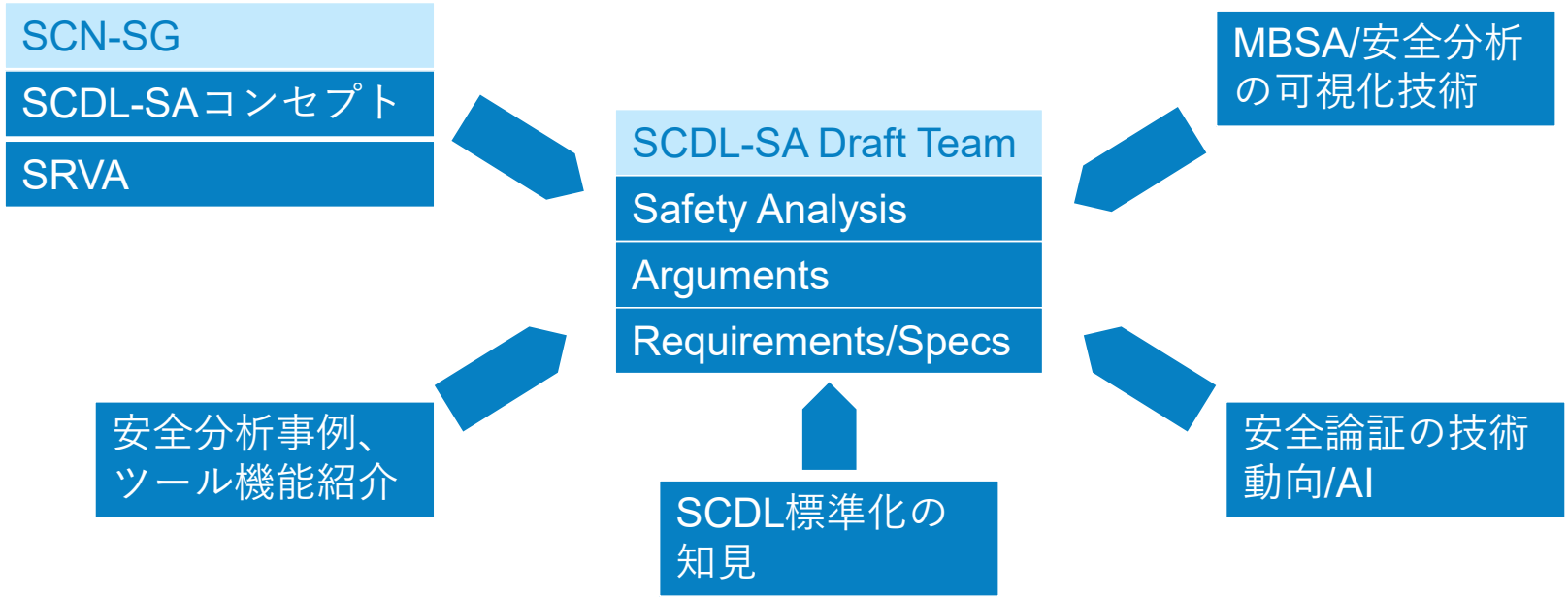
- システム設計の構造と故障の伝播の関係をモデル化しようとするとモデルが複雑化する。

- モデルで扱う情報量(数)が膨大になる
  - 故障をまとめて扱う、省略するなどを適切に行わないと扱いきれない
  - 1つの巨大なモデルを適切に分割して実用的な図を作成しないと利用者が理解しにくい

- モデル化すると、従来の安全分析で省略、簡略化していた記述内容の矛盾が目立ってしまう
  - 例：FMEAとFTAの結果のずれもモデル化すると明白になってしまう

6. 今後の取り組み

- ASAM コンセプトプロジェクトへの提案
  - ASAM庄井様にアドバイスを頂き、運営/技術内容を議論中
- 準形式化のケーススタディ、カンファレンス発表
- MBSAの知見もSCDLに取り込み、より実務で役立つ方法論、図法を目指していきます



統合アシュアランスケースをサポートするSCDLへ

- 業界の関心事がアーキテクチャを含む統合アシュアランスケースに移る中で、安全アーキテクチャの記述を準形式化したSCDLを活用できる場面が増えるのではないか