ASAM Regional Meeting JAPAN 2022

ASAM SCDL Standard V1.6.0 Report

Kiyoshi SASAKI (佐々木 喜好)

June 29, 2022
13:30 – 17:00 JST

ASAM Association for Standardization of Automation and Measuring Systems

Agenda

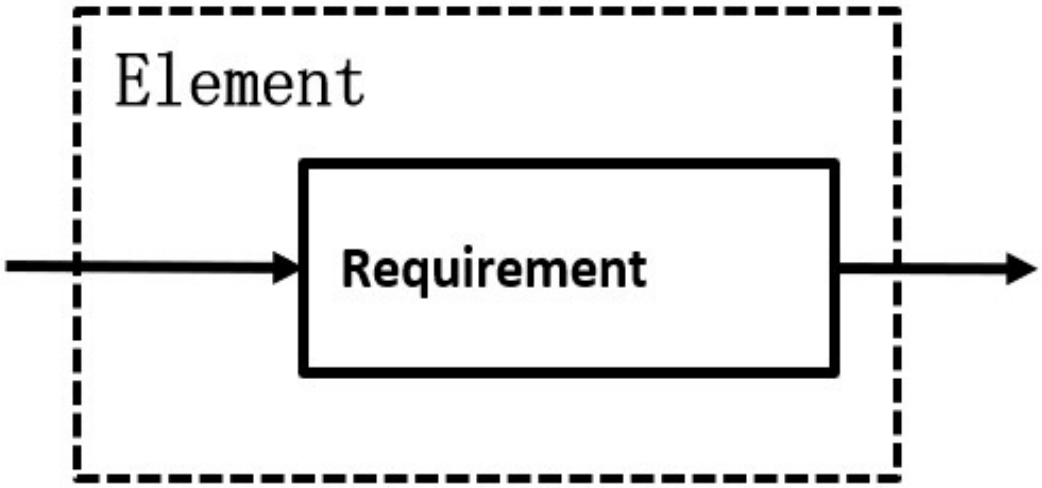
1	ASAM SCDLとは何か
2	なぜASAM SCDLが必要とされるのか
3	ASAM SCDL表記法の例
4	注目の話題

1. ASAM SCDLとは何か

ASAM SCDLとは何か

モデリング言語

- **ASAM** Safety Concept Description Language（安全コンセプト記述言語）
- グラフィック表現に基づく機能ブロック図



ASAM SCDLとは何か

安全のため

- 安全要求や安全コンセプトを記述するためのモデリング言語
  - ISO 26262:2018の意図を実現

- 特に次のような要件をサポート
  - 要求
  - 要求間の相互作用（インタラクション）
  - エレメント
  - エレメントへの要求の配置
  - ASIL割り当て
  - デコンポジション
  - 無干渉

ASAM SCDLとは何か

ISO 26262

- ASAM SCDLは, ISO 26262:2018で規定されている以下に関連する要件の効果的／効率的な実装をサポート

-	第３部	７節： 機能安全コンセプト
-	第４部	６節： 技術術安全コンセプト
-	第５部	６節： ハードウェア安全要求の仕様 ７節： ハードウェア設計
-	第６部	６節： ソフトウェア安全要求の仕様 ７節： ソフトウェアアーキテクチャ設計
-	第８部	６節： 安全要求の仕様および管理
-	第９部	５節： ASILテーラリングのための要求のデコンポジション ６節： エレメントの共存に関する基準 ７節： 従属故障の分析 ８節： 安全分析

2. なぜASAM SCDLが必要とされるのか

なぜASAM SCDLが必要とされるのか

第一の動機

- ISO 26262では，要求仕様に**準形式記述**が求められている.
  - ASIL C / ASIL D では強く推奨 ”++“ (例：Part 8-6)

表 1 ― 安全要求の仕様化の手法

Ref. ISO 26262-8:2018

手法		ASIL			
		A	B	C	D
1a	要求仕様の非形式記述	++	++	+	+
1b	**要求仕様の準形式記述**	**+**	**+**	**++**	**++**
1c	要求仕様の形式記述	+	+	+	+

“++” 記載された手法を強く推奨することを示す

“+” 記載された手法を推奨することを示す

なぜASAM SCDLが必要とされるのか

第一の動機

- ISO 26262が求める**準形式記述**とは？

手法	文法	意味論	記述手法の例
非形式記述 [3.80]	定義は完全とは 限らない	定義は完全とは 限らない	自然言語;
準形式記述 **[3.149]**	**完全に** **定義されている**	**定義は完全とは** **限らない**	**Structured And Design Technique(SADT);** **Unified Modeling Language (UML);** **System Modeling Language (SysML);**
形式記述 [3.63]	完全に 定義されている	完全に 定義されている	Z notation (Zed); NuSMV (symbolic model checker); Prototype Verification System (PVS); Vienna Development Method (VDM).

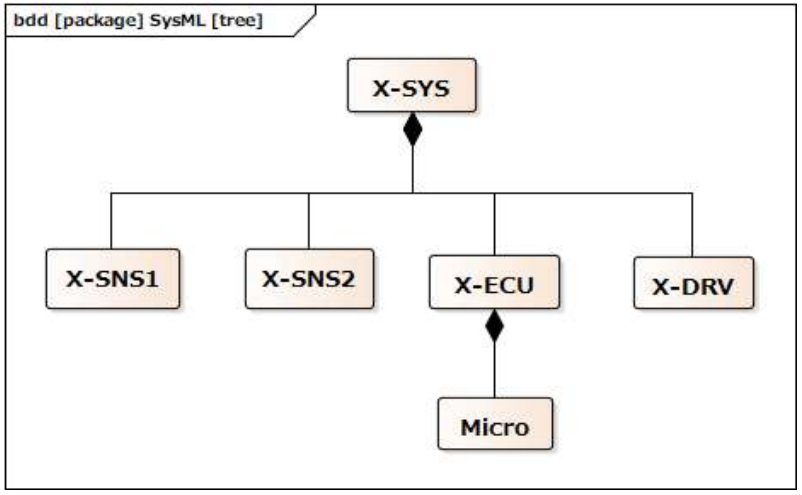
Ref. ISO 26262-1:2018; ISO 26262-8:2018

なぜASAM SCDLが必要とされるのか

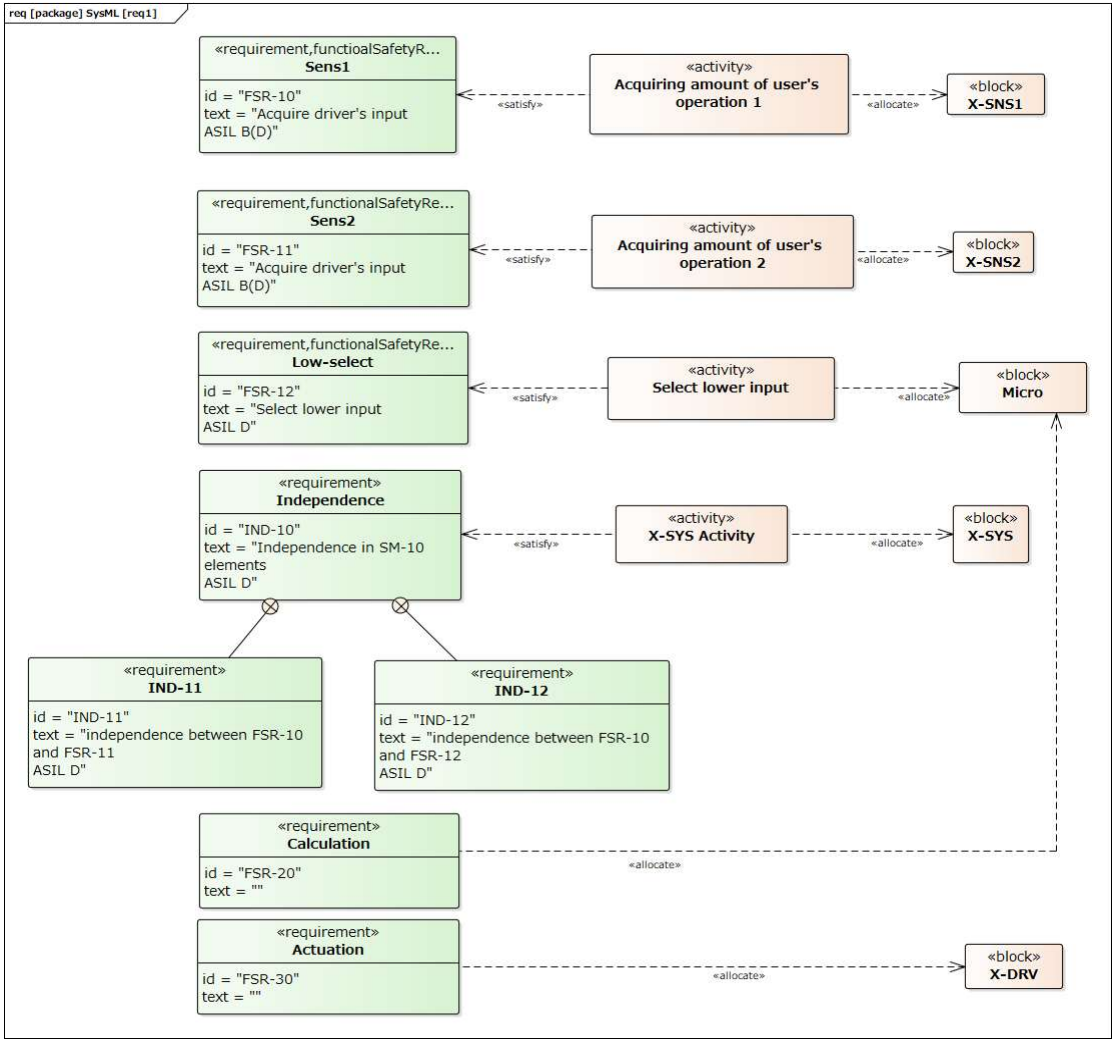
第二の動機

- **SysML**による安全コンセプト記述

冗長センサー入力による
安全アーキテクチャ例



構造図



要求図

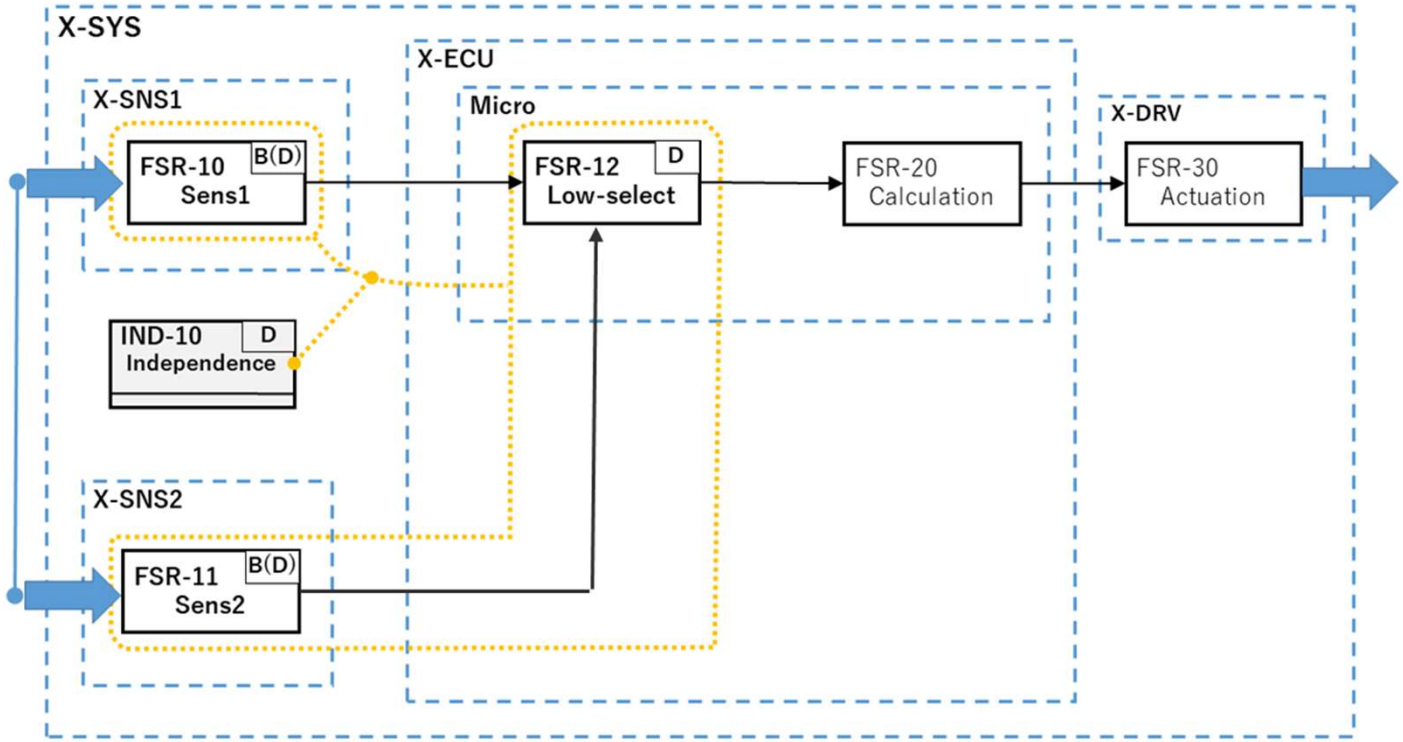
ASAM

なぜASAM SCDLが必要とされるのか

第二の動機

ASAM SCDLによる安全コンセプト記述

冗長センサー入力による安全アーキテクチャ例　(SysMLの例と同じ)



ASAM

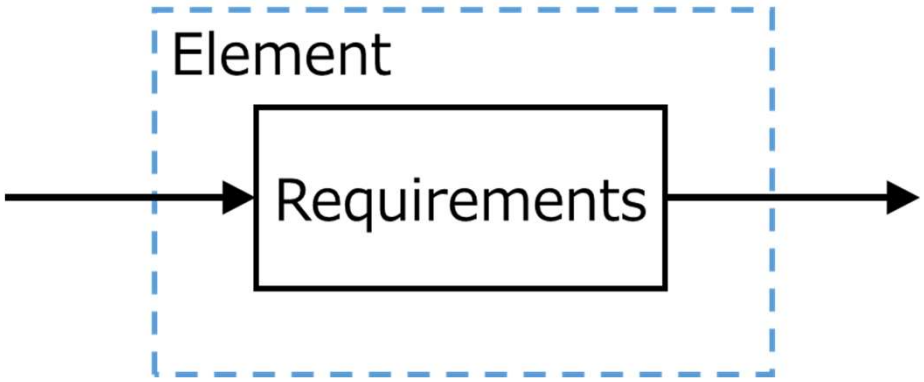
なぜASAM SCDLが必要とされるのか

第二の動機

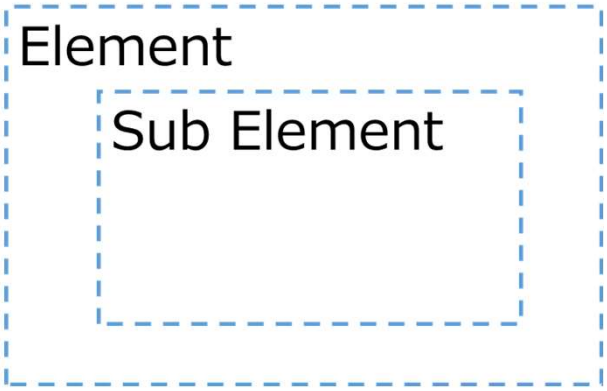
■ ASAM SCDLは，**アーキテクチャを直感的に理解**するのを助ける

おなじみのブロック図の一種

- 要求はエレメントに重ねることができる
- エレメントは階層構造を持つことができる



要求とエレメントの重ね合わせ



エレメントの階層構造

3. ASAM SCDL表記法の例

ASAM SCDL表記法の例

記号の定義

■ 要求（Requirements）

要求は以下を表す

- 機能
- 役割
- 動作

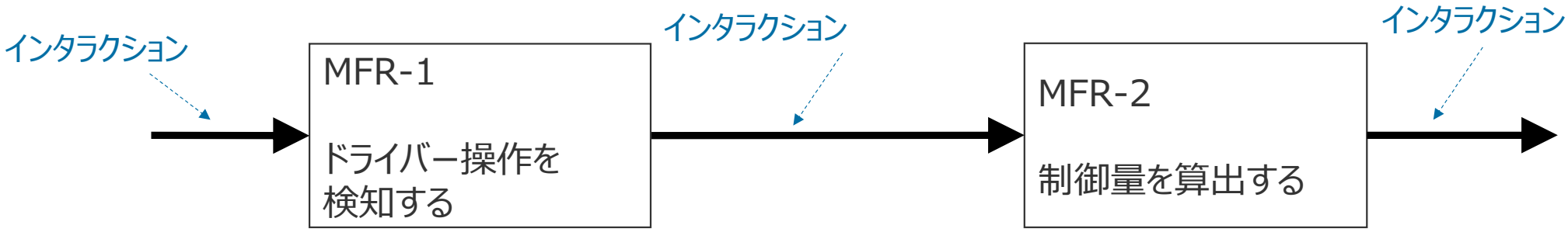
ASAM SCDL表記法の例

記号の定義

- インタラクション（Interactions）

  インタラクションは以下を表す

  - 情報
  - 信号
  - 要求間のメッセージ

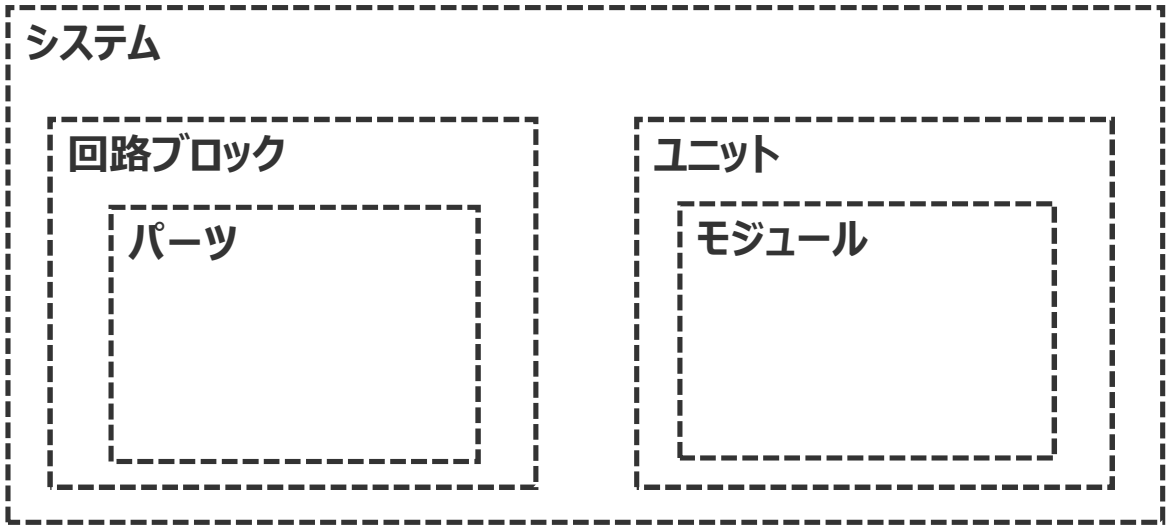


ASAM SCDL表記法の例

記号の定義

■ エレメント（Elements）

- エレメントは以下を表す
  - システム，コンポーネント，ユニット，モジュール，パーツ，回路ブロックなど
- エレメントは入れ子構造を表すことができる

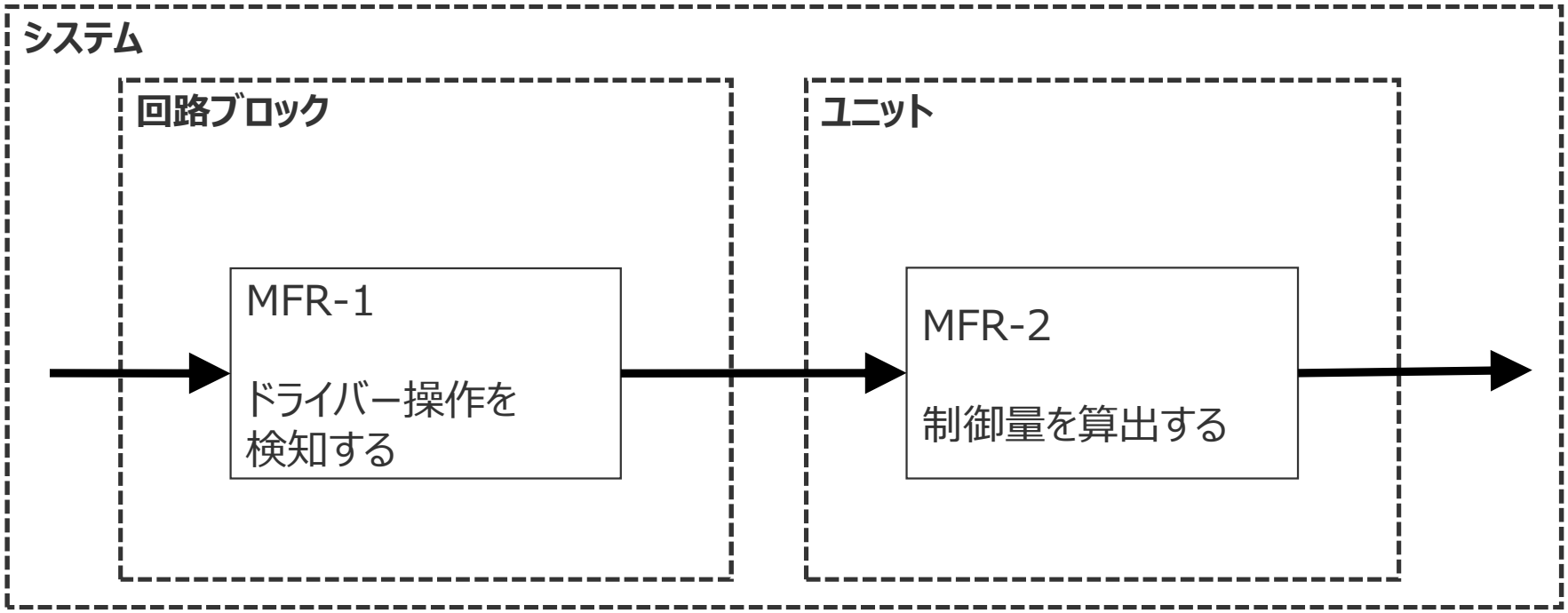


ASAM SCDL表記法の例

記号の組み合わせ

- エレメントへの要求の配置

  要求は，要求を実現するエレメントへ配置できる

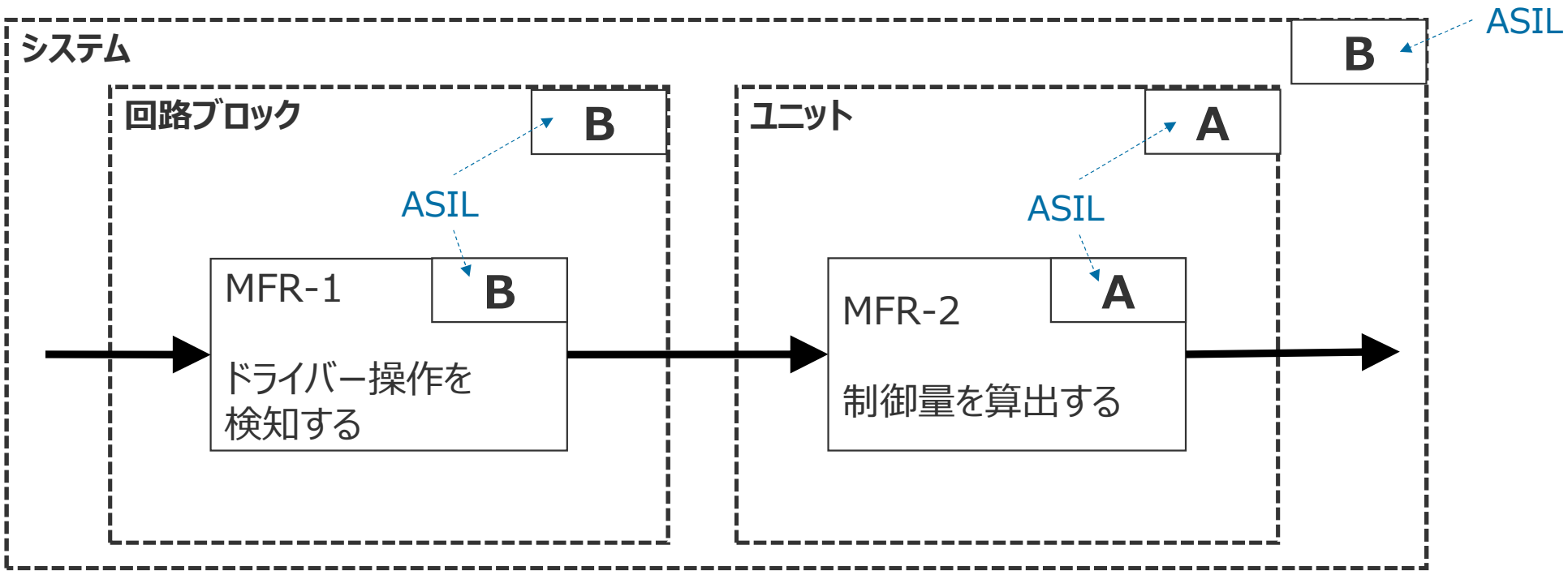


ASAM SCDL表記法の例

記号の組み合わせ

- ASIL割り当て

  ASILは要求とエレメントに割り当てることができる



ASAM SCDL表記法の例

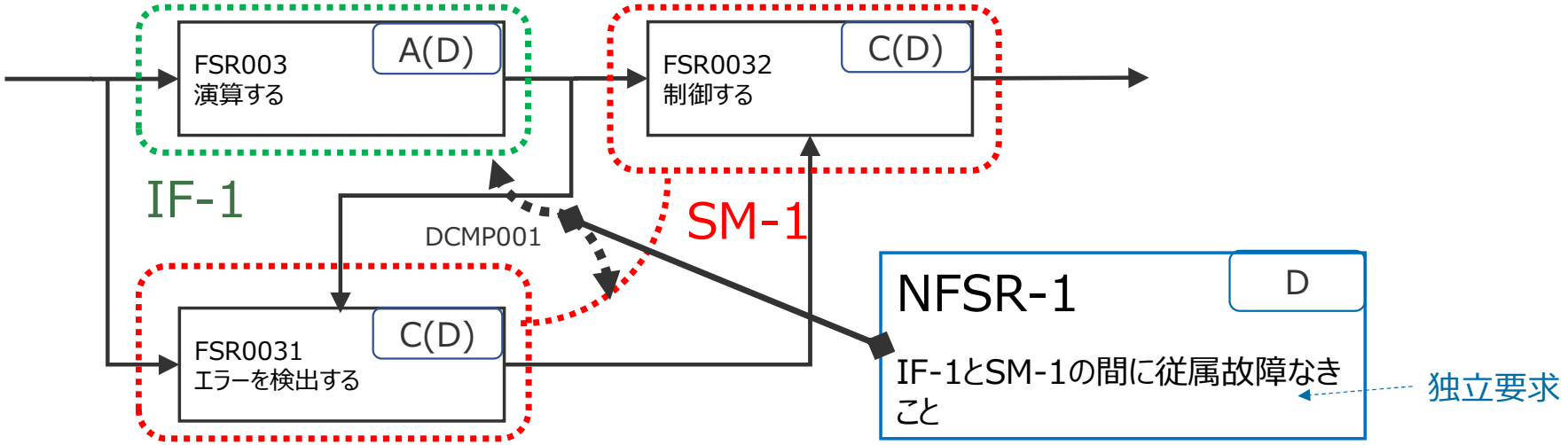
記号の組み合わせ

■ デコンポジション（Decomposition）

デコンポジションは独立要求の記号といくつかの記号の組み合わせで表現することができる

例）

この図は，要求グループ “IF-1”と要求グループ “SM-1” 間の独立のための要求を表している



ASAM SCDL表記法の例

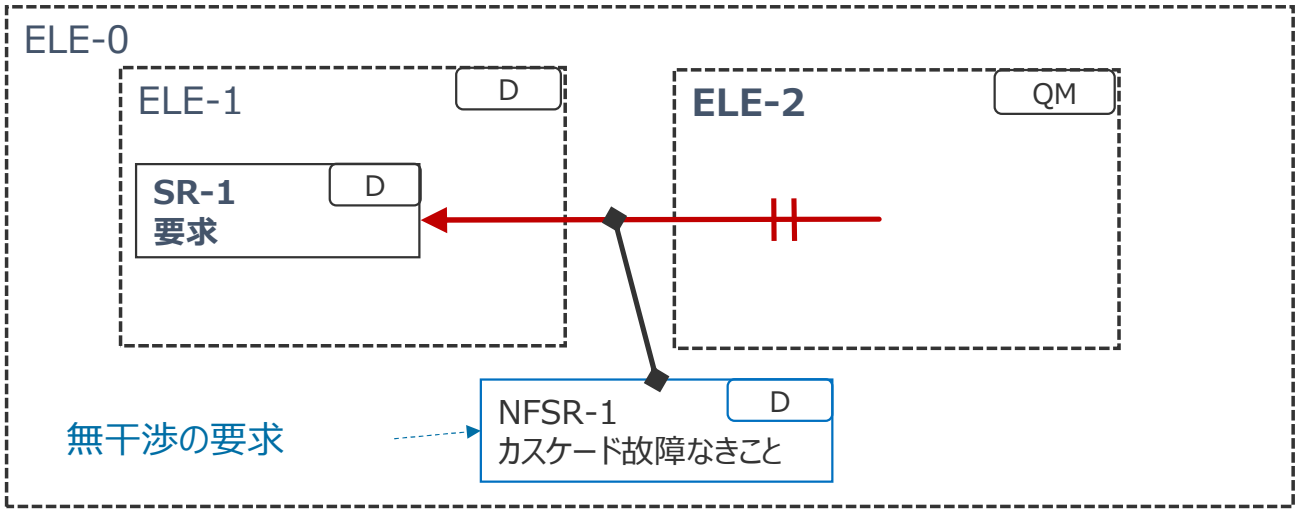
記号の組み合わせ

■ 無干渉（Freedom From Interference）

無干渉はエレメントの共存のための要求を表現することができる

例）

この図は，ELE-2エレメントの故障が「SR-1要求」に影響を与えてはならないことを示している.



4. 注目の話題

新しい取り組み

安全コンセプト記法研究会（SCN-SG）の紹介

SCN
Safety Concept Notation - Study Group

アクセス&合流をお待ちしております

SCN-SG　検索

会費や制約などございません

- 情報発信
- お問い合わせ

ASAM

SCN-SG SOTIF拡張SWG活動

背景

ISO 21448のLCはFS-LCに大きなインパクトとなる可能性がある

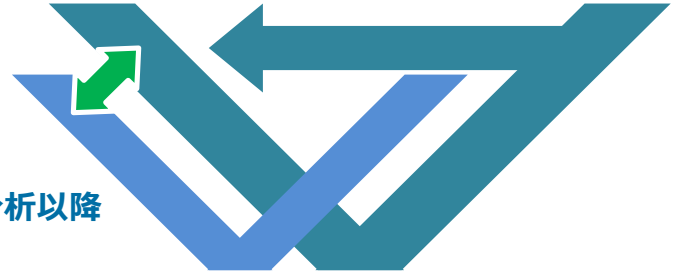
活動目標

FSから参照されるIFアーキを安全要求ベースで論じることで効果的効率的なインタラクションが可能となるか検証する

（１）SOTIF/FSのプロセス連携ケーススタディ
（２）拡張SCDL記法／文法追加の要否検討

SOTIF/FS communication:
SRベースのインタラクションが望ましい

機能安全ライフサイクル（FS-LC）：
IFアーキ修正が行われた場合には影響分析以降の再活動が必要になる



SOTIF-LC：
シナリオベースのバリデーションテストやフィールドオペレーションによる大きなフィードバックループがが基本となる

活動概要

2022年4月キックオフ
メンバー14名（OEM, サプライヤー, ツールベンダ, 団体等で構成）

LC：Life Cycle（ライフサイクル）
FS：Functional Safety（機能安全）
IF：Intended Functionality（意図機能）
SOTIF：Safety Of The Intended Functionality（意図した機能の安全性）
SCDL：Safety Concept Description Language（安全コンセプト記述言語）

In conclusion

- ASAM SCDLは，システムアーキテクチャのためのモデリング言語の1つである.
- ASAM SCDLは，ISO 26262の安全開発を支援する.
- ASAM SCDLは，直感的で理解しやすい表記法である.
- ASAM SCDLは，まだまだ進化を続けています.

Thank you !