

SCN-SGとSCDLの紹介

@ASAM Regional Meeting in Japan
20180425

安全コンセプト記法研究会
山下修平 (DNV GL)

山下自己紹介

- 1983年日産自動車に入社、30年にわたりエンジン電子制御システムの開発などに従事
- この間2005年より自動車技術会(JSAE)機能安全分科会長に就任し、ISO 26262策定活動に参画、関連活動を主導
- 2013年より欧州系認証機関に移り、テクニカルディレクタとして国内外自動車業界における当該規格対応で広範囲に活動
- 2014年4月より現職 (DNV GL BAJ シニアディレクタ)
- **SCN-SG** (安全コンセプト記法研究会) チェアマン



SCN-SGとSCDL

■ SCN-SG (Safety Concept Notation Study Group)

- ミッション

安全アーキテクチャを効果的・効率的に設計，分析，レビュー，共有，説明するための記法SCDLを広く世間に提供していく

- モチベーション

ISO 26262の効率的実装の一助となる方法論を検討し、さらに当該規格のスコープである自動車分野に限定せず、大規模システムから組み込みソフトウェアに至る各レベルの、安全アーキテクチャの合理的な表現法を深ぼり共有する

■ SCDL (Safety Concept Description Language)

- ISO 26262の規格意図に着目した安全コンセプト記述用の準形式言語

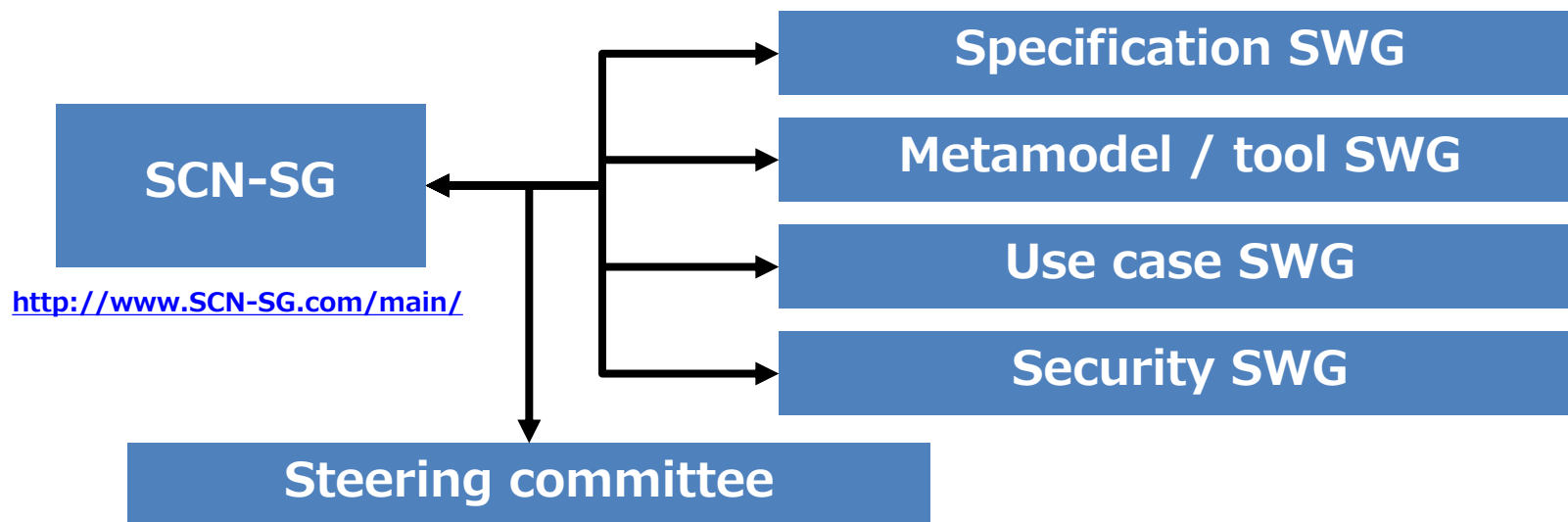
SCN-SGの発足のいきさつと活動内容

- **SCN-SG**発足の背景：自動車電子制御分野における安全設計の指針を提供する規格として広く普及・定着したISO 26262の、より効率的・効果的実装を目指すエンジニアが自発的に参加する研究会として発足した
- 活動のスコープ：安全要求と安全コンセプトの仕様記述，モデリング，分析法，論述法，シンボルやダイアグラムの最適化，他の記述法や分析法との整合の研究
- 実績：
 - ユースケースを含む**SCDL**仕様書Ver.1.2を公開中
 - オープンカンファレンス開催など4年間にわたる活動実績
 - SAE,VDAカンファレンスにおける発表等

SCN-SGの組織

■ SCN-SGの概要：

- 日本国内中心に約50の会社・団体からの参画
- 約100名の登録メンバ
- 個別の案件を議論する4つのサブワーキンググループ



SCDL標準化の動機

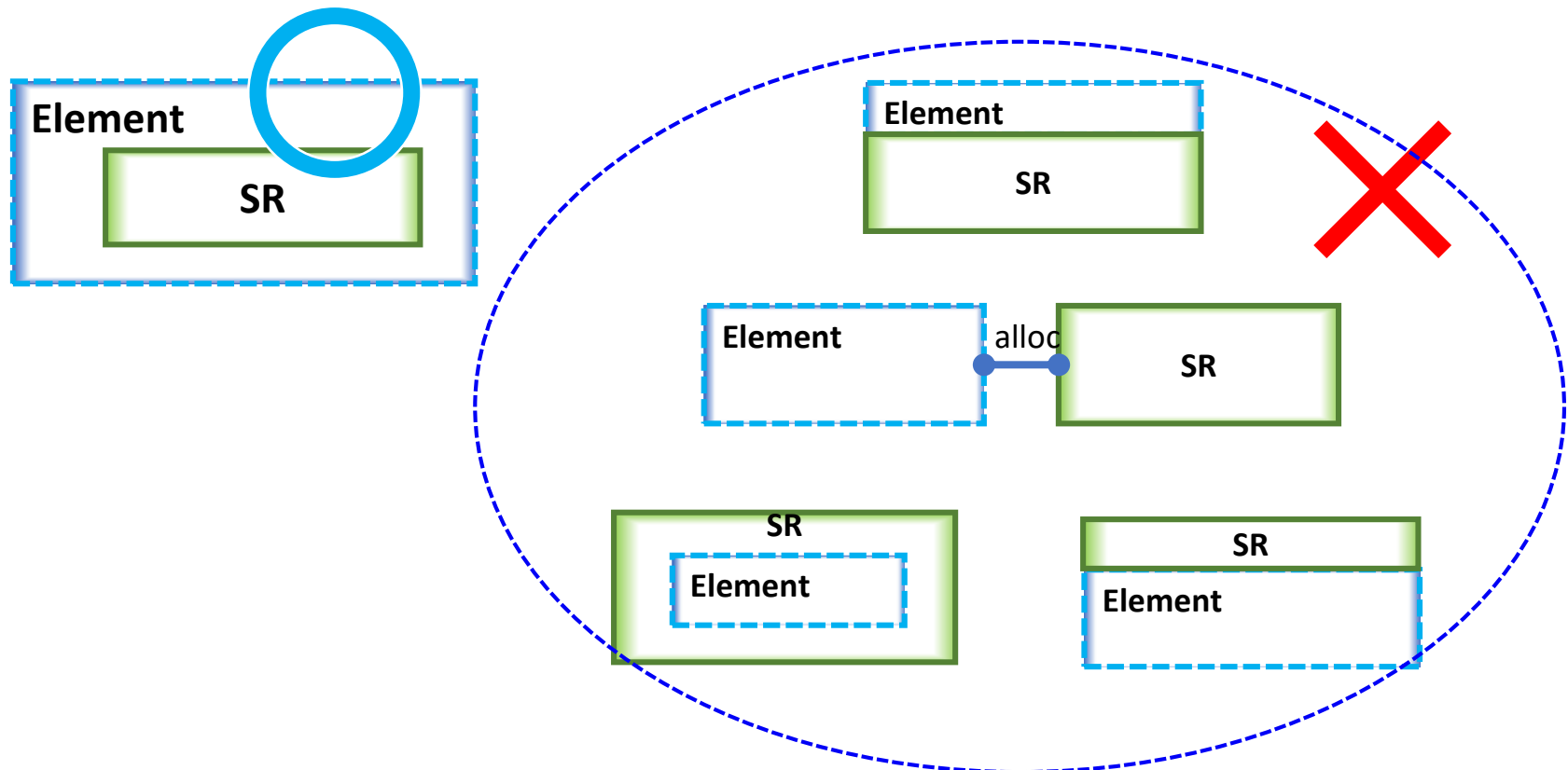
- **SCDL**はISO 26262の効率的・効果的実装の一方策として、実プロジェクトやトレーニングの現場で広く活用されるようになってきた
- これに合わせて各方面で支援ツールの開発も進んでいる
- この状況に対して、記法を支える**SCDL**言語仕様の公共性と中立性を確保し、将来にわたって記述ルール（文法）の一貫性や、ツール間連携におけるデータの互換性を確保すべきとの意見が挙がり始めた
- 標準化団体の枠組みを活用した規格化を検討することになった

SCDLのユースケース

- ISO 26262が準形式記述を推奨している安全要求仕様と、これを物理層アーキテクチャに配置した安全コンセプトをダイアグラム表記する場合に使用することを想定している
- 具体例：システム設計におけるFSC（機能安全コンセプト）やTSC（技術安全コンセプト）、ハードウェア設計やソフトウェア設計における安全アーキテクチャの記述
- 文法の検討事例：次ページ以降で解説

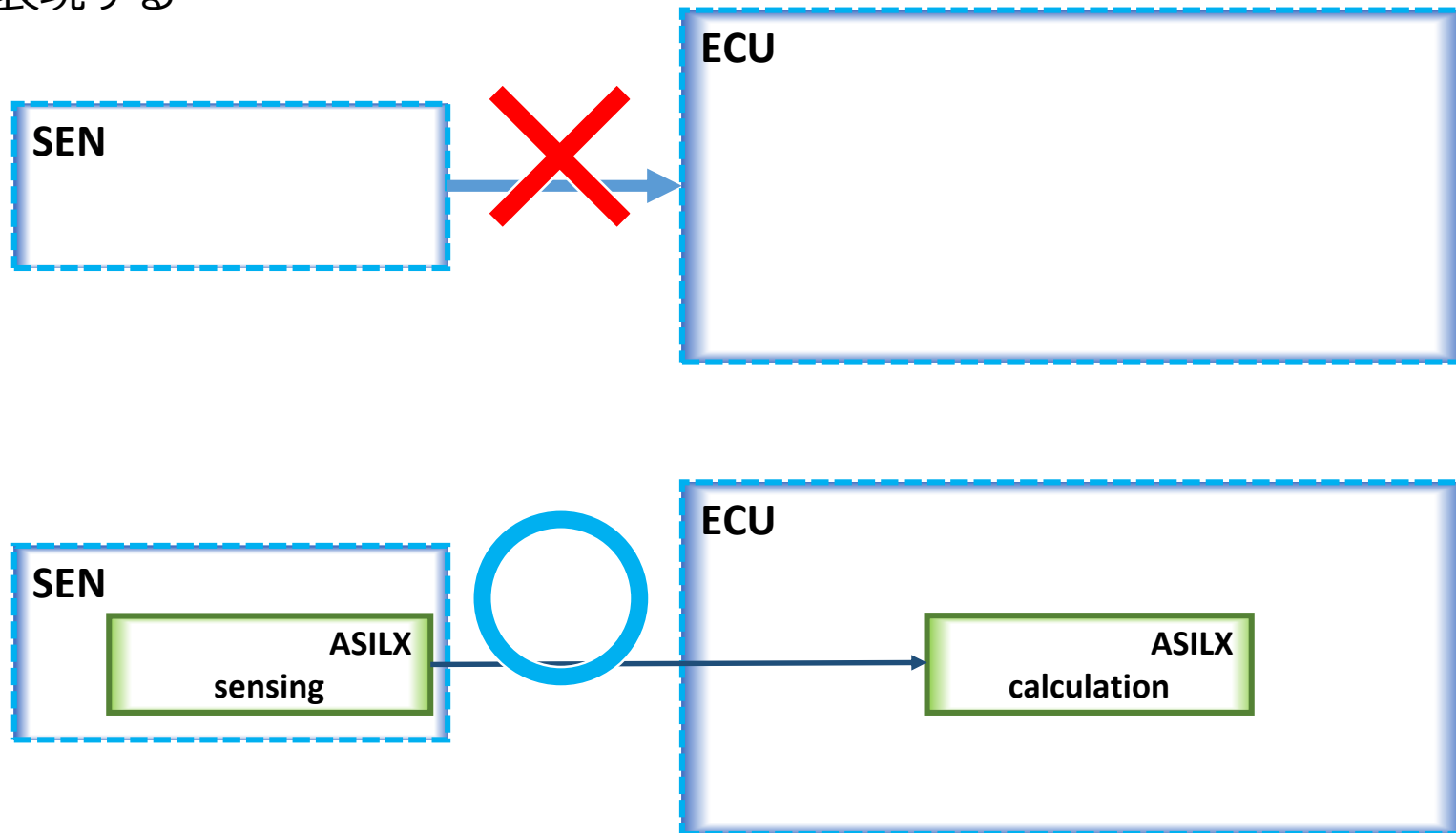
SCDL文法の事例 1

- エlement（コンポーネントなど）に対する安全要求(SR)配置はエlementの内側に安全要求のブロックを収める



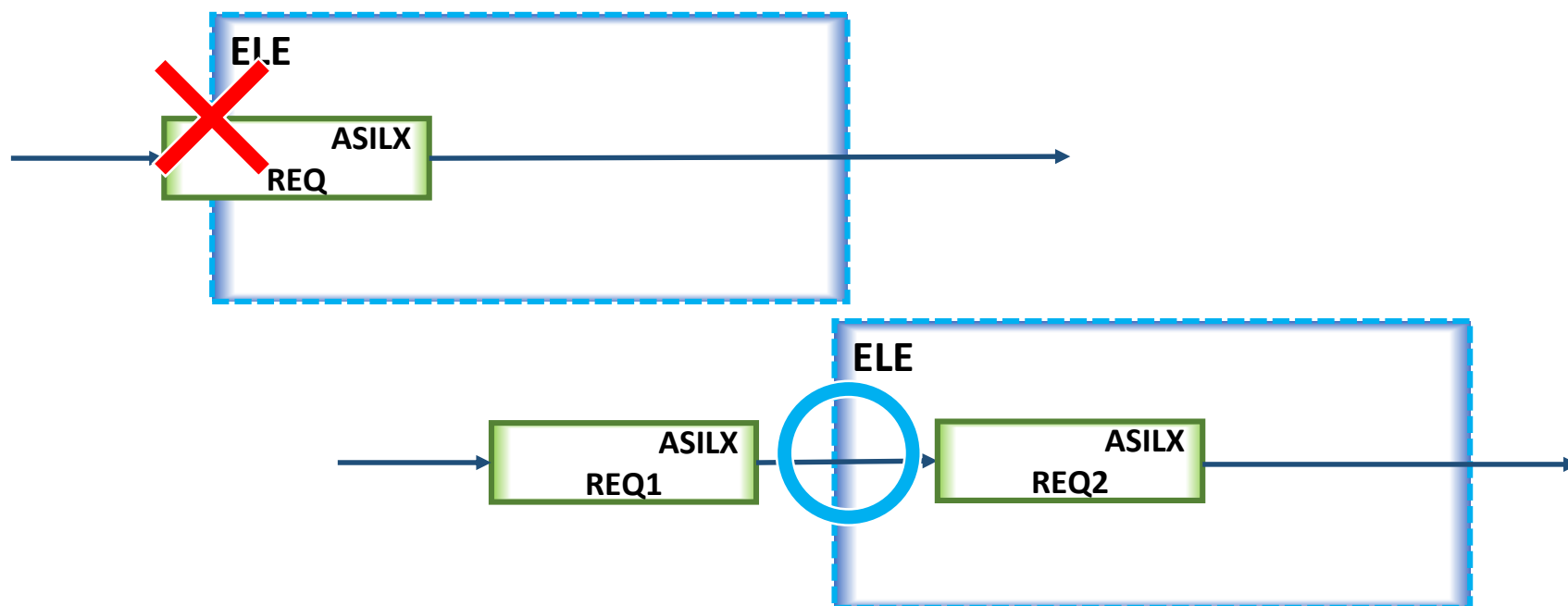
SCDL文法の事例 2

- 接続関係はエレメント間の物理的な結線ではなく、要求間の依存関係を表現する



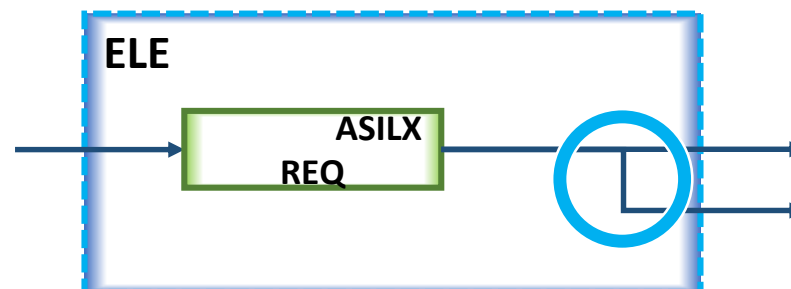
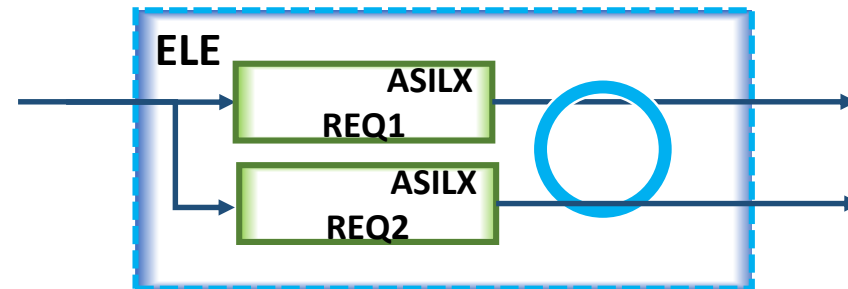
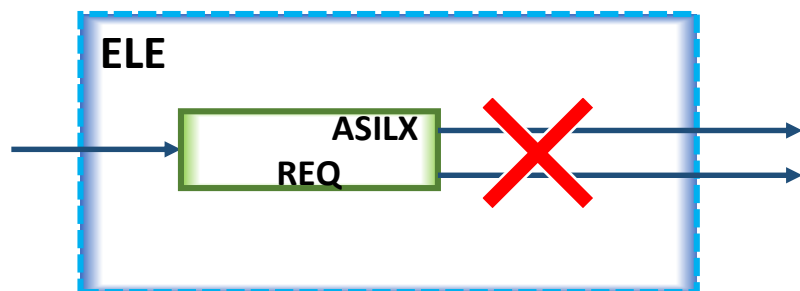
SCDL文法の事例 3

- 要求の適切な粒度を確保する為に、要求はエレメントの境界をまたいではならない。エレメントの内外の要求に分解して配置する。



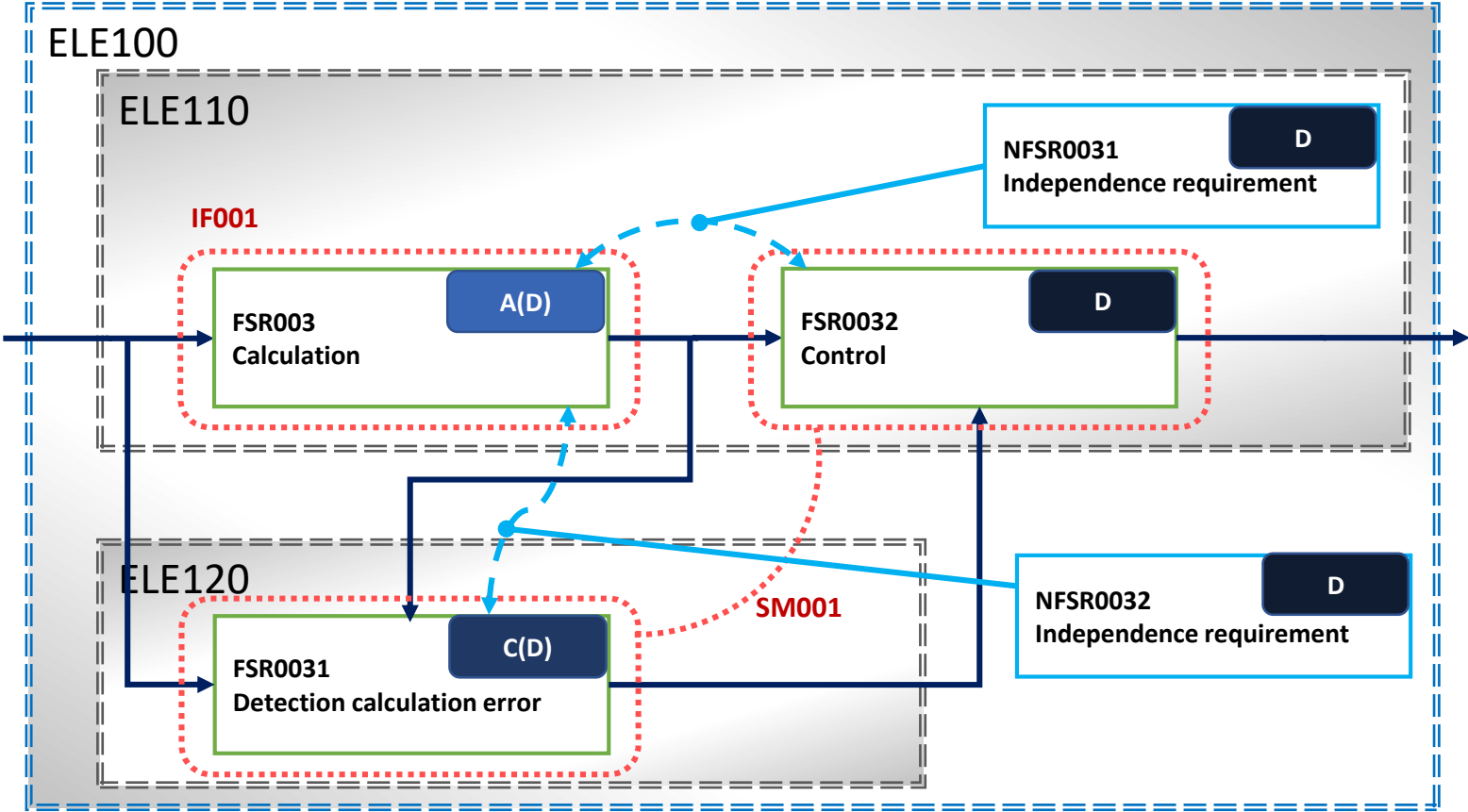
SCDL文法の事例 4

- 要求の適切な単位性を確保する為に、要求は複数の出力を持たない。要求を適切に分解する、または出力を分岐する。



SCDL文法の事例 5

- SM（安全機構）にデコンポジションを適用した場合の表記例



ASAM標準化で目指すもの

- **SCDL**の言語仕様を公共性の高い団体に託すことで、高い中立性と将来にわたる一貫性を確保したい
- このことにより、ISO 26262が求める安全コンセプト仕様の記述法の選択肢の一つとして、**SCDL**を定着させたい
- さらにグローバルな自動車業界からの意見を反映して、一層使いやすい言語仕様に磨き上げることを目指したい

ASAM標準化で得られるメリットの想定例

- OEMの皆様にもたらす利点：言語仕様が安定することにより、複数のシステムにまたがる協調制御の安全アーキテクチャを論じる際の仕様記述共通語の選択肢幅拡大
- サプライヤの皆様にもたらす利点：社内外資料における安全アーキテクチャ記法の共通化による、受け渡し工数削減や仕様誤認識によるヒューマンエラーの低減
- モビリティ・ソサエティにもたらす利点：モビリティと外界の接続が急速に増加する自動運転時代において、安全アーキテクチャを扱う共通言語としてドメイン間の敷居を下げることに對する貢献

-
- ご清聴ありがとうございました
 - ご意見、ご提案または質問はありますでしょうか？