

SCDLの背景と標準化

@ASAM Regional Meeting Japan, 2019
June, 27th 2019

SCN-SG
Shuhei YAMASHITA
(DNV GL)

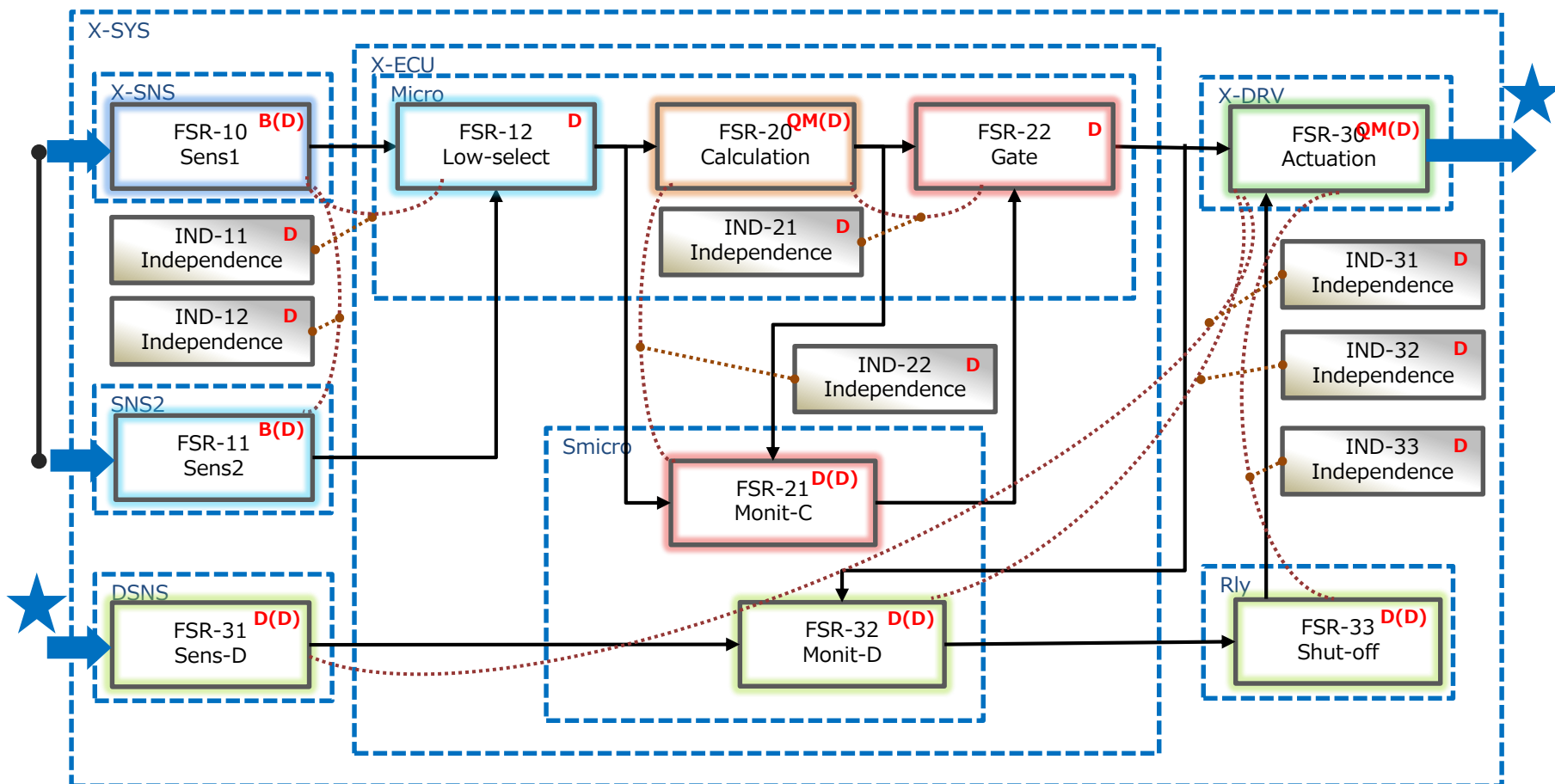
SCDL?

Safety Concept Description Language



- 自動車用機能安全規格ISO 26262の規格意図に忠実な**安全コンセプト記述言語**
- 任意団体**SCN-SG**が言語仕様を策定し公開している
- 日本国内を中心に順調に普及してきている

SCDLによる安全コンセプト表記例

■ FSC (機能安全コンセプト) の構築事例



ISO 26262実装初期の取り組みと反省点

- 規格のセミフォーマル記述要件から
SysML等での安全要求仕様作成の取り組みが行われた
- 
- 共通記述ルールの不在による
汎用言語ならではの表現のバラエティー問題が発生した
- 
- 反省点：規格審議の中でISO 26262の意図に特化した
統一表現を議論すべきだった

SCDL誕生 → 草の根運動に発展

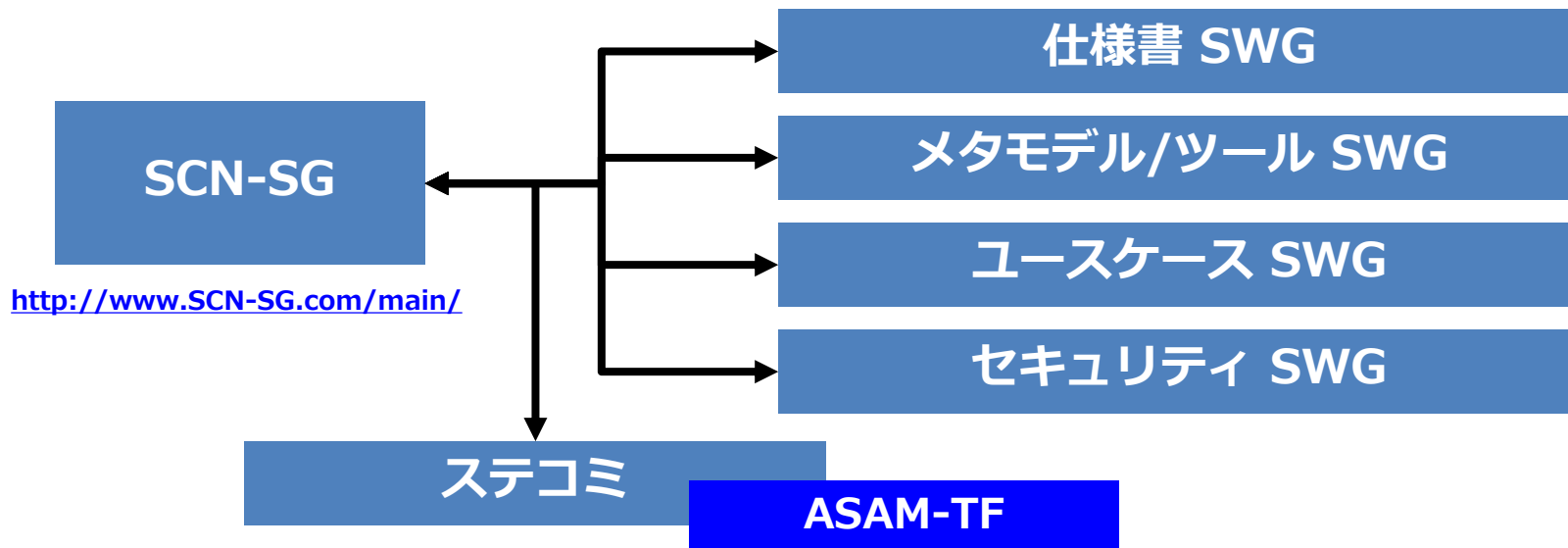
- 安全コンセプトのダイアグラムの書き方ガイドとして誕生
- UML, SysML エキスパートとの出会い
- 言語仕様化活動への賛同者が合流



- SCN-SG（安全コンセプト記法研究会）が発足
- SCDL（安全コンセプト記述言語）仕様の検討を開始

SCN-SG

- SCN-SG (Safety Concept Notation Study Group)
 - SCDLの仕様やユースケースを研究し提供
 - ISO 26262の効率的実装を支える方法論の検討
 - And more..



パラダイムシフトの中の機能安全

- **モビリティの多様なパラダイムシフトが進行中**
 - **機能安全は自動運転の基礎工事**
 - **機能安全実装の高効率化は緊急課題**

- **ISO 26262 第二版が発行された（2018）**
 - **SA,DFAに加えてFSC,TSCがCR対象に**
 - **主要WPのより厳格な規格準拠性が問われる**
 - **セミフォーマル対応も重要**

FSC : Functional Safety Concept
TSC : Technical Safety Concept
CR : Confirmation Review
SA : Safety Analysis
DFA : Dependent Failure Analysis
WP : Work Product

セミフォーマルとしてのSCDL

- SCDL は汎用セミフォーマルと異なりセマンティクスを固定

仕様記述メソッド	シンタクス	セマンティクス
インフォーマル	定義は完全とは限らない	定義は完全とは限らない
‘汎用’ セミフォーマル	完全に定義されている	定義は完全とは限らない
‘SCオリエンテッド’ セミフォーマルとしてのSCDL	完全に定義されている (メタモデル等による)	完全に定義されている (ISO 26262のコンテキストによる)

SCDL の活用レベル

■ SCDL はさまざまなレベルでの普及が進んでいる

レベル		代表的な使われ方
1	挿絵	<ul style="list-style-type: none">・ ISO 26262 のロジックや安全メカニズムの図解・ 教育用途などで使用する
2	システム図	<ul style="list-style-type: none">・ システム構成の図示に用いる・ SysMLなどのシステム仕様記述言語と併用する
3	セミフォーマル記述	<ul style="list-style-type: none">・ 安全コンセプトの仕様記述の手段として用いる
4	モデリング	<ul style="list-style-type: none">・ 安全アーキテクチャのモデリング手段として用いる

SCDL標準化議論の背景

- SCDLはISO 26262の効果的実装の一方策として、
実プロジェクトで活用されるようになってきた
- 言語仕様の公共性に配慮し、記述ルールの一貫性や、
データ互換性を将来にわたって確保すべきとの指摘が出た



- 標準化団体活用の検討を開始（ISO, SAE, OMG等）
- この中で自動車領域の標準化団体としてASAMが候補と
なった

ASAMにおけるSCDL標準化

- ここから先は佐々木さんにバトンタッチ