

Concept project proposal for SCDL Next Gen. SCDL-SA (Safety Analysis/Arguments)

Nobuaki Tanaka / OTSL Inc.
SCN-SG SCDL-SA Draft Team

Sep. 19th, 2023



Association for Standardization of
Automation and Measuring Systems

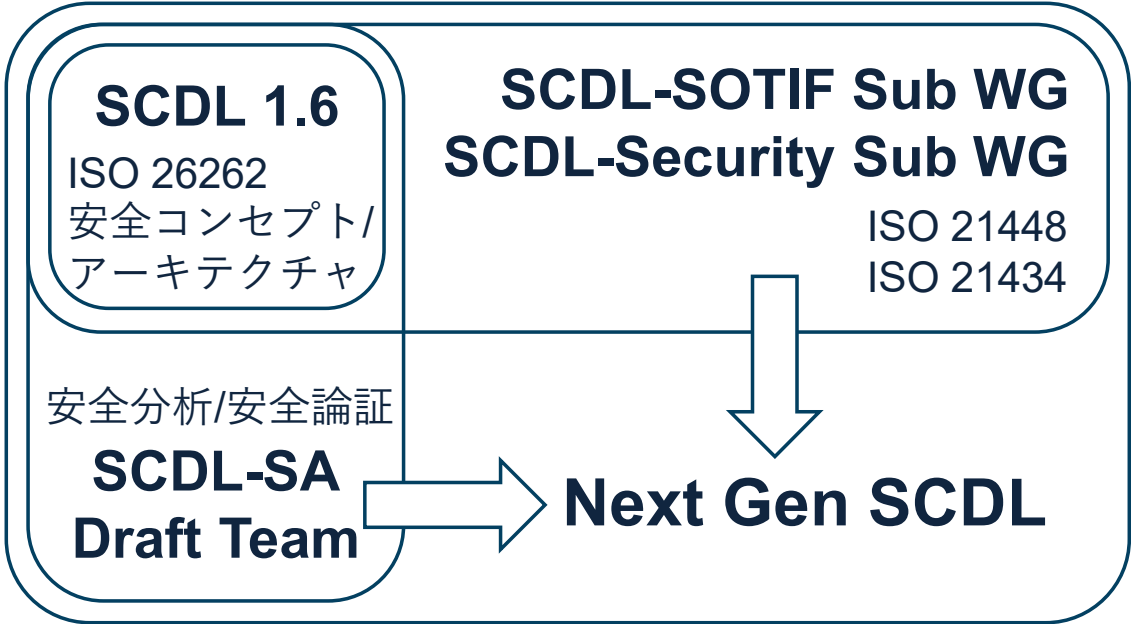
目次

- 1.SCDL-SAとは?
 - ▣ SCDL-SA DT(ドラフトチーム)の経緯、目的、構成
 - ▣ 活動内容
- 2.要求事項と議論した項目
 - ▣ 2.1 SCDLへのニーズ、HLR(High Level Requirements)
 - ▣ 2.2 表現方法とメタモデル検討
- 3.標準化への動機
- 4.ユースケース

1. SCDL-SAとは？

- 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

→ SOTIF SWG, Security SWGはより広い
技術分野/標準規格をカバーする



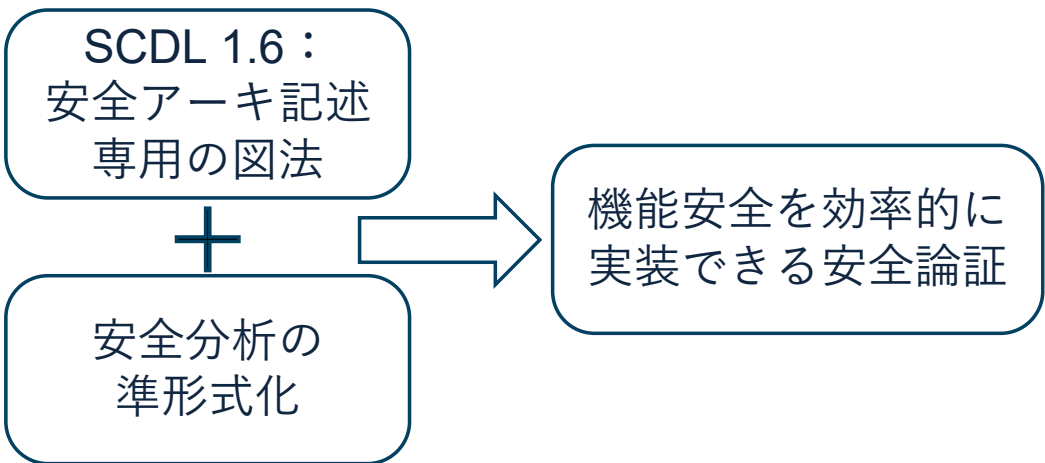
SCDL-SAは成果物/活動の範囲を拡大する

産業界からのニーズ：
開発効率化のために安全コンセプト/アーキテクチャ以外にも準形式化したい

SCDL-SA DT(Draft Team) の経緯、目的、構成

- 2022年4月に活動開始
- 目的：
 - ▣ SCDL1.6がカバーしていない分野の準形式記法の検討

- 安全分析
- 安全要求
- 安全論証



- メンバー(敬称略) :

岩永寿来 (Change Vision)
佐々木喜好 (Marelli)
田口研治 (UL Japan)
宮本秀徳 (構造計画研究所)

大西建児 (GAIO technology)
関康大 (Toyota)
田中伸明 (OTSL)
座長 : 山下修平 (DNV)

SCDL-SA チームのこれまでの活動

広い対象分野

安全分析/論証/アセスメント/保証/アーキ



多方面からの情報収集と議論

安全コンセプト図と安全
分析の現場実装経験

仕様記述ツール実装経験

論証工学・要求工学分野
のナレッジ

機能安全成果物の準形式
化のアイデア提案

SCDL 1.6標準化経験

安全分析手法のメタモデ
ルとユースケース

議論/ケーススタディか
ら要求事項抽出(HLR)



今後の取り組み

SRVAを題材とした安全
分析の準形式化スタディ

ASAM コンセプトプロ
ジェクトプロポーザルへ
のアウトプット

国内外カンファレンスな
どへの打ち込み計画

2. 要求事項と議論した項目

2.1 SCDL-SAへのニーズ、HLR(要求事項)

	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、どの故障をどこの安全機構(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

SCDL-SAへの要求事項

新規の要求事項

- 1. 故障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

Changes : SCDL1.6→SCDL Next Gen(proposal)

SCDL 1.6

- 安全コンセプト図の文法を定義した
- 安全要求表の併用を前提としていた
- 安全分析の展開はユーザー任せだった



SCDL Next Gen は三点セット

- 安全コンセプト図
- 安全要求仕様
- SRVA (安全要求侵害分析)

SCDL 1.6 Work Products	Item	SCDL Next Gen Work Products		
		Safety Concept	Safety Requirement	Safety Analysis
安全コンセプト図	Structure of Safety Req.	✓		
	Structure of elements	✓		
	Allocation of Safety Req.	✓		
	ASIL	✓		
	Requirement Group		✓	✓
	Pairing btw groups		✓	✓
	Independence Req.	(✓)	✓	✓
	FFI		✓	✓
	FFI Req.	(✓)	✓	✓
	Interface	(✓)	✓	
(安全要求表)	Req. ID, Label		✓	✓
	Natural Lang. Express.		✓	
	Type (IF, SM, etc.)		✓	(✓)
	Input, output		✓	
	ASIL		✓	
	Status		✓	
	Traceability		✓	
(安全分析)	Safety Req. ID			✓
	Safety Req.			✓
	Type			✓
	Safety Req. Violation Mode			✓
	Effect of Safety Req. Violation			✓
	Safety Measure/Mechanism			✓

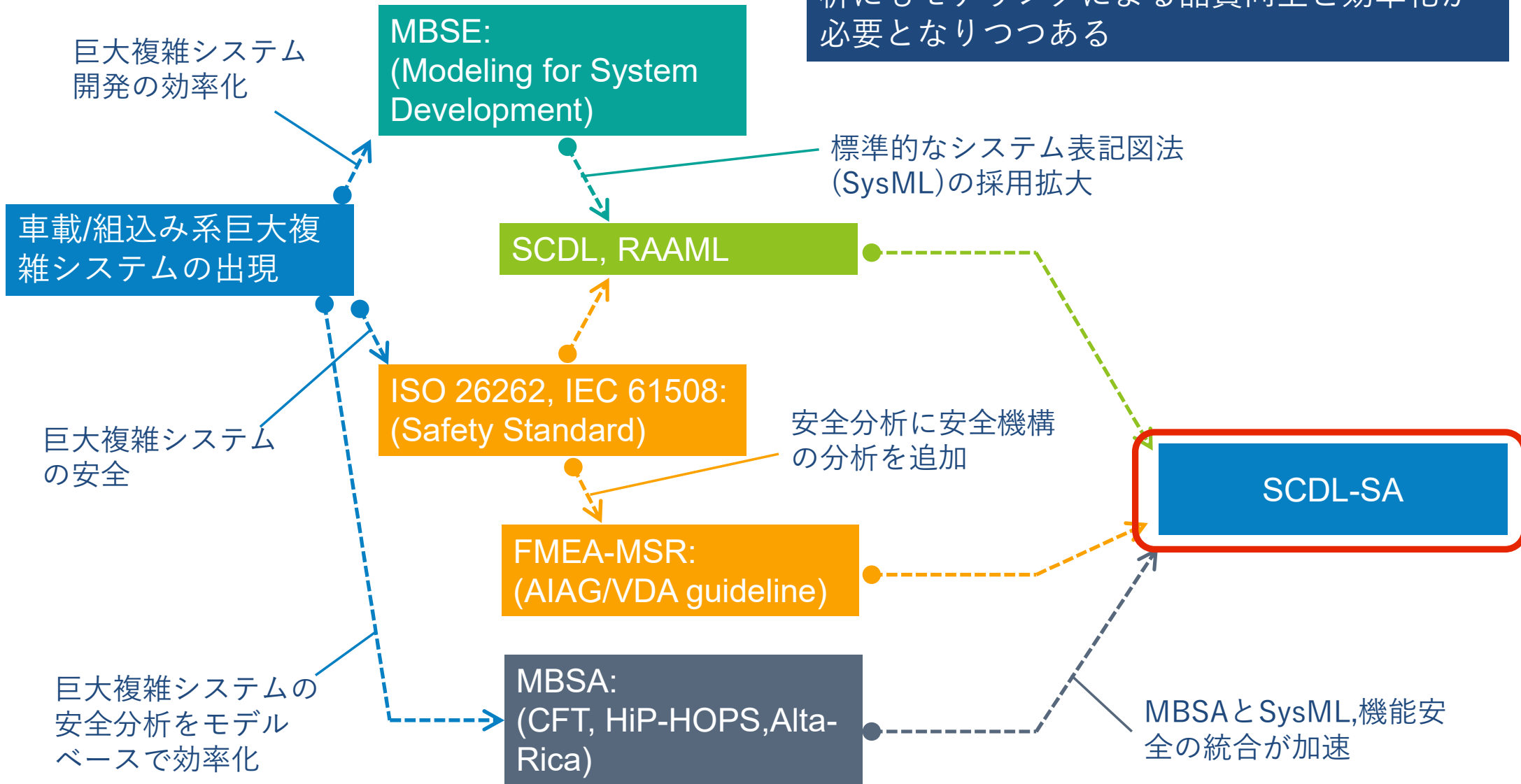
3. 標準化の動機

- 技術的背景：
 - ▣ 現在、モデルベース安全分析/論証はアカデミック及び産業分野で活発に研究開発が行われている技術である
- 業界からのニーズ：
 - ▣ 安全分析/安全論証の成果物の準形式化による業務効率化が求められている
- 標準化のニーズ：
 - ▣ この技術を自動車、航空のような大規模開発で活用するためには、標準的な表記方法とツール間/組織間の相互運用性が不可欠である

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

11



4. ユースケース

□ 次のコミュニケーションで用いる：

■ 開発者と安全分析実施者の間の検証/レビュー(開発チーム内)

- 安全分析者はSCDL-SA形式の安全分析結果を作り、分析結果を共有するために開発者に提供する

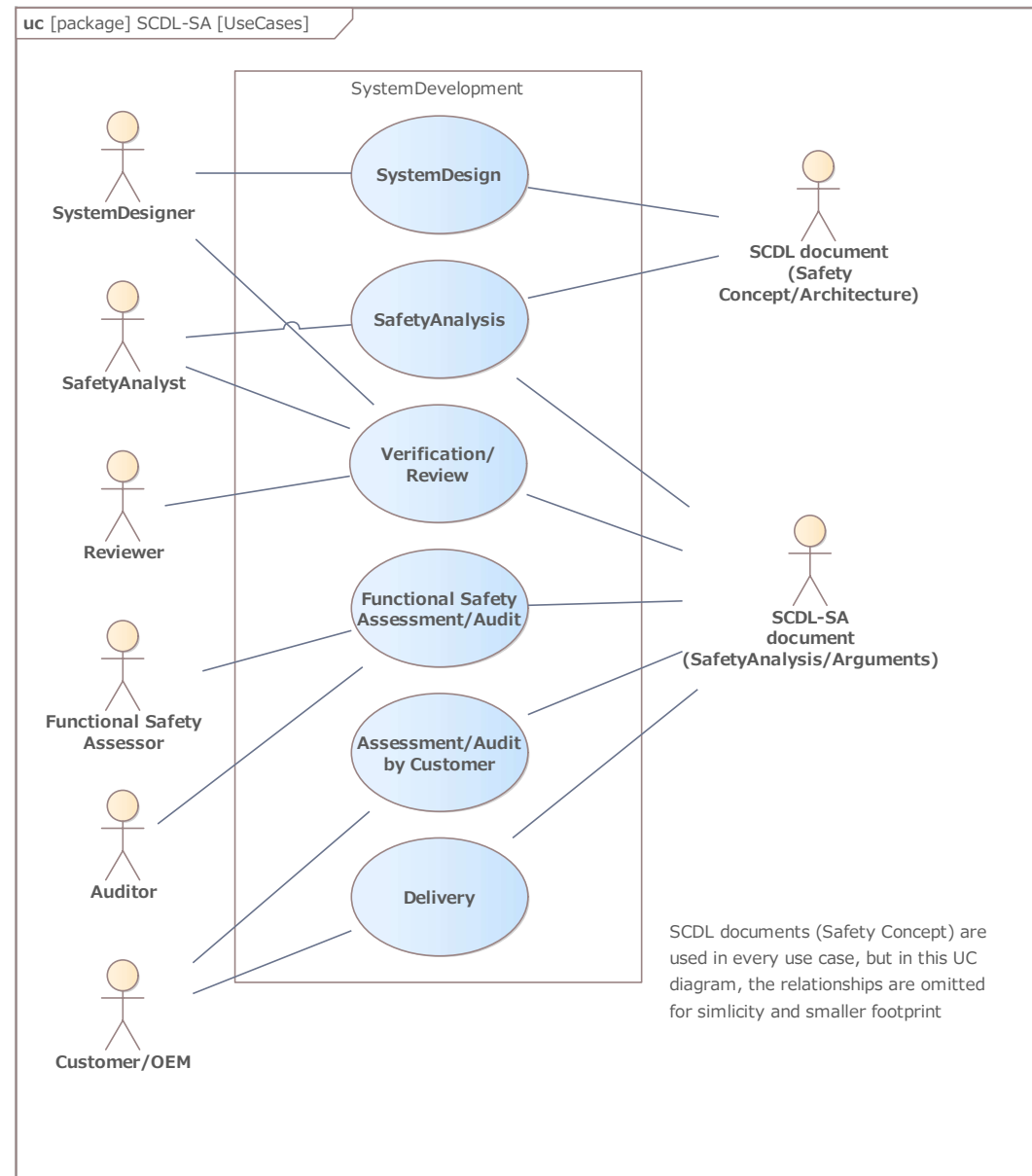
■ 開発者/安全分析実施者とアセッサー/監査者(組織間)

- 開発者と安全分析実施者は安全分析結果/安全論証をSCDL-SA形式で作成し合意する。その結果をアセスメント、監査のためにアセッサー、監査者に提供する
- アセッサーと監査者は、成果物の表現方法の理解を開発者/安全分析者と共有しているので容易に理解できる

■ サプライヤーとカスタマー(会社間)

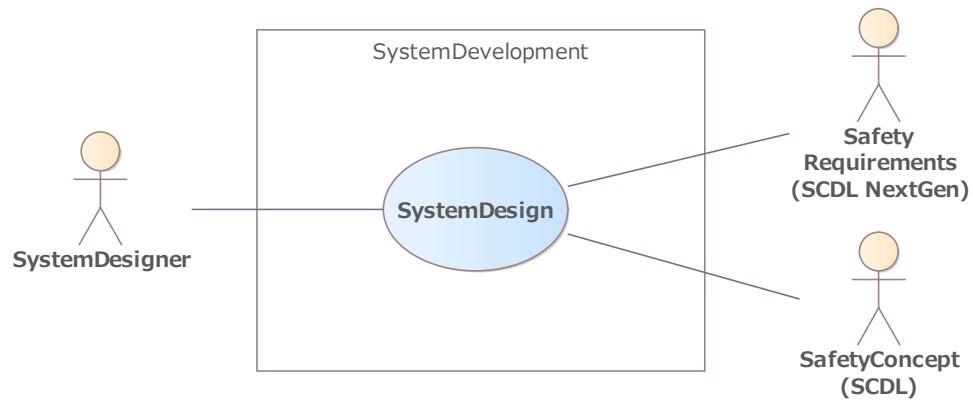
- サプライヤーは安全分析結果と安全論証の結果をSCDL-SA形式でカスタマーに提供する
- 双方の会社は形式の知識を共有しているため、その結果を容易に理解できる

ユースケース図



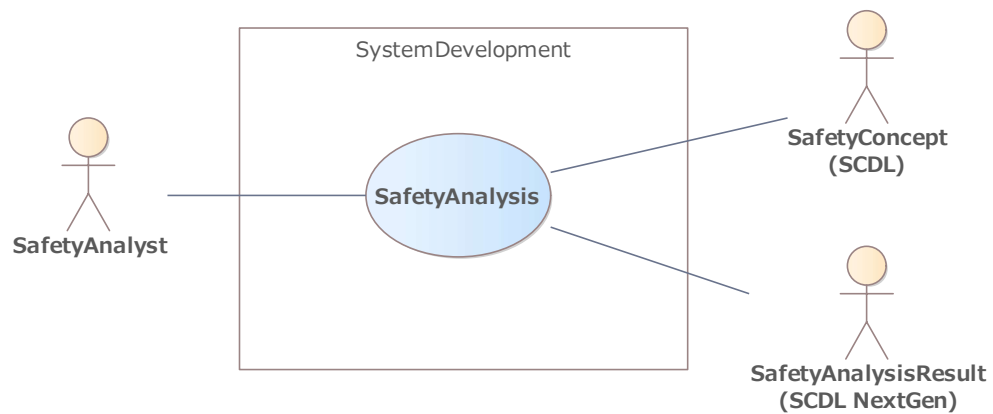
System Design

uc SCDL-SA-UseCases



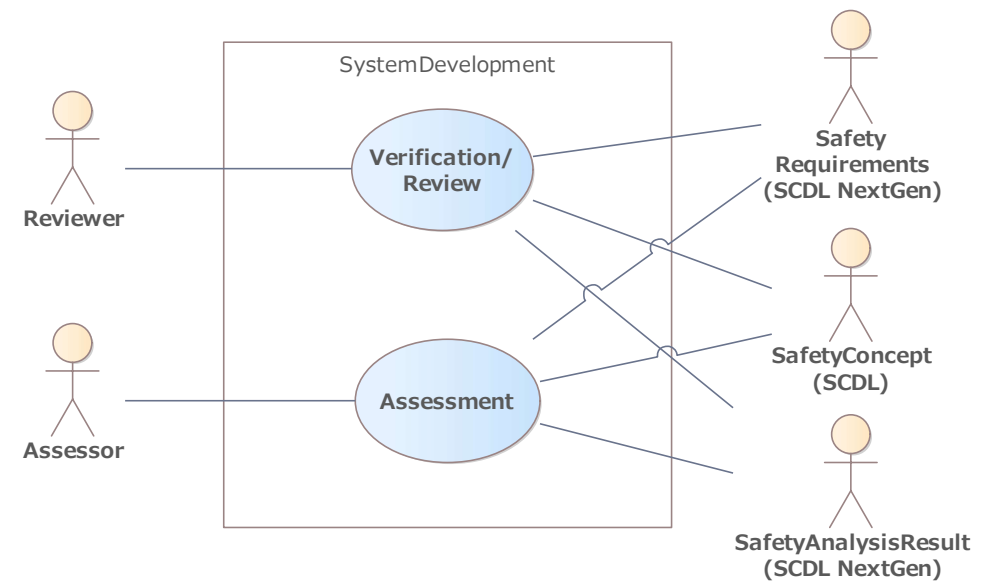
Safety Analysis

uc SCDL-SA-UseCases



Review/Assessment

uc SCDL-SA-UseCases



Thank you for your attention

Question?