SCN-SG Safety Concept Notation Study Group

SCDL
Safety Concept Description Language

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

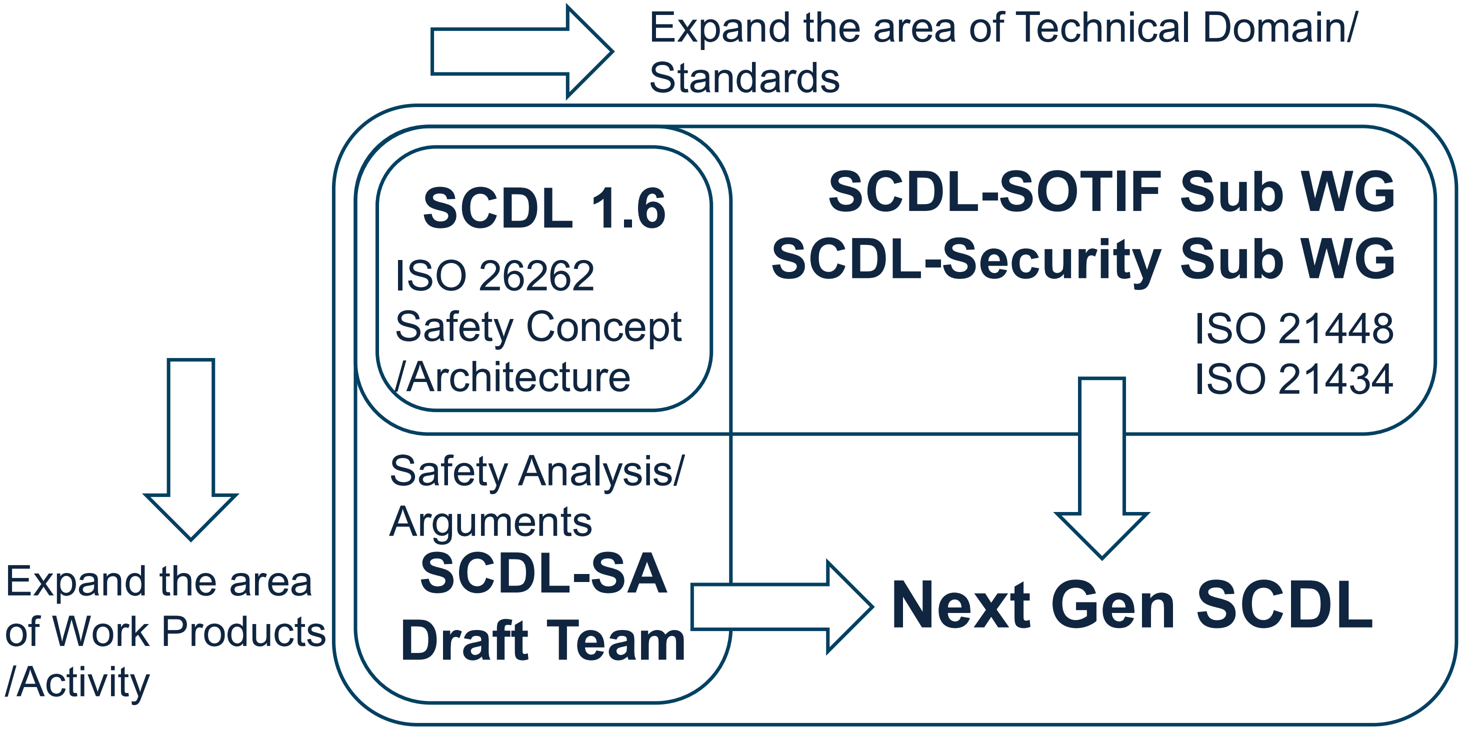
ASAM Association for Standardization of Automation and Measuring Systems

Table of Contents

- □ 1.What is SCDL-SA?
  - SCDL-SA Draft Team：Background, Objective, Members
  - Activities
- □ 2.Requirements and Discussion items
  - 2.1 Needs and HLR (High Level Requirements)
  - 2.2 Changes : SCDL1.6→SCDL Next Gen.
  - 2.3 Discussion on Representation and Metamodel
- □ 3.Motivation for Standardization
- □ 4.Use Cases

1. What is SCDL-SA?

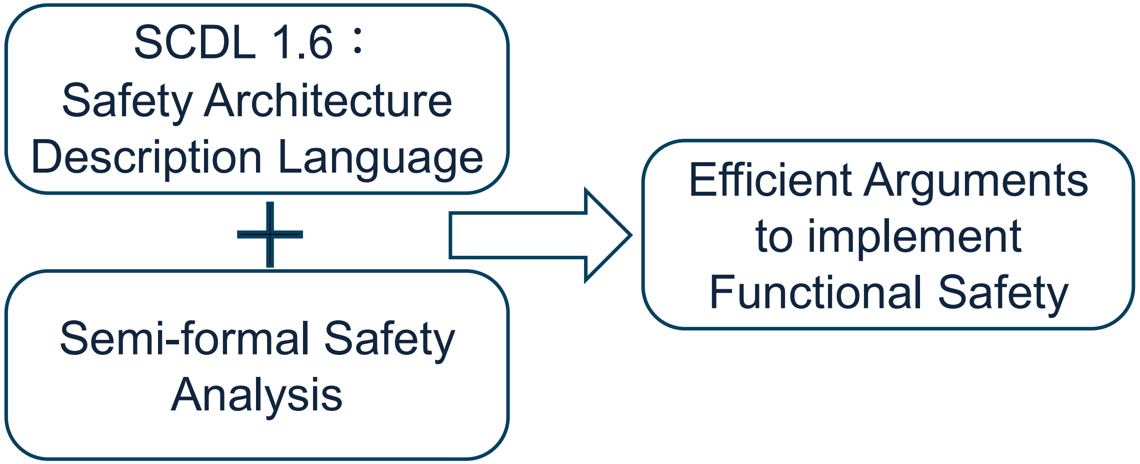
- SCDL-SA covers Safety Analysis/Safety Arguments
  - 2022/Apr. Started investigation on Semi-formal Safety Analysis with SCDL.
  - Later, expanded the discussion also on Safety Arguments
    - Utilize "Safety Concept + Safety Analysis" as Safety Arguments


Expand the area of Technical Domain/ Standards
SCDL 1.6
ISO 26262
Safety Concept /Architecture
SCDL-SOTIF Sub WG
SCDL-Security Sub WG
ISO 21448
ISO 21434
Expand the area of Work Products /Activity
Safety Analysis/ Arguments
SCDL-SA Draft Team
Next Gen SCDL

Strong needs from industry : Semi-formal notation standard in areas other than Safety Concept / Architecture for better efficiency.

SCDL-SA Draft Team in SCN-SG

- □ Established in April/2022
- □ Objectives :
  - Investigate the Semi-formal notation not covered by SCDL1.6
    - Safety Analysis
    - Safety Requirements
    - Safety Arguments



SCDL 1.6：
Safety Architecture
Description Language

Semi-formal Safety
Analysis

Efficient Arguments
to implement
Functional Safety

- □ Members :

Toshiki Iwanaga (Change Vision)

Yoshiyuki Sasaki (Marelli)

Kenji Taguchi (UL)

Hidenori Miyamoto (Kouzou Keikaku Eng. Inc.)

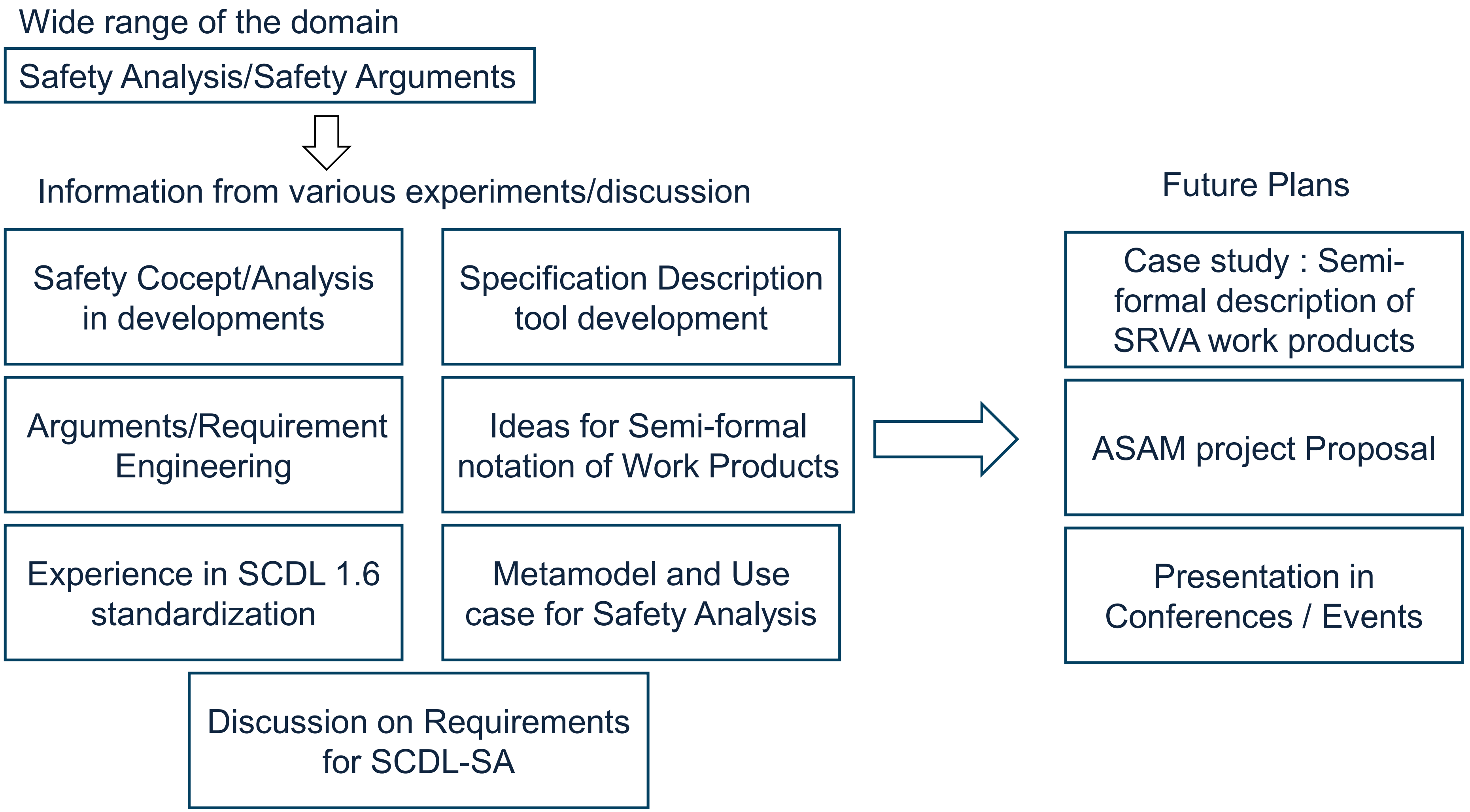
Kenji Ohnishi (GAIO technology)

Kodai Seki (Toyota)

Nobuaki Tanaka (OTSL)

Chair : Shuhei Yamashita (DNV)

Past/Future Activities of SCDL-SA team



Wide range of the domain

Safety Analysis/Safety Arguments

Information from various experiments/discussion

- Safety Cocept/Analysis in developments
- Specification Description tool development
- Arguments/Requirement Engineering
- Ideas for Semi-formal notation of Work Products
- Experience in SCDL 1.6 standardization
- Metamodel and Use case for Safety Analysis
- Discussion on Requirements for SCDL-SA

Future Plans

- Case study : Semi-formal description of SRVA work products
- ASAM project Proposal
- Presentation in Conferences / Events

2.Requirements and Discussions

2.1 Needs and HLR(High Level Requirements)

	Needs from investigation/discussion
1	SCDL-SA shall be able to represent the relationship between failures and the Safety Mechanisms in terms of Safety Goal Violations (SGV).
2	SCDL-SA shall be able to build the analysis result of the system from the combination of the analysis results for components.
3	SCDL-SA shall be able to express the Independence btw. Safety Requirements efficiently.
4	SCDL-SA shall be able to align the result of top-down analysis and bottom-up analysis when the requirements are refined.
5	This activity shall provide the pattern(s) of the FTA result which separates the failures of intended functionality and the failures of Safety Mechanism.

HLR for SCDL-SA

New Requirements

1. Representation of the relationship btw. failures and Safety Mechanism
2. Layering Safety Analysis
3. Inductive/Deductive Analysis

Improvement from SCDL1.6

1. Efficient expression for the Independence btw. Safety Requirements

2.2 Changes : SCDL1.6→SCDL Next gen(proposal)

SCDL 1.6

- Defined syntax for Safety Concept
- Assumed the use of Safety Req. table
- Left the selection of Safety Analysis notation

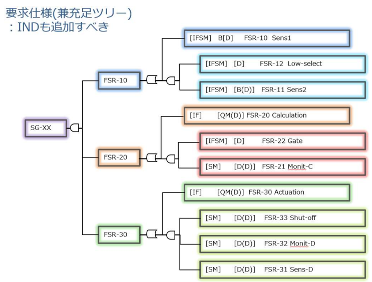
➡SCDL Next Gen will provide

- Safety Concept diagram
- Safety Req. specification
- Safety Req. Violation Analysis

SCDL 1.6 Work Products	**Item**	**SCDL 1.7 Work Products**		
		Safety Concept	Safety Requirement	Safety Analysis
Safety Concept Diagram.	Structure of Safety Req.	✓		
	Structure of elements	✓		
	Allocation of Safety Req.	✓		
	ASIL	✓		
	Requirement Group		✓	✓
	Pairing btw groups		✓	✓
	Independence Req.	(✓)	✓	✓
	FFI		✓	✓
	FFI Req.	(✓)	✓	✓
	Interface	(✓)	✓	
(Safety Requirements)	Req. ID, Label		✓	✓
	Natural Lang. Express.		✓	
	Type (IF, SM, etc.)		✓	(✓)
	Input, output		✓	
	ASIL		✓	
	Status		✓	
	Traceability		✓	
(Safety Analysis)	Safety Req. ID			✓
	Safety Req.			✓
	Type			✓
	Safety Req. Violation Mode			✓
	Effect of Safety Req. Violation			✓
	Safety Measure/Mechanism			✓

Discussion on Representation and Metamodel

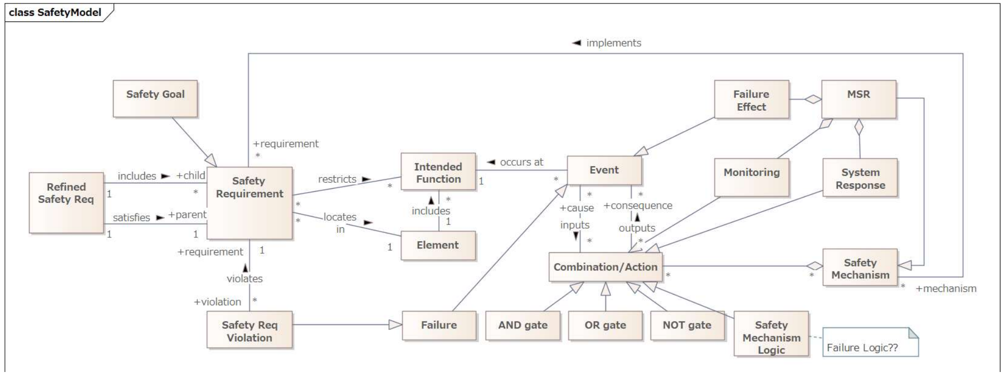
Discussion based on Representation

<table>
<tr><th></th><th>Table form</th><th>Graphical form</th></tr>
<tr><td>Req.</td><td>安全要求仕様
<table>
<tr><th>SR
ID / 短縮名</th><th>自然言語表記</th><th>ASIL</th><th>input</th><th>output</th><th>allocation</th></tr>
<tr><td>FSR-10 / Sens1</td><td>ドライバの操作を取り込む</td><td>B(D)</td><td>User's input</td><td>Sensor value1</td><td>X-SNS</td></tr>
<tr><td>FSR-11 / Sens2</td><td>ドライバの操作を取り込む</td><td>B(D)</td><td>User's input</td><td>Sensor value2</td><td>SNS2</td></tr>
<tr><td>FSR-12 / Low-select</td><td>セレクトローする</td><td>D</td><td>Sensor value1, Sensor value2</td><td>Sensor value (selected)</td><td>Micro</td></tr>
<tr><td>FSR-20 / Calculation</td><td>出力量を算出する</td><td>QM(D)</td><td>Sensor value (selected)</td><td>Drive command</td><td>X-ECU</td></tr>
<tr><td>FSR-21 / Gate</td><td>ドライブコマンドをゲートする</td><td>D</td><td>Drive command Gating</td><td>Drive command (gated)</td><td>Micro</td></tr>
<tr><td>FSR-22 / Monit-C</td><td>算出値をモニタする</td><td>D(D)</td><td>Sensor value (selected)</td><td>Gating</td><td>S-Micro</td></tr>
<tr><td>FSR-30 / Actuation</td><td>アクチュエイタを駆動する</td><td>QM(D)</td><td>Drive command (gated)</td><td>X-output</td><td>X-driver</td></tr>
<tr><td>FSR-31 / Sens-D</td><td>X-outputを取り込む</td><td>D(D)</td><td>X-output</td><td>Sensor-D value</td><td>D-SNS</td></tr>
<tr><td>FSR-32 / Monit-D</td><td>X-outputをモニタする</td><td>D(D)</td><td>Drive command (gated), Sensor-D value</td><td>Shut- off info</td><td>S-Micro</td></tr>
<tr><td>FSR-33 / Shut off</td><td>X-drive電源をシャットオフする</td><td>D(D)</td><td>Shut-off info</td><td>Shut-off</td><td>RLY</td></tr>
</table></td><td>
要求仕様(兼充足ツリー)
：INDも追加すべき
SG-XX
FSR-10
FSR-20
FSR-30
[IFSM] B[D] FSR-10 Sens1
[IFSM] [D] FSR-12 Low-select
[IFSM] [B(D)] FSR-11 Sens2
[IF] [QM(D)] FSR-20 Calculation
[IFSM] [D] FSR-22 Gate
[SM] [D(D)] FSR-21 Monit-C
[IF] [QM(D)] FSR-30 Actuation
[SM] [D(D)] FSR-33 Shut-off
[SM] [D(D)] FSR-32 Monit-D
[SM] [D(D)] FSR-31 Sens-D

</td></tr>
<tr><td>Safety Analysis</td><td>
<table>
<tr><th>FSR</th><th>SRVモード</th><th>Safety measures /
Safety mechanisms (ID)</th><th>FSR(derived)</th><th>NFSR</th></tr>
<tr><td>[IFSM] B[D]
FSR-10
Sens1</td><td>センシングエラー
(過大側)</td><td>デュアルチャネル型
センサ構成
(SM-10)</td><td>[IFSM] [D]
FSR-12
Low-select
[IFSM] [B(D)]
FSR-11
Sens2</td><td>[NFSR] [D]
FSR-12
Low-select
[IFSM] [B(D)]
FSR-11
Sens2</td></tr>
<tr><td>[IF] [QM(D)]
FSR-20
Calculation</td><td>算出エラー
(Δ20W以上の超過)</td><td>サブマイコンによる算出値のオンラインモニタ＋エラー検出時の固定値への切り替え
(SM-20)</td><td>[SM] [D(D)]
FSR-21
Monit-C
[IFSM] [D]
FSR-22
Gate</td><td>[SM] [D(D)]
FSR-21
Monit-C
[IFSM] [D]
FSR-22
Gate</td></tr>
<tr><td>[IF] [QM(D)]
FSR-30
Actuation</td><td>出力エラー
(Δ20W以上の超過)</td><td>追加センサによる出力モニタ＋エラー検出時のドライバ電源のシャットオフ機能
(SM-30)</td><td>[SM] [D(D)]
FSR-31
Sens-D
[SM] [D(D)]
FSR-32
Monit-D
[SM] [D(D)]
FSR-33
Shut-off</td><td>[SM] [D(D)]
FSR-31
Sens-D
[SM] [D(D)]
FSR-32
Monit-D
[SM] [D(D)]
FSR-33
Shut-off</td></tr>
</table></td><td>SafeDeML,
RAAML etc</td></tr>
</table>

Discussion based on Metamodel

Metamodel for SCDL-SA (draft/simplified)



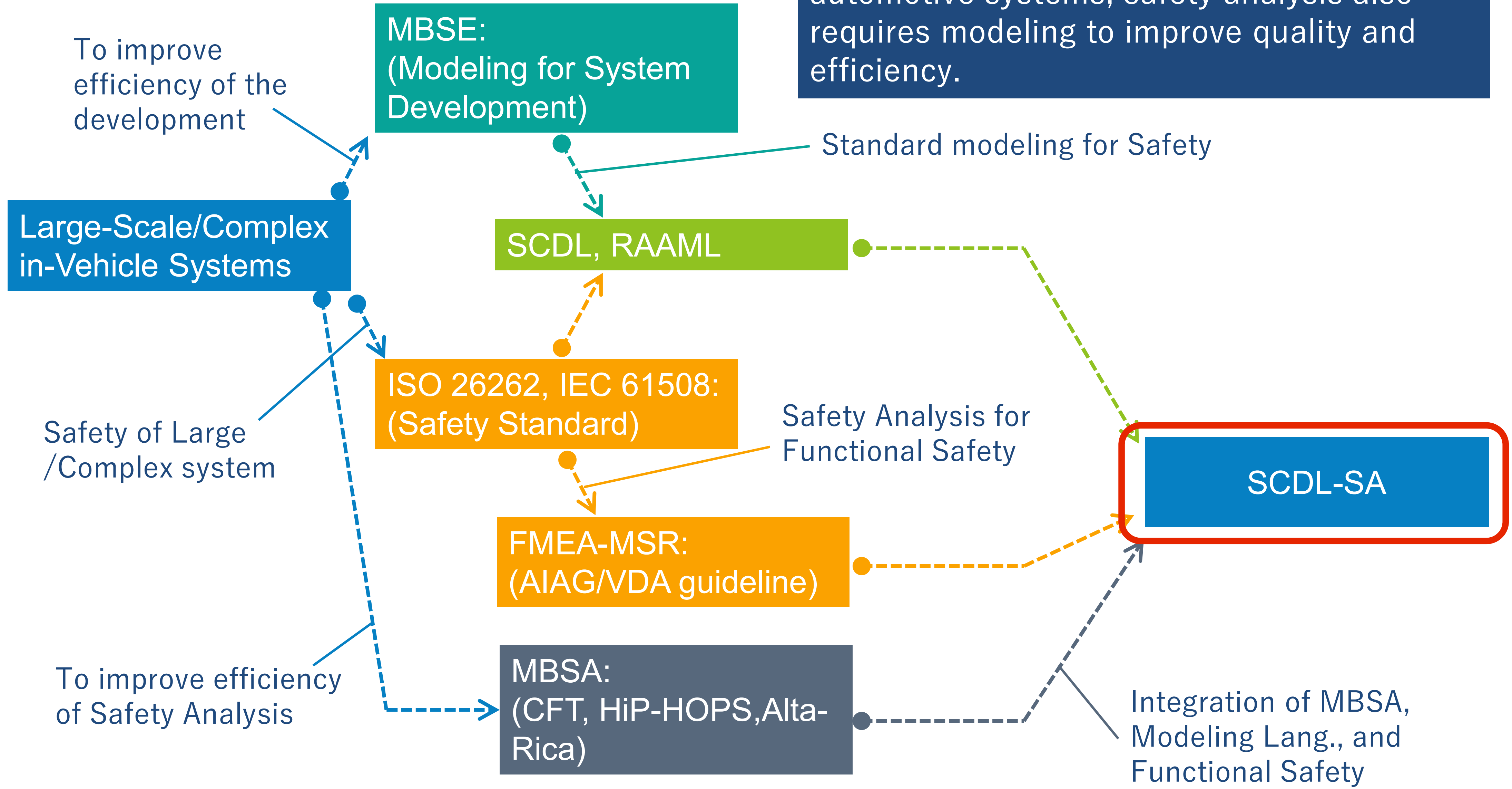
The team is conducting the discussion based on both of Representation and Metamodel for deeper understanding/investigation.

Motivation for standardization

- Technical Background :
  - Currently, Model-Based Safety Analysis/Argument is an active technical field in academic and industrial organizations.
- Strong needs from the industry :
  - Efficient implementation of Safety Analysis/Assurance with Semi-formal work products.
- Needs for standardization :
  - Standard notation and interoperability between different tools /different organizations are necessary for the acceptance of the technology in the large scale development such as automobile, aviation, etc.

Why SCDL-SA?

With the emergence of large and complex automotive systems, safety analysis also requires modeling to improve quality and efficiency.



To improve efficiency of the development

MBSE:
(Modeling for System Development)

Standard modeling for Safety

Large-Scale/Complex in-Vehicle Systems

SCDL, RAAML

ISO 26262, IEC 61508:
(Safety Standard)

Safety of Large /Complex system

Safety Analysis for Functional Safety

SCDL-SA

FMEA-MSR:
(AIAG/VDA guideline)

To improve efficiency of Safety Analysis

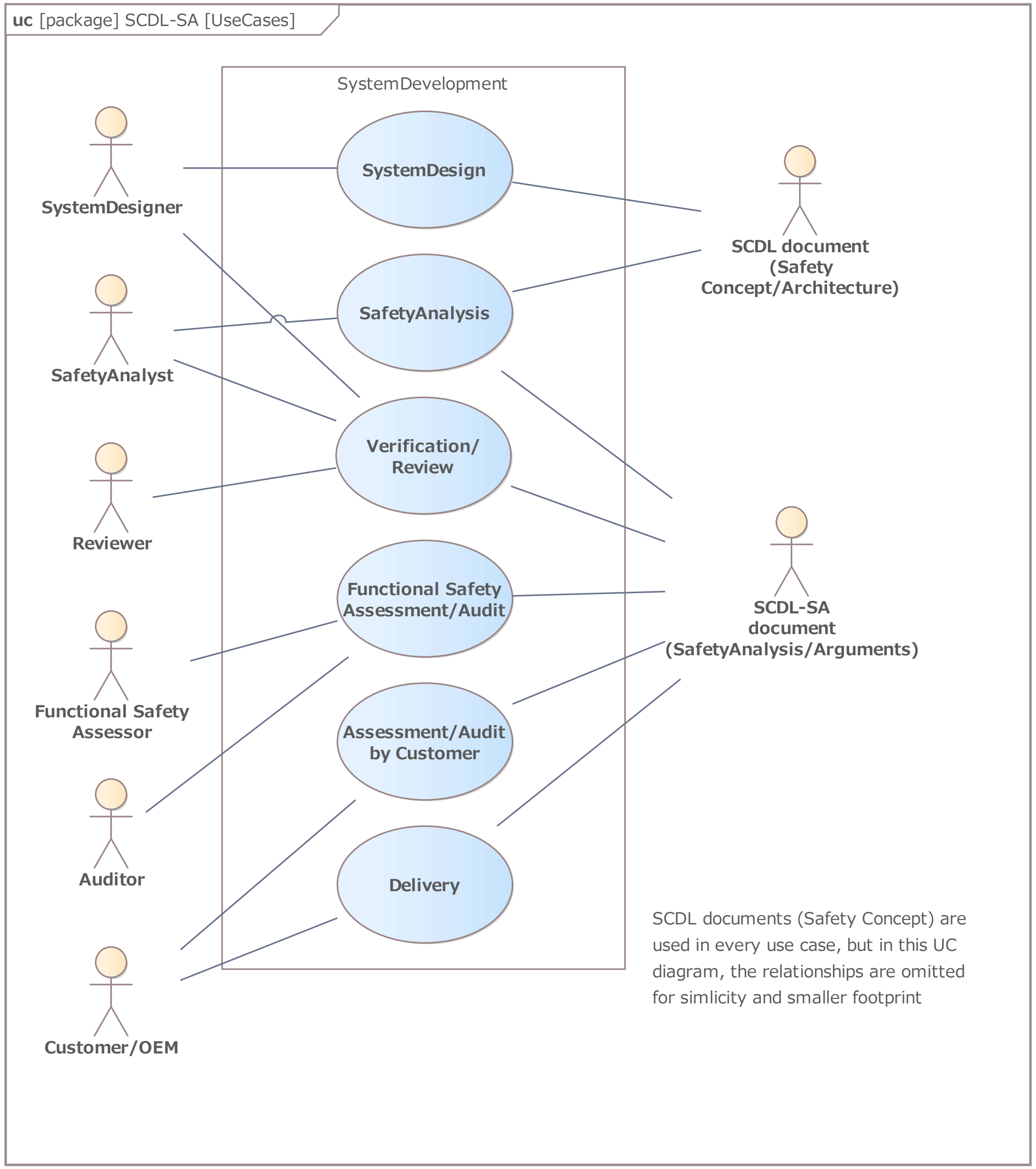
MBSA:
(CFT, HiP-HOPS,Alta-Rica)

Integration of MBSA, Modeling Lang., and Functional Safety

Use cases

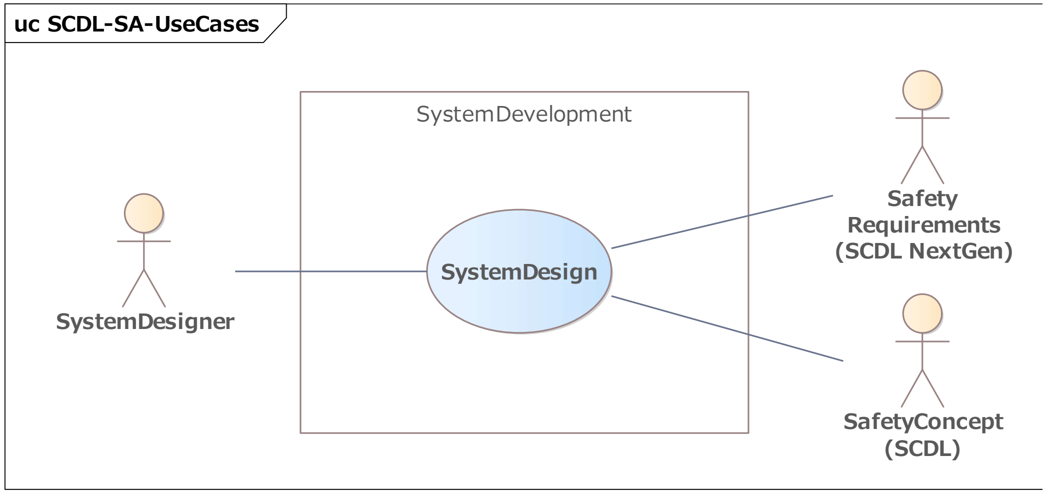
- Communications between :
  - Verification/Review btw Developers and Safety Analysts (in a development team)
    - Safety Analysts make Safety Analysis results in SCDL-SA format and provide them to Developers to share the analysis result.
  - Developer/Safety Analyst and Assessor/Auditor (between divisions)
    - Developers and Safety Analysts build and agree with Safety Analysis result and Safety Arguments in SCDL-SA format and provide them to Assessor and Auditor for assessment and audit.
    - Assessor and Auditor can easily understand the result because of the common understanding of the representation of the work products.
  - Supplier and Customer (between companies)
    - Supplier provides the Safety Analysis results and Assurance results in SCDL-SA form.
    - Both company can easily understand the results because of the common understanding of the format.

Use Case Diagrams

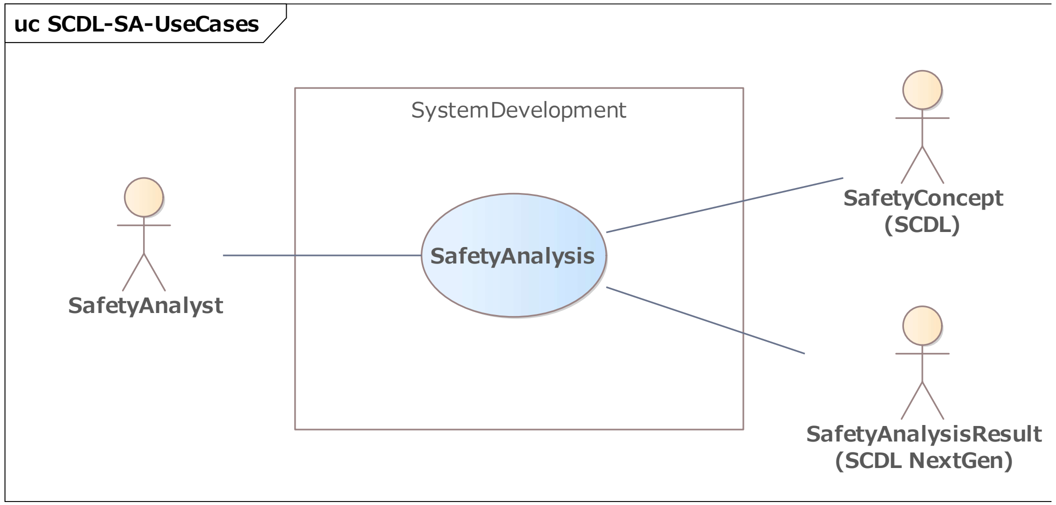

uc [package] SCDL-SA [UseCases]
SystemDevelopment
SystemDesigner
SafetyAnalyst
Reviewer
Functional Safety Assessor
Auditor
Customer/OEM
SystemDesign
SafetyAnalysis
Verification/ Review
Functional Safety Assessment/Audit
Assessment/Audit by Customer
Delivery
SCDL document (Safety Concept/Architecture)
SCDL-SA document (SafetyAnalysis/Arguments)

SCDL documents (Safety Concept) are used in every use case, but in this UC diagram, the relationships are omitted for simlicity and smaller footprint

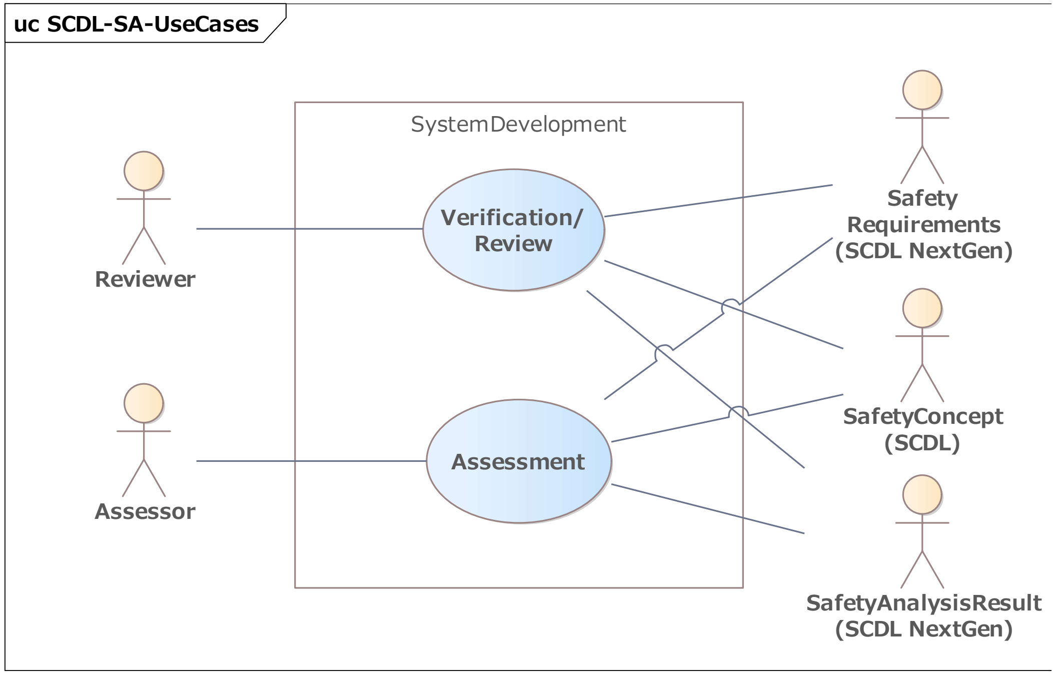
System Design



Safety Analysis



Review/Assessment



Thank you for your attention

Question?