

ASAM SCDL Next Generation

Kiyoshi Sasaki (佐々木 喜好)
SCN-SG, Safety Concept Notation – Study Group,

June. 28, 2023



Agenda

- 1 ASAM SCDL v1.6.0
- 2 ASAM SCDLへの期待
- 3 Workshop: ASAM SCDL next Generationの提案

1 ASAM SCDL v1.6.0

ASAM SCDL v1.6.0

- ISO 26262の最重要成果物である安全コンセプト（安全アーキテクチャ）の記述法に着目
- ASAM SCDL v1.6.0 (2021年)として初版が発行された
- ASAM SCDLは, 機能安全開発の現場で広く活用されている

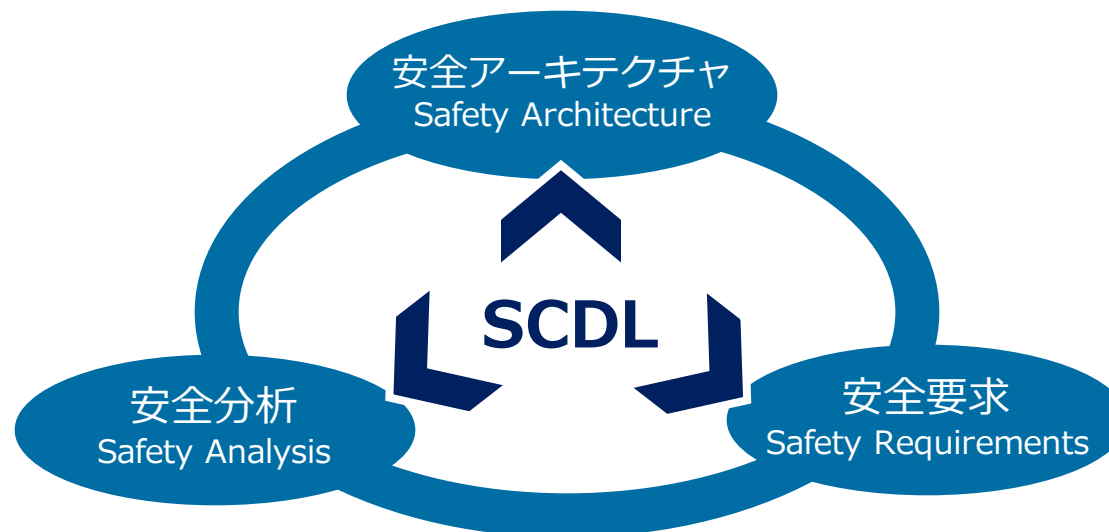


• FS – Functional Safety

なぜ ASAM SCDL v1.6.0が活用されているのか？

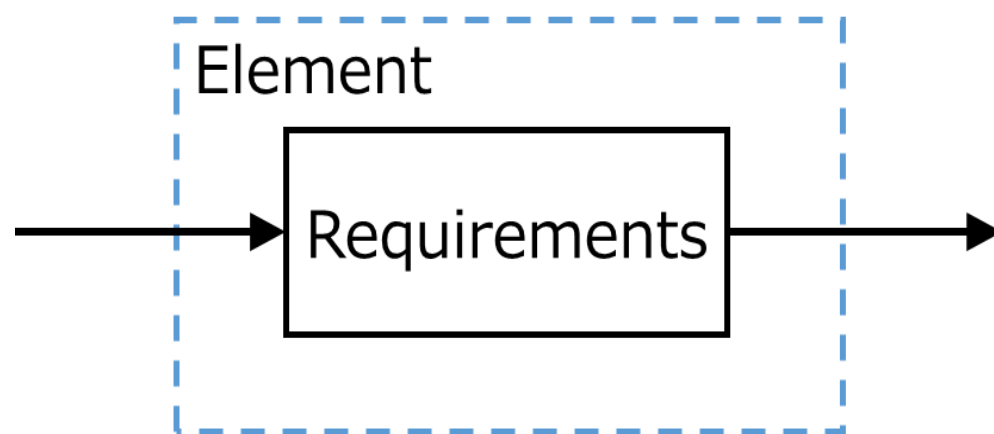
一つの見解として

- ISO 26262:2018 -機能安全- の効果的かつ効率的な実装を支援する
- 安全アーキテクチャを視覚的かつ簡素に構築できる
- 安全の議論を, シームレスかつ合理的に論じることができる
- 論証／安全ケースの中核を担う成果物となる
- OEMとサプライヤ間などの共通言語として活用できる
- ツールベンダーによる活用支援が, ASAM SCDLの普及・展開に貢献している

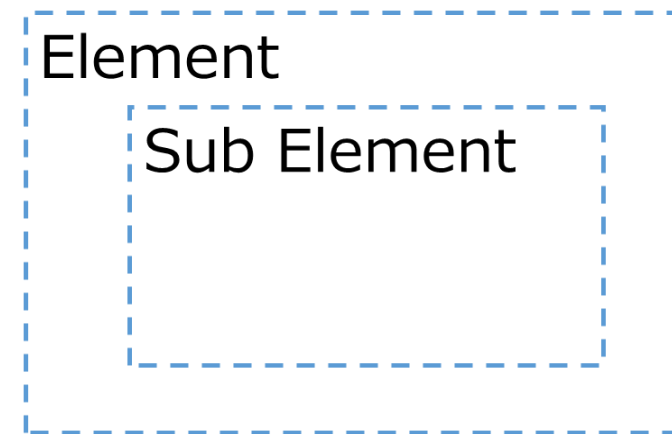


ASAM SCDL v1.6.0の記号

- Safety Concept Description Language, 安全コンセプト記述言語
- 安全アーキテクチャを設計, 分析, レビュー, 共有するための表記法
- モデリング言語による準形式記述



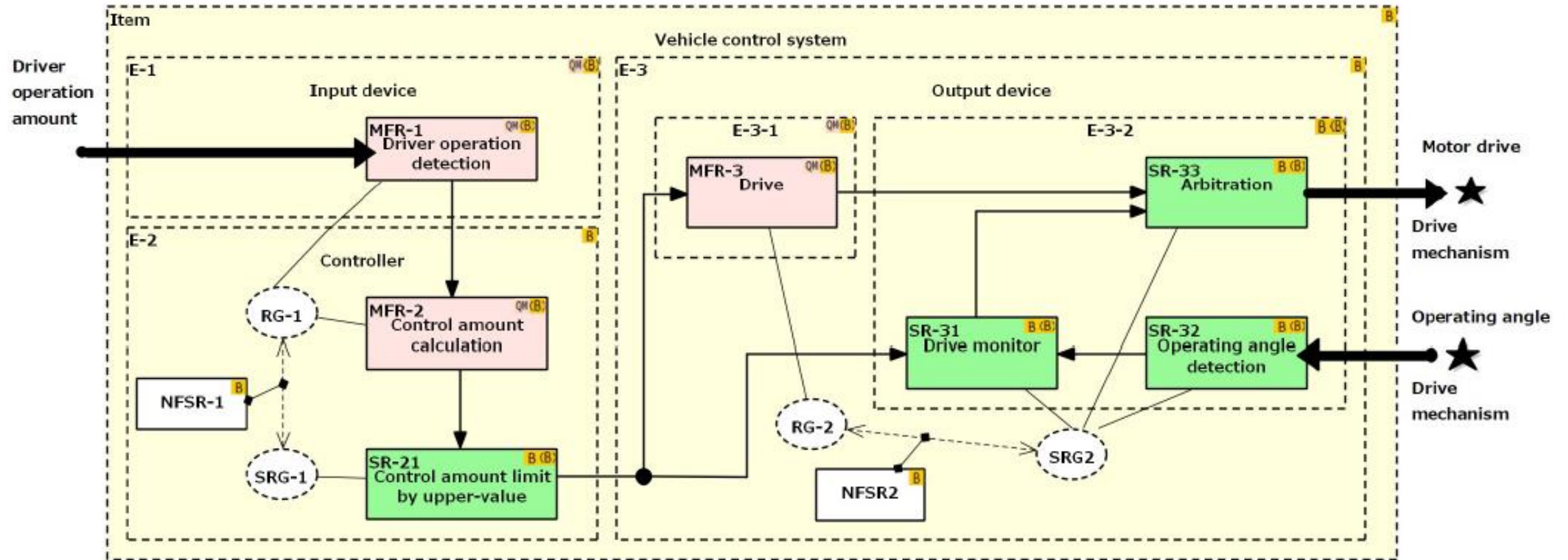
要求とエレメントの関係



階層化

例) ASAM SCDL 1.6.0に基づく安全アーキテクチャ記述

□ ISO 26262における機能安全コンセプトのSCDL記述例：

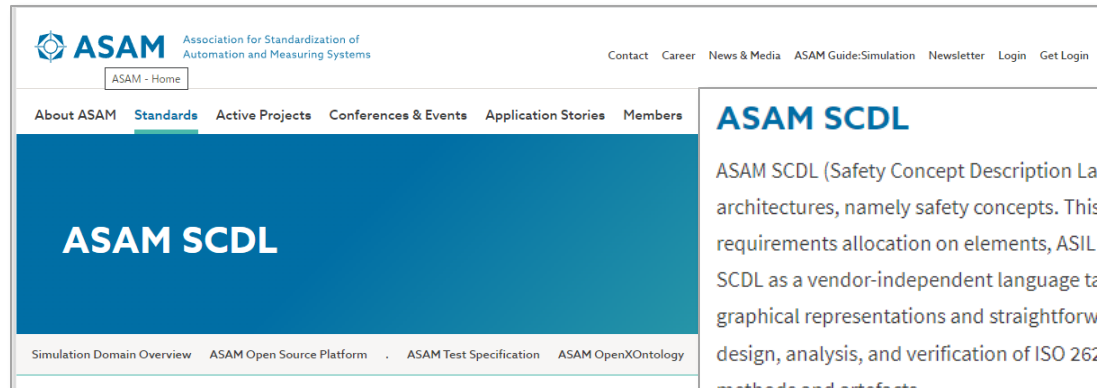


Ref : "ASAM SCDL Practical Examples", Version 1.6.0, 2021-11-09, Figure 2 Architectural diagram using SCDL

ASAM SCDL v1.6.0公開中

□ASAM SCDL v1.6.0 公開中, ASAM HPより誰でも※ 無償でダウンロードできる

※XMLデータ交換仕様はASAM会員のみ公開



ASAM SCDL

ASAM SCDL (Safety Concept Description Language) is a semi-formal notation to describe ISO 26262 safety architectures, namely safety concepts. This includes safety requirement specifications, element architectures, requirements allocation on elements, ASIL assignments, decompositions for safety mechanisms and others. SCDL as a vendor-independent language targets modeling methods for ISO 26262 by providing intuitive graphical representations and straightforward processes. Tools based on SCDL support the development, design, analysis, and verification of ISO 26262 artefacts. It allows for interoperability and exchangeability of methods and artefacts.

Use cases

- ASAM SCDL is utilized as a standardized representation to support development and verification of functional / technical safety concepts and requirements.
- ASAM SCDL and its graphical representation are intuitive and are used as a basis to commonly discuss and further develop ISO 26262 related aspects.
- ASAM SCDL is also utilized to specify safety architecture in HW/SW integrated system.

Benefits

- ASAM SCDL is a vendor-independent language to apply ISO 26262 requirements and design safety architectures.
- ASAM SCDL supports tool-based development of safety concepts and software interfaces to link all ISO 26262 artefacts.

DOWNLOADS

ASAM SCDL v 1.6.0
(Free of charge for members)



VIEW ONLINE (Free of charge)

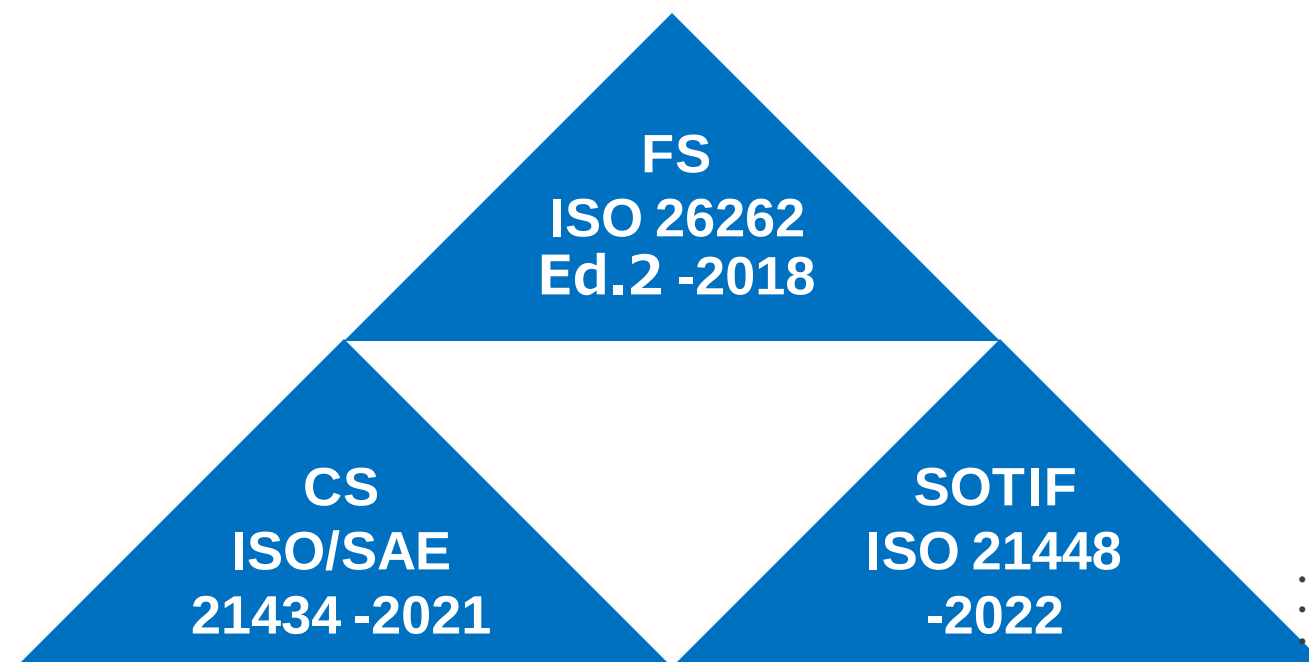
ASAM SCDL Specification	PDF (1 MB)	↓
ASAM SCDL Specification [JP]	PDF (3 MB)	↓
ASAM SCDL Practical Examples	PDF (1 MB)	↓
ASAM SCDL Practical Examples [JP]	PDF (883 KB)	↓
ASAM SCDL Release Presentation	PDF (774 KB)	↓

Ref: <https://www.asam.net/standards/detail/scdl/>

2 ASAM SCDLへの期待

安全安心に関する三つの規格が到来

- 2022年に自動車制御系の安全関連三規格が出揃った
- 三つの規格は密接に関連している
- 制御システム開発においては効率的で効果的な連携による実装が求められる

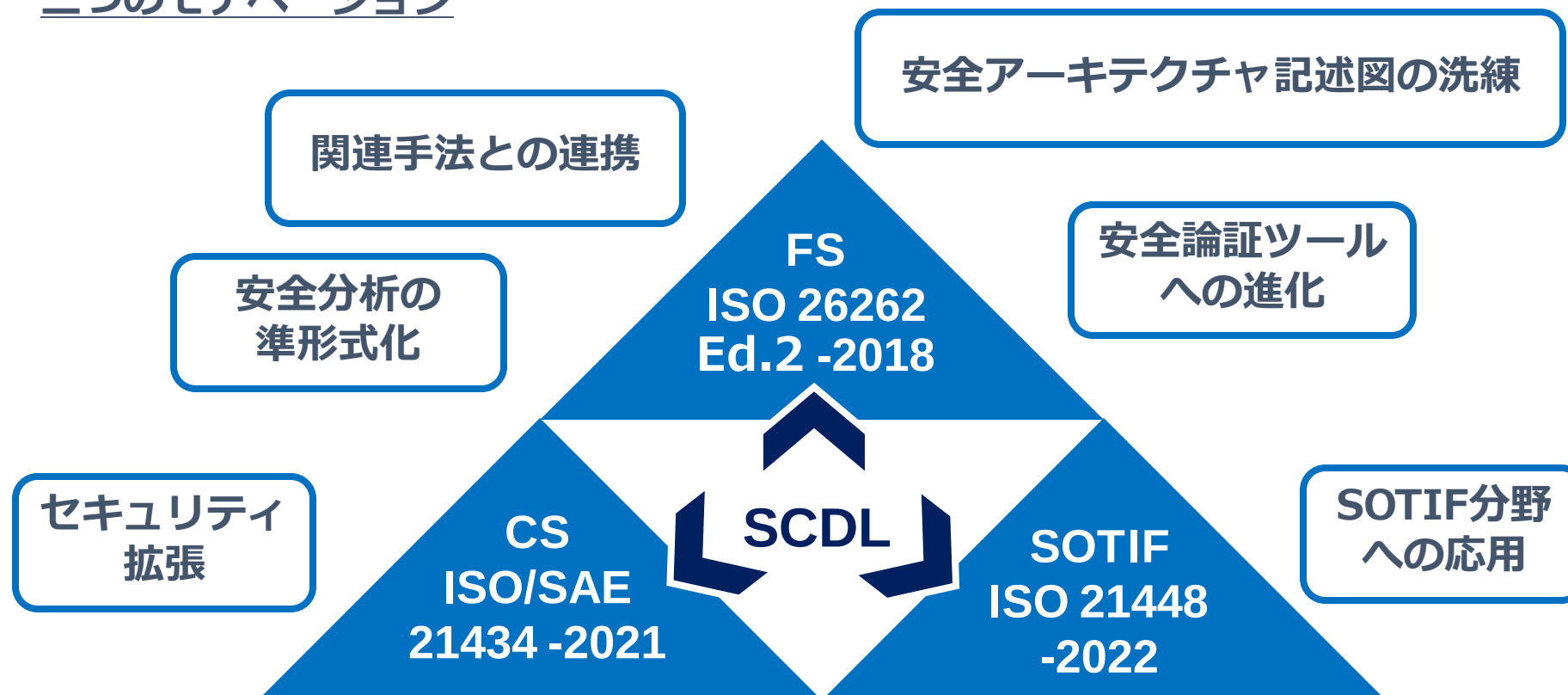


- FS – Functional Safety
- CS – Cyber Security
- SOTIF – Safety Of The Intended Functionality

三つの規格時代に対応したASAM SCDL進化の議論

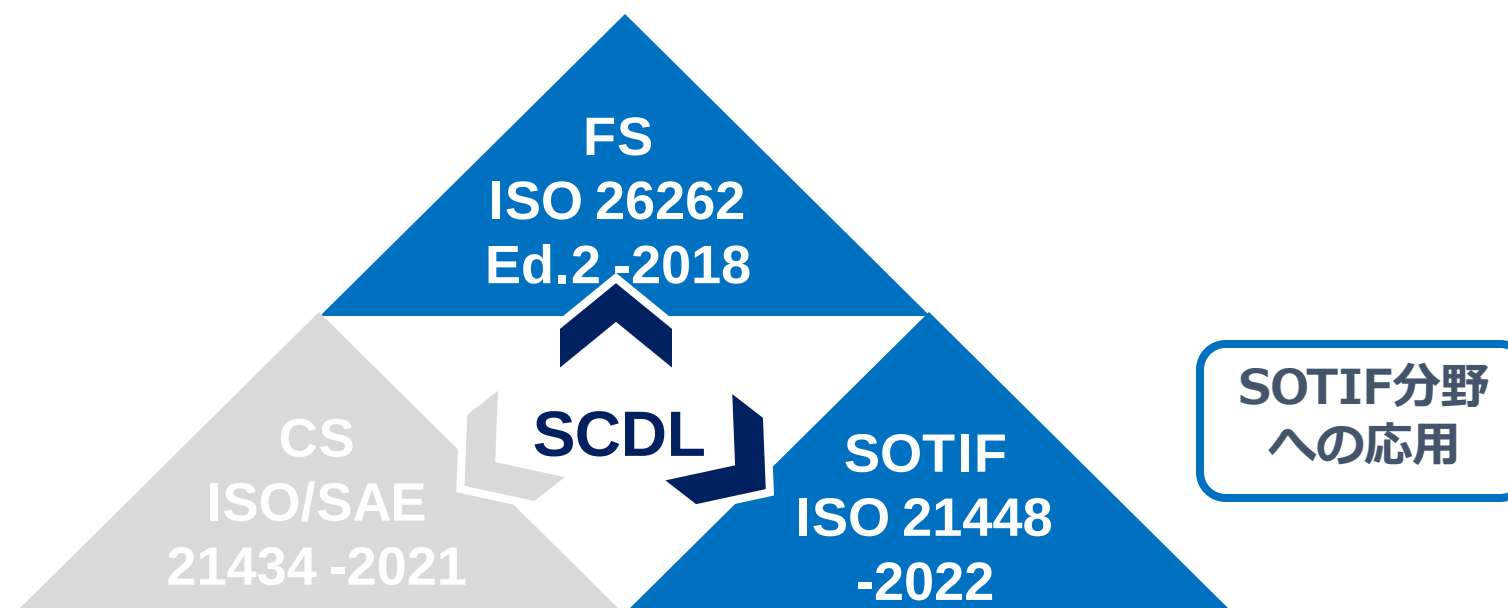
- 三つの安全関連規格を考慮したASAM SCDL拡張の必要性が指摘されるようになってきた
- ASAM SCDLの実用性向上の要望も多い

➡ 三つのモチベーション



モチベーション : SOTIF

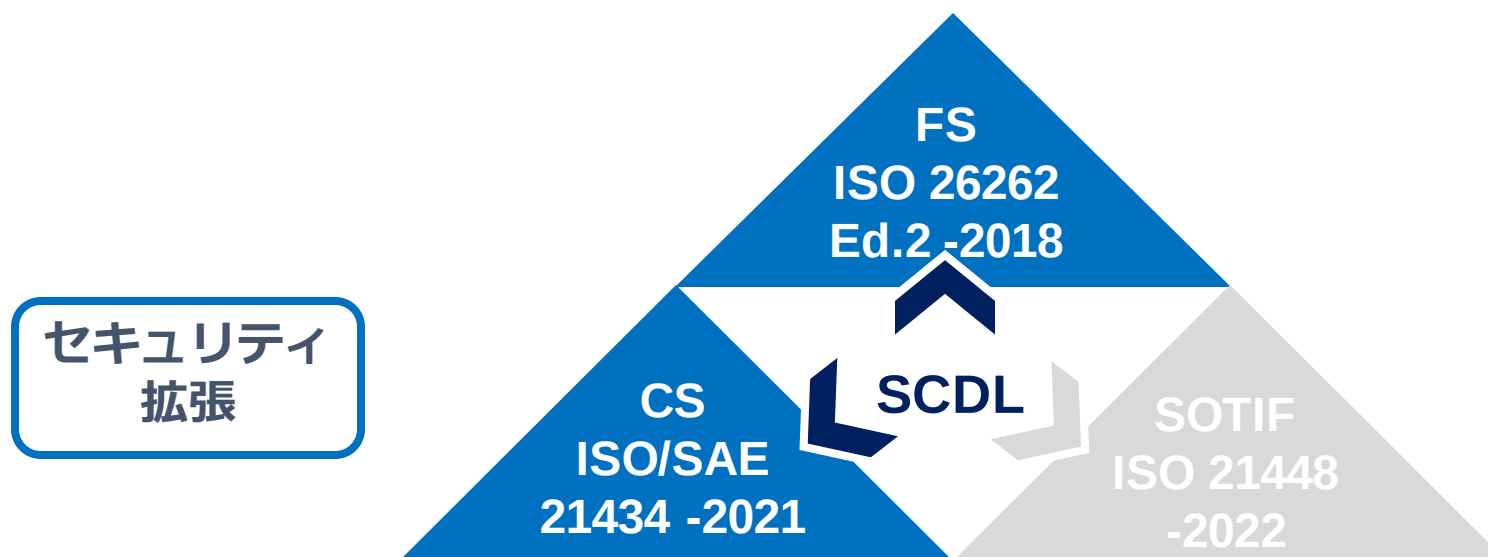
- SOTIF分野へのASAM SCDLの応用拡大
- ISO 21448による意図機能の構築結果が、機能安全のアイテム定義として提示されることになる
- SOTIF取り組みの段階からアーキテクチャ記述にASAM SCDLを活用することで、両規格の効率的かつ効果的な実装をサポートしたい



モチベーション：サイバーセキュリティ

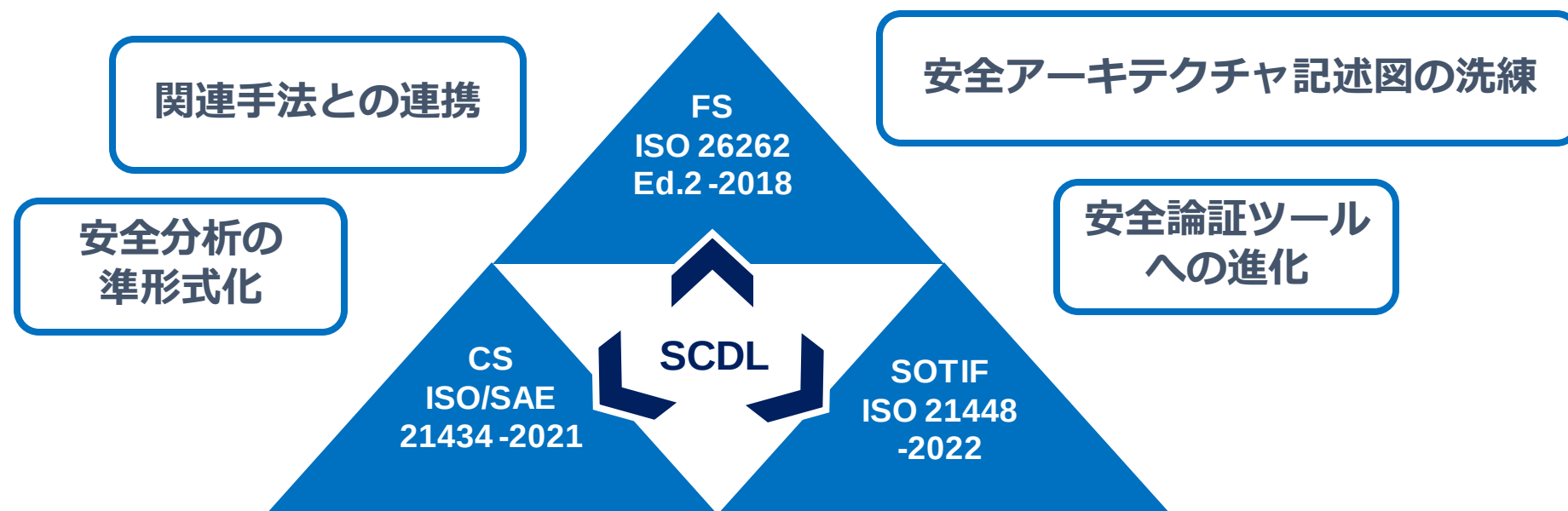
- CS分野へのASAM SCDLの拡張
- ISO/SAE 21434 では, 脅威の対象となりうる情報, 機能, 物理的資産を特定し, そのリスクを分析・処理しなければならない
- 安全性の観点からASAM SCDLを脅威分析に適用することが有効であることは既に報告※されている
- 両規格をより効果的に関連付けるために, ASAM SCDLをさらに拡張する可能性に期待されている

※ “Threat Analysis Framework for Safety Architectures in SCDL” @SafeComp2020



モチベーション：安全関連

- 現行のASAM SCDLの実用性向上
- 多数の安全目標・安全要求を取り扱う大規模システムに対応した表記法の一層の洗練への期待がある
- 安全アーキテクチャの分析を効果的に結びつける安全分析側の準形式化ができるのではないか
- これらに対応した安全要求/エレメント/デコンポジション/共存/安全分析/従属故障分析の、効率的・効果的な取り扱いを可能にするためのASAM SCDLのさらなる洗練が必要であると考えられる
- 三つの規格時代に求められる明瞭な安全論証をサポートするツールとしての役割も重要になってきている

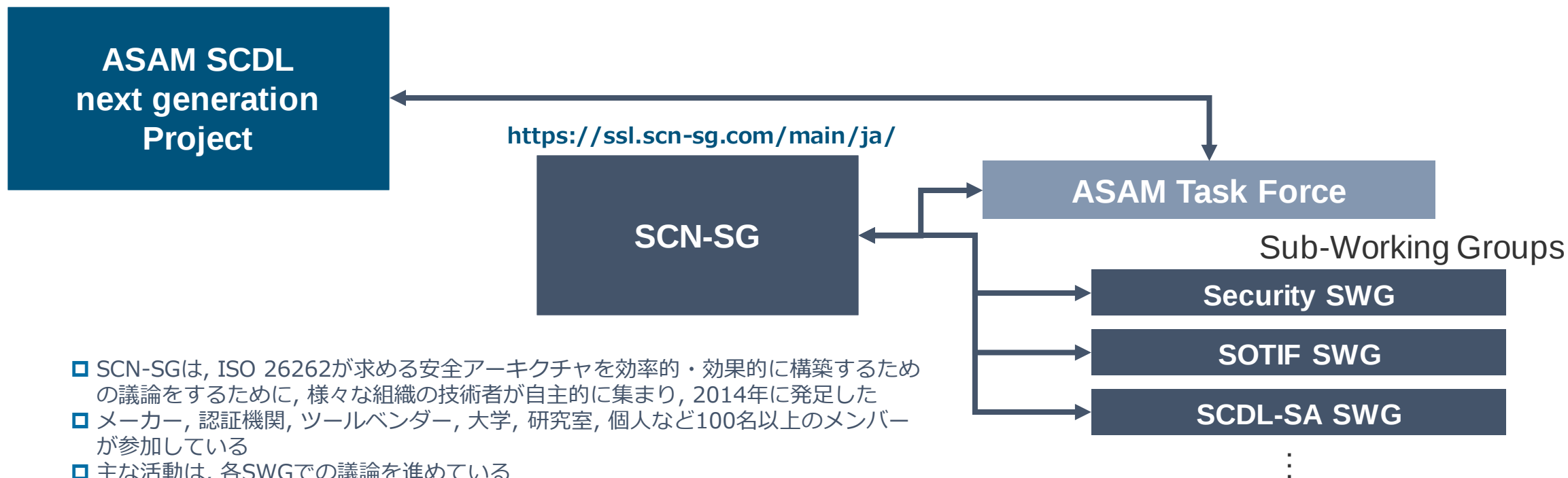


3 Workshop: ASAM SCDL next Generationの提案

ASAM SCDL next generationに関する議論の現状

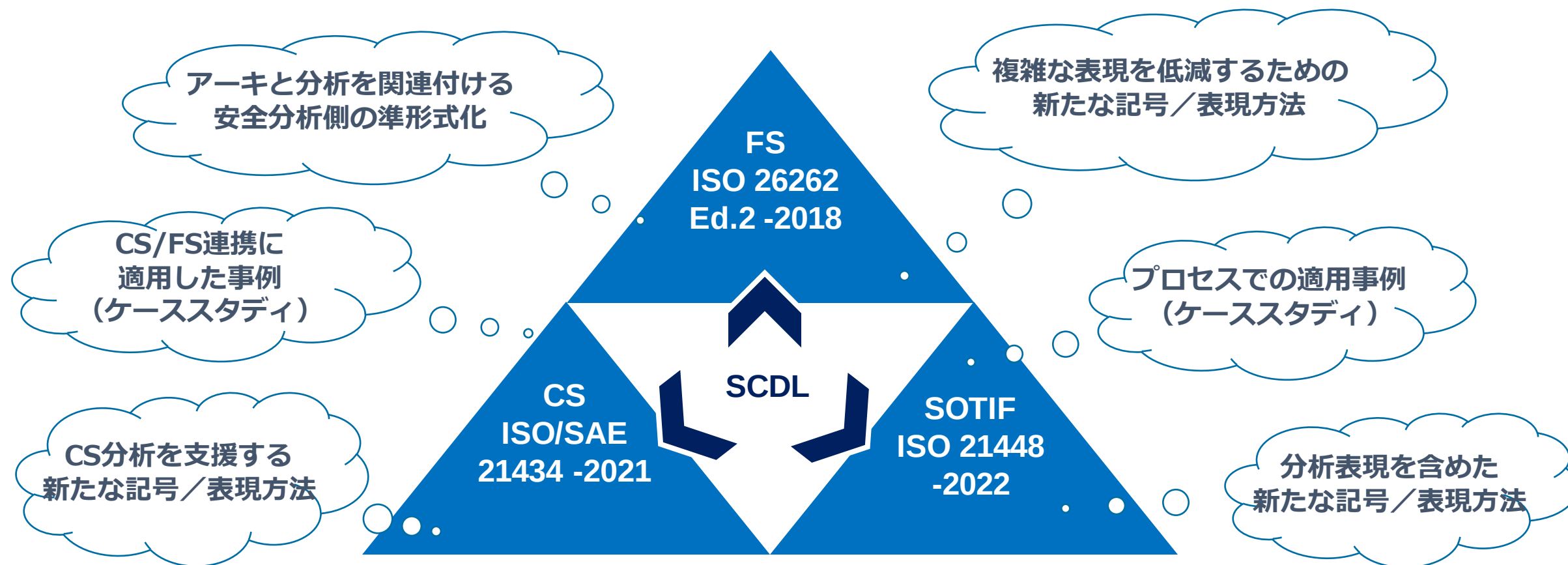
- ASAM SCDL v1.6.0を提案した任意団体SCN-SG※にて, 次世代議論が始まっている
- SCN-SGの検討結果を踏まえて, 次世代構想をまとめたいと考えている

※SCN-SG: Safety Concept Notation – Study Group (安全コンセプト記法研究会)



検討状況から見えてきた次世代構想

- ASAM SCDLを用いたケーススタディーの拡充
- ASAM SCDLの新たな表記法（記号や表現方法）の追加



ワークショップへの誘い

- 次世代構想について, 世界中の多くの方との議論を通じて, フィードバックを頂きたい
- ワークショップの結果に基づき, ASAM SCDLの新しいプロジェクトを立ち上げる予定
- 皆様からの貴重なお声が, 次世代ASAM SCDLを洗練する

2023年7月27日 (木) 16:00 – 19:00日本時間 (9:00 – 12:00 CEST) Online開催



Ref: <https://www.asam.net/conferences-events/detail/workshop-asam-scdl-next-generation/>

ワークショップ : Agenda (6/28時点)

□ 三つの拡張 (Security, SOTIF, Safety analysis) について, 議論を行う予定である

Time (JST)	Topic	Speaker
9:00	Welcome	Yoshiaki Shoi (ASAM)
9:05	Motivation of ASAM SCDL Next Generation	Akira Takada (DNV)
9:35	Security extension	tbd
10:20	SOTIF extension	Sandra Watanabe (JARI)
11:05	Safety analysis extension	Nobuaki Tanaka (OTSL)
11:50	Closing	Yoshiaki Shoi (ASAM)
12:00	End of Meeting	

<https://www.asam.net/conferences-events/detail/workshop-asam-scdl-next-generation/agenda-69/>

今後の予定

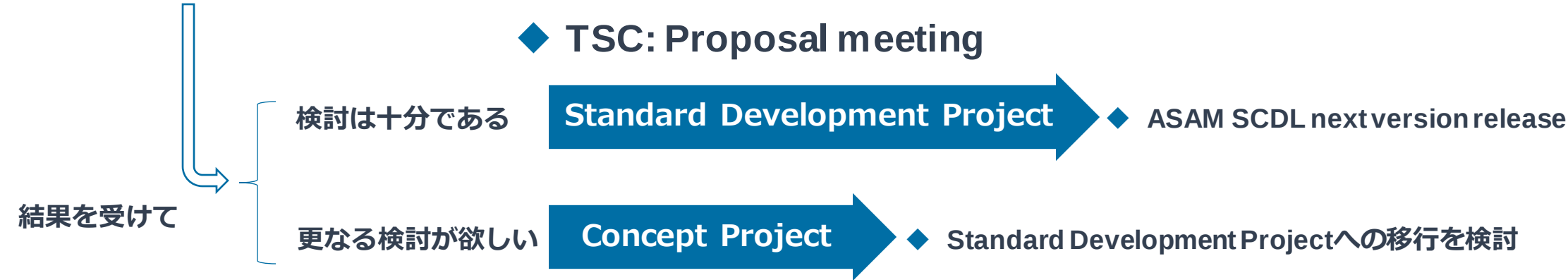
□ タイムスケジュール

ワークショップの結果に応じて、どちらかの新しいプロジェクト提案を考えている

- Standard Development Project (Major / Minor / Revision)
- Concept Project

2023					2024	2025
7	8	9	10	11	1	1

◆ 7/27 : ワークショップ



Thank you for your attention

ワークショップでお会いできるのを楽しみにしております

<Contact>

SCN-SGについて

・安全コンセプト記法研究会 事務局まで

<https://ssl.scn-sg.com/main/ja/contact>

