

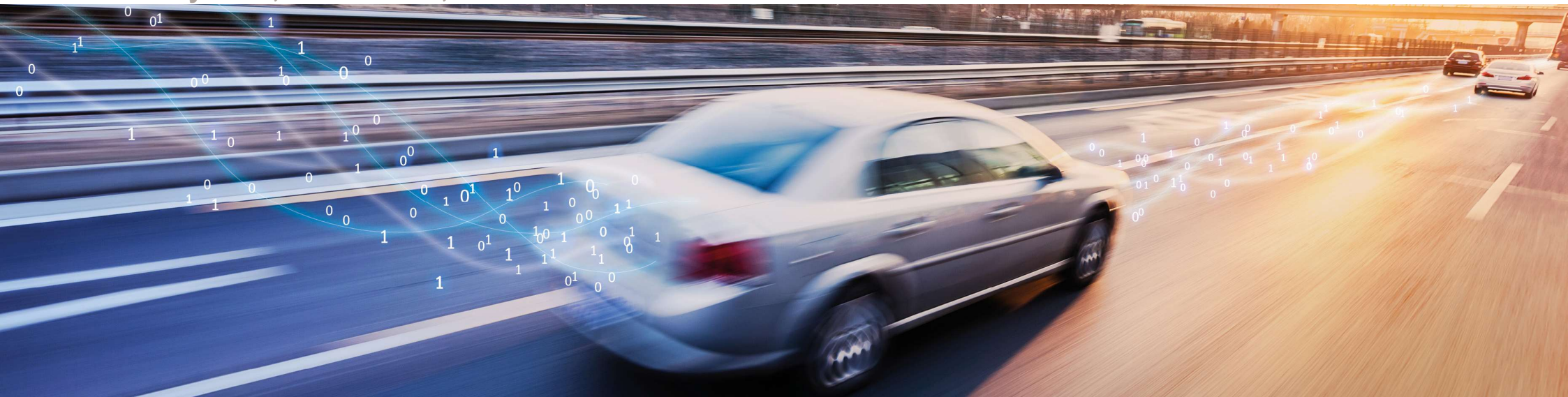
SCDL Next Gen. のご紹介

Akira Takada

SCN-SG

Security SWG, SOTIF SWG, SCDL SA Draft team

Sept. 19th, 2023



アジェンダ

1	ASAM SCDL Next gen.のモチベーション (現行版の課題と限界含む)
2	次世代版への拡張の概要
3	新プロジェクトへのお誘い

アジェンダ

1	ASAM SCDL Next gen.のモチベーション (現行版の課題と限界含む)
2	次世代版への拡張の概要
3	新プロジェクトへのお誘い

安全安心三規格時代が到来

- 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
- ➡上記を考慮したASAM SCDL拡張の必要性が指摘されるようになってきた



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

ASAM SCDL v1.6.0の課題と限界

また、v1.6.0の使用実績から以下のような課題が挙がってきている：

- システムの大規模化等により、図表が複雑化してきている為、可読性が低下してきている
- 安全コンセプト図、安全要求仕様表、安全分析結果は、個別に生成する為、内容の対応関係の追跡が困難



ASAM SCDL
Safety Concept Description Language

Part 1 of 3
Notation Specification
Version 1.6.0
Date: 2021-xx-xx

Base Standard

© by ASAM e.V., 2021

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 of functional / technical safety concepts and requirements.
- ASAM SCDL and its graphical representation are intuitive and are used to design, analyze, and further develop ISO 26262 related aspects.
- ASAM SCDL is also utilized to specify safety architecture in HW/SW integration.

Benefits

- ASAM SCDL is a vendor-independent language to apply ISO 26262 requirements to safety architectures.
- ASAM SCDL supports tool-based development of safety concepts and artifacts.

DOWNLOADS

ASAM SCDL v 1.6.0
(Free of charge for members)

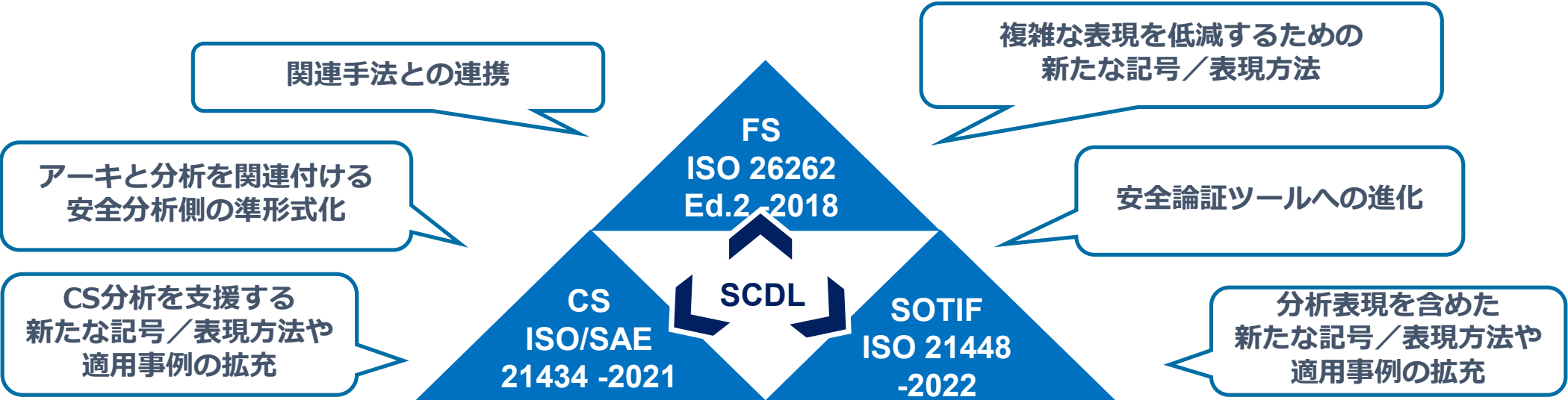
VIEW ONLINE

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

新時代に対応したASAM SCDL進化の議論

三規格時代への対応, v1.6.0の課題と限界 ➡ 三つのモチベーション

- CS分野への拡張
- SOTIF分野への応用拡大
- 現行SCDLの実用性向上



アジェンダ

1	ASAM SCDL Next gen.のモチベーション (現行版の課題と限界含む)
2	次世代版への拡張の概要
3	新プロジェクトへのお誘い

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・対策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
- 両規格への対応の効率的な連携にむけた, ASAM SCDLのさらなる拡張の可能性に期待されている

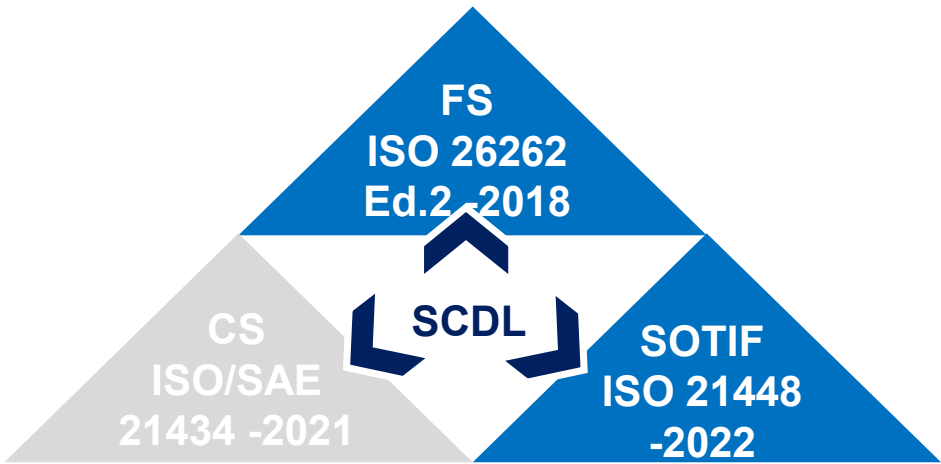
※ “Threat Analysis Framework for Safety Architectures in SCDL” @SafeComp2020



モチベーション : 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、安全アーキテクチャ上でおこるSM重複を合理的に論じる等、両規格の効率的かつ効果的な実装をサポートしたい

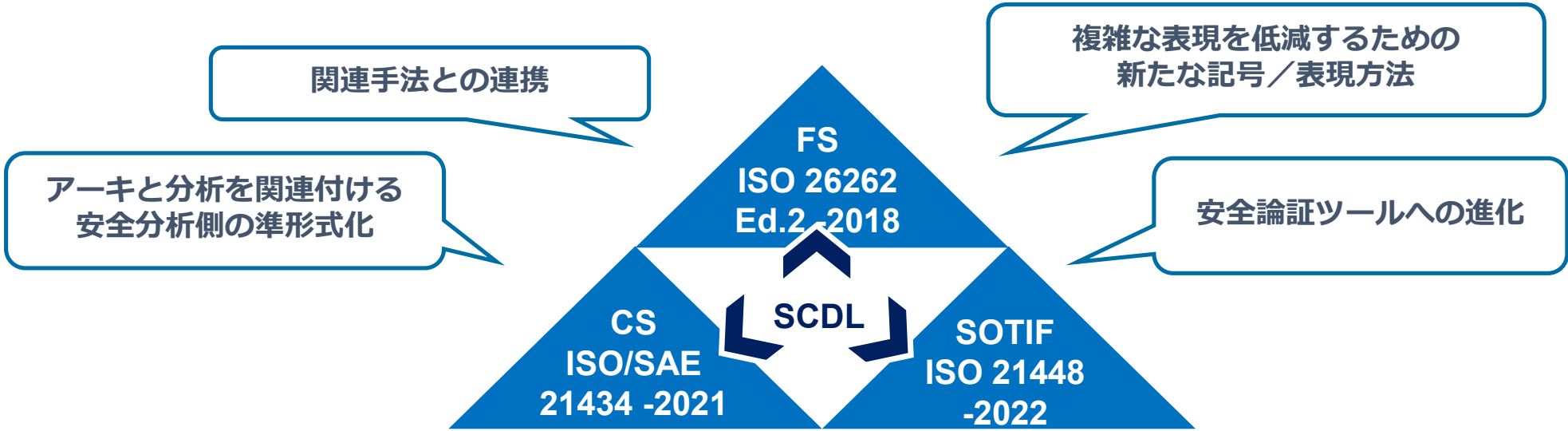


分析表現を含めた
新たな記号／表現方法や
適用事例の拡充

モチベーション：実用性向上

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が必要
- ❑ 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の議論が始まっている
- ❑ 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



アジェンダ

1	ASAM SCDL Next gen.のモチベーション (現行版の課題と限界含む)
2	次世代版への拡張の概要
3	新プロジェクトへのお誘い

SCDL Next Gen.検討プロジェクトへのお誘い

- 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
- ASAM SCDLの新しいプロジェクトを立ち上げ予定
- 皆様からの貴重なお声が, 次世代ASAM SCDLを洗練する
- 今後の予定
 - 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
9	10	11	12	1	1
◆ 9/19 : ワークショップ		◆ TSC: Proposal meeting			



Thank you for your attention

お会いできるのを楽しみにしております