

Concept project proposal for SCDL Next Gen.

Expand SCDL application to SOTIF area

Tomoyoshi Murata
SCN-SG SOTIF-Extension Sub-Working Group

Sep. 19th, 2023

JAPANESE



Agenda

1	SCDLをSOTIFに拡張するモチベーションについて
2	SOTIF拡張サブワーキンググループの検討概要
3	SOTIF拡張のケーススタディの紹介
4	SCDL拡張のための議論のポイント
5	まとめ

SOTIF拡張サブワーキンググループメンバーの紹介

- 2022年4月設立

- メンバー：

小笠原 豊和 (ODEP & Gunma University)

北島 創 (JARI)

越山 勉 (NISSAN)

佐々木 喜好 (MARELLI)

関 康大 (TOYOTA)

田口 研治 (UL Japan)

田中 伸明 (OTSL)

東道 徹也 (DENSO)

西原 秀明 (AIST)

村田 智良 (JARI)

山下 修平 (DNV)

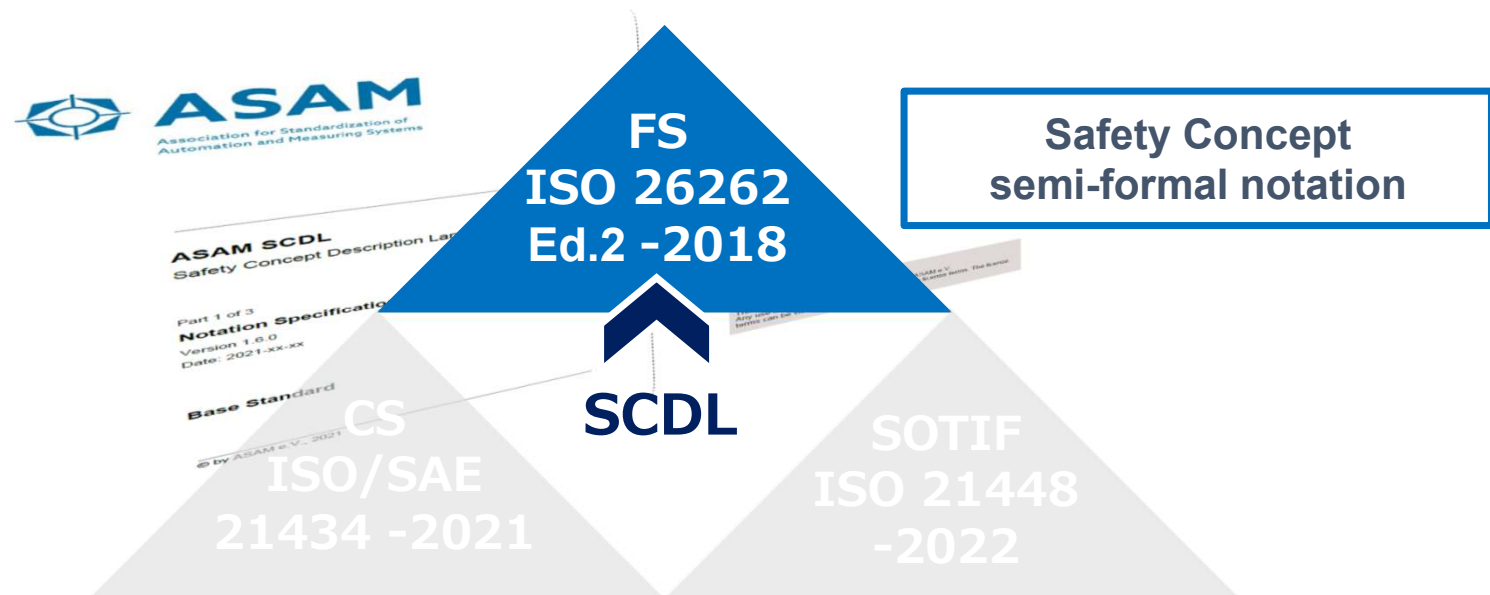
吉田 知樹 (HINO)

渡辺 サンドラ (JARI)

副主査：高田 聖 (DNV)

主査：今井 美紗子 (DNV)

- ASAM Standard SCDL 1.6.0 :2021は、ISO 26262機能安全の安全コンセプトを表記するための標準としてリリースされた
- SCDLは、機能安全規格の適用開発で利用される



1. SCDLをSOTIFに拡張するモチベーションについて

□ SOTIFとは何か？

Safety Of The Intended Functionality

意図した機能の仕様の不十分性、性能限界 又は 合理的に予見可能なミスユースから生じる不合理なリスクがないこと（意図した機能の安全性）

- ISO26262（機能安全）が故障に起因する安全系の規格として先行して発行されたが、ISO21448（SOTIF）は故障だけではカバーできない意図した機能の安全性に着目した規格である

ISO 26262（機能安全）

2018年12月第2版発行

危険の原因：故障

- ・ハードウェア部品の故障
- ・仕様記載ミス、設計ミスなどのヒューマンエラーによる機能不全

ISO 21448（SOTIF）

2022年7月発行

危険の原因：正常機能の不十分、非故障

- ・性能限界や外部環境の影響
- ・ミスユース（誤用）

1. SCDLをSOTIFに拡張するモチベーションについて

□ 背景

安全設計を進めるには、ISO 21448（SOTIF）とISO 26262（機能安全）の活動を連携させる必要があるが、ASAM SCDL1.6は機能安全のために標準化され、SOTIFに対応していない

□ 活動内容

意図機能のアーキテクチャをSCDLで示し、SOTIFの設計検証活動にも活用することで、SOTIFと機能安全の効果的・効率的なインタラクションが可能となると仮定し、ケーススタディで検証する

- ➡ SCDL 1.6をSOTIFで活用し、機能安全とのインタラクションの確認と、追加要件の有無を研究する



2. SOTIF拡張サブワーキンググループの検討概要

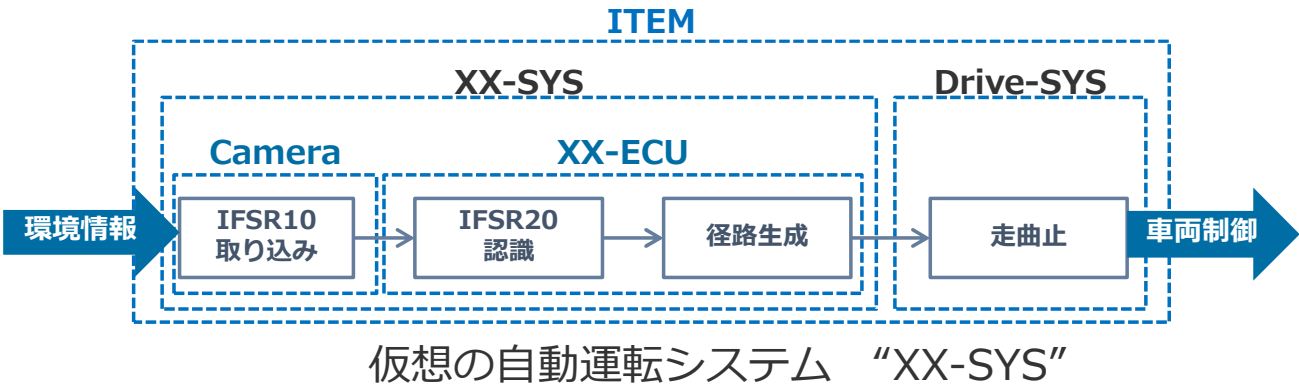
- 意図機能の性能不足の分析やその対処の段階におけるSCDL適用のケーススタディを作成。さらにこの検討結果を機能安全のアイテム定義とみなして安全分析や安全機構の追加の事例を作成する
- この中から、機能要求の性能要件、意図機能の作りこみにおけるプロセス要件記述などに関して、分析表現含めたSCDL拡張の課題を検討する



3. SOTIF拡張のケーススタディの紹介

ケーススタディの実施は、以下のステップで行う

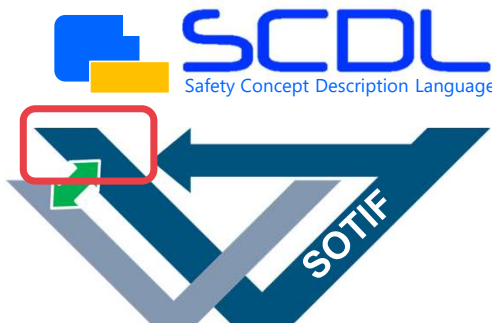
- 1. 仮想の自動運転システム“XX-SYS”を定義する
- 2. 意図機能安全アーキテクチャ構築を安全要求ベースで行う（SOTIF）
- 3. これに基づく安全コンセプトを作成する（機能安全）
- 4. バリデーションからのフィードバックによりアーキテクチャの更新をする（SOTIF）
- 5. 安全コンセプトの見直しを行う（機能安全）



安全目標の定義

U-SG : Universal - Safety Goal
ITEMのハザードは機能安全／SOTIF共通として扱うことにし、その和集合をU-SGと定義

※本ケーススタディのU-SGは
『自動運転を失敗しない』と設定した

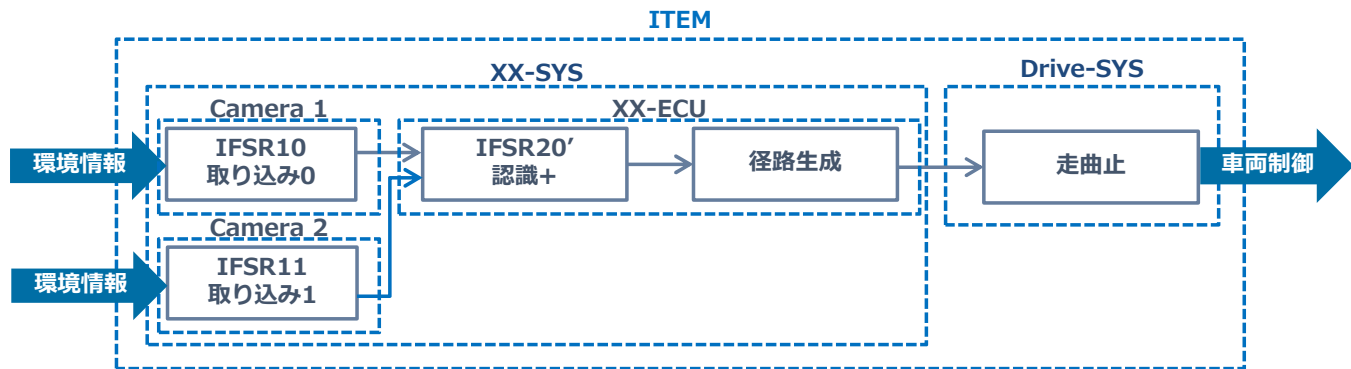


3. SOTIF拡張のケーススタディの紹介

- 1. 仮想の自動運転システム“XX-SYS”を定義する
- 2. 意図機能安全アーキテクチャ構築を安全要求ベースで行う（SOTIF）
 - ・ 意図機能安全アーキテクチャのハザード分析を実施する
 - ・ 分析結果よりリスク対策を検討し、意図機能のアーキテクチャを完成させる

SOTIFの安全要求侵害の原因として以下が挙げたと仮定し、対策を検討した

- （１）原因：カメラからの映像の偽陽性・偽陰性 →対策：カメラを複数とする
- （２）原因：フュージョンにおけるAI学習の不十分性 →対策：ML再学習を行う



SOTIFのハザード分析の際に、**機能的不十分性又はトリガー条件を検知する機能の表現**について、SCDL上で誤解を与えないような表現ができるかが議論となった

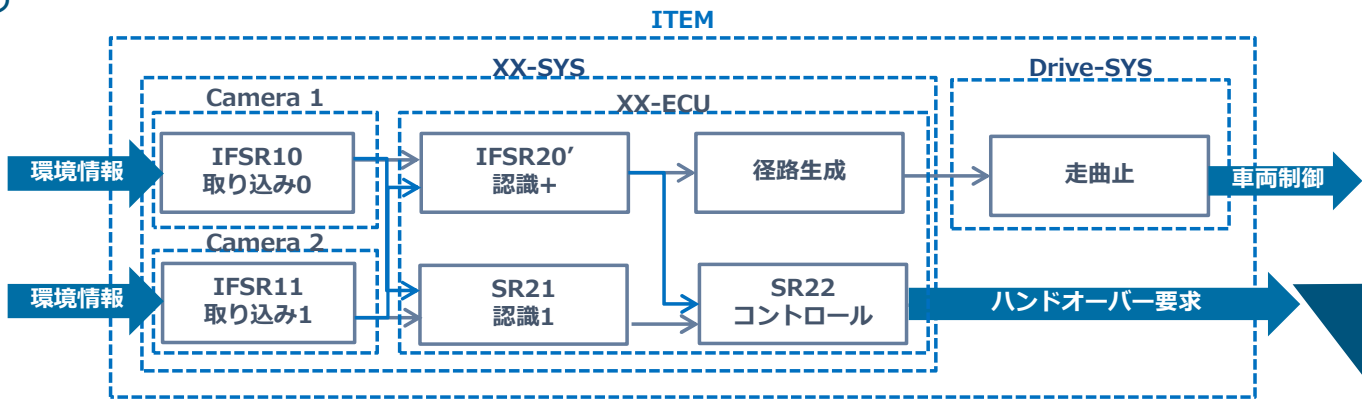
【SCDLにおける性能要求の取り扱い方法】



3. SOTIF拡張のケーススタディの紹介

3. 意図機能アーキテクチャに基づく安全コンセプトを作成する（機能安全）

- 機能安全観点での安全分析を行う
 - カメラの故障はSOTIFで追加した安全機構で対応が可能と考える（カメラの多重化）
 - 認識は、機能安全としてソフトウェア演算などのシングルフェールの対応の検討が必要となる
- 安全分析結果に基づきアーキテクチャを更新する
 - ECU内の演算は、認識に相違があった場合に運転手に必要な操作を促す等のハンドオーバーを行う



IFSR20'の中のMLの対策など、プロセス的安全方策(学習補強、性能向上を含む)をアーキテクチャ上で表現できる方法があるか

【SCDLにおけるプロセス要求の取り扱い方法】

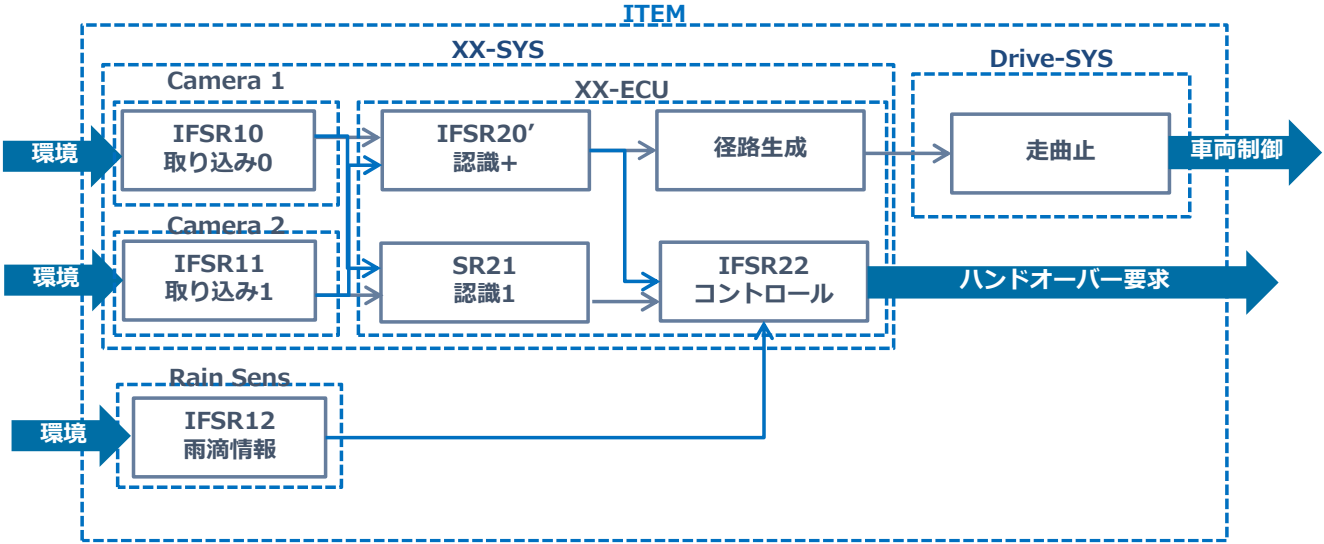


3. SOTIF拡張のケーススタディの紹介

4. バリデーションからのフィードバックでアーキテクチャの更新をする（SOTIF）

- 構築されたコンセプトに基づき設計開発が行われ、バリデーションを実施する
- バリデーション結果より、雨天走行時に雨滴によるカメラのセンシング性能低下の指摘あり

→安全方策を検討する：意図機能要求としてIFSR12を追加し雨滴情報をIFSR22へ送信する



* SR22は意図機能要求の対応を追加し機能の再定義を行うため、SR22⇒IFSR22とIDを変更している

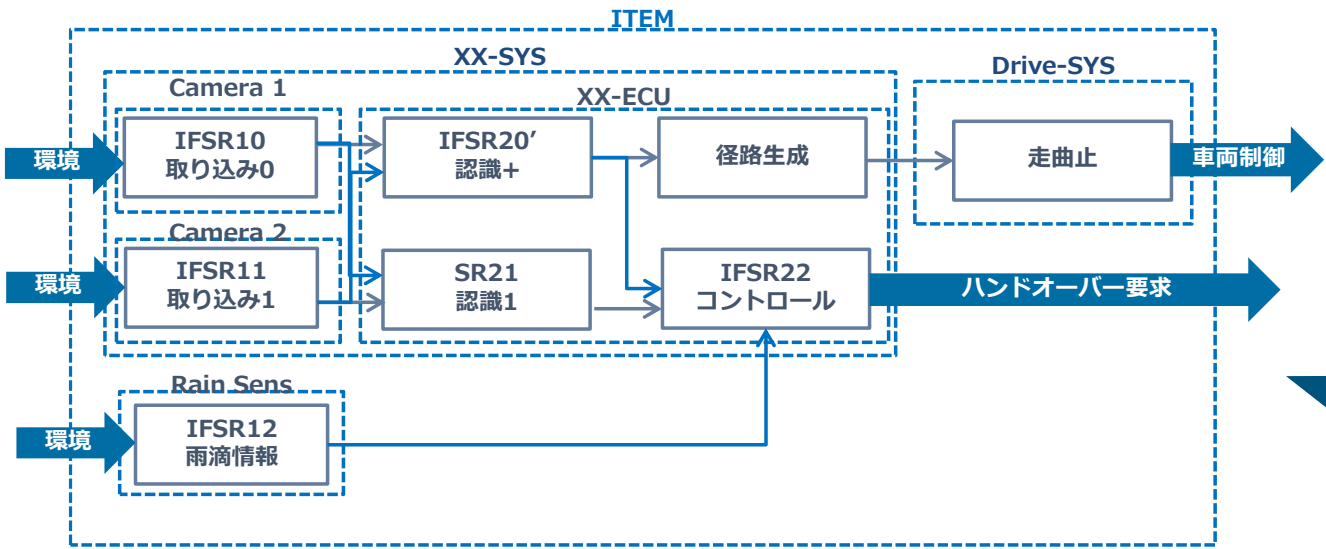
* 本ケーススタディ題材においてはレインセンサ情報のセンサフュージョン等には使用しておらず、雨滴情報は雨滴の一定量超過の判断とその後のコントロールとハンドオーバーの為にのみ使用している。



3. SOTIF拡張のケーススタディの紹介

5. 安全コンセプトの見直しを行う（機能安全）

- SOTIF的更新が行われた以下を元に安全コンセプトの更新を実施する
- 機能安全の安全分析の更新
 - 意図機能安全要求のIFSR12, IFSR22はSOTIF対応で追加されたが、いずれも機能不全を起こすと新たなハザードの候補となる為、機能安全でのHARA再実施が必要



SOTIFの安全機構(IFSR12の故障)の故障した場合の対策を表現方法が特に必要か
【SOTIFの安全機構の故障対応の表現方法】

4. SCDL拡張のための議論のポイント

ケーススタディより、SCDL拡張のための議論ポイントとしてHLR（High Level Requirement）を抽出し、議論を実施した

① SCDLにおける性能要求の取り扱い方法

- ➡ 機能的不十分性又はトリガー条件を検知するなどのSOTIF意図機能の表現について、SCDL上で誤解を与えないような表現ができるか検討する
- ➡ 性能の不十分性などを分析するためSOTIF性能要求をSCDL上で表現する方法を検討する

② SCDLにおけるプロセス要求の取り扱い方法

- ➡ SOTIF安全論証に必要なプロセス的安全方策(学習補強、性能向上を含む)の表現について(構造図、表など表現方法は未定)検討する

③ SOTIFの安全機構の故障対応の表現方法

- ➡ SOTIFの安全機構の故障(latent faultに相当)の場合の対処の表現について

4. SCDL拡張のための議論のポイント

HLRの議論結果より得られた知見を整理する

① SCDLにおける性能要求の取り扱い方法

- ➡ 機能的不十分性又はトリガー条件を検知するなどのSOTIF意図機能の表現はアーキテクチャではないためSCDLでの表現が難しい
- ➡ 非機能要求は表せないが、意図機能アーキテクチャはSCDLで表現することは可能である

② SCDLにおけるプロセス要求の取り扱い方法

- ➡ プロセス的安全方策も非機能的な安全要求となるため、アーキテクチャでの表現は難しい
(コンストレインツ標記は可能、プロセス的安全方策は他のサブワーキンググループでも検討)

③ SOTIFの安全機構の故障対応の表現方法

- ➡ 機能安全の対応として対処できれば問題ないためSOTIF特有の課題ではない

5. まとめ

今回のケーススタディでは以下の事例を取り上げた：

- SOTIFの安全機構が機能安全の安全機構を兼ねる事例
- SOTIFアーキテクチャに機能安全の安全機構を追加する事例
- 意図機能アーキテクチャが更新された時のSOTIFと機能安全のインタラクションや機能安全のイテレーションの事例

まとめ：

- SOTIFの意図機能アーキテクチャはSCDLで提示でき、機能安全活動との効果的で効率的な連携が可能である
- SOTIF対策は非機能要求が多く、対策結果をアーキテクチャでは表現できない。そのため、SCDLとしての新たな記号・文法の追加は現時点では見えていない
- 分析結果の非機能要求とアーキテクチャとの効果的・効率的な連携については継続して検討する

➡今後の活動

- SCDL Next Generationへの具体的な提案内容としてケーススタディを含め整理する
- 他のサブワーキンググループと共通の課題は協働し、さらなる効果的な利用方法を検討

Thank you for your attention