安全三規格時代にSCDLに期待される役割

SCN-OC 2023

20231229 DNV 山下

本日の内容

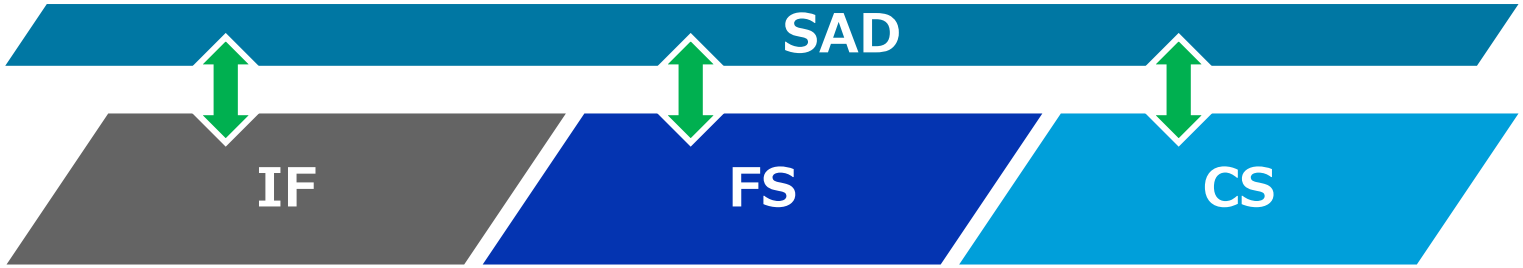
★アブストラクト----------

　ISO 26262，ISO 21448，ISO 21434が求めるWPの特性を理解することで　各規格間の連携時にSCDLが果たすべき役割を見出すことができる：各方面でご好評をいただいているFCワイズアプローチ概要を紹介する

➡　SG活動方向性見直しアナウンス

三規格の連携プロセス？

三規格の競合問題を解き 方策やメカニズムの重複を最小化するために アーキ・仕様・デザイン を 効果的・効率的に整合してシステムをまとめたい



IF➡FS➡CS の順序で検討するのは間違いなさそう：

・まず意図機能を作り込む，これに機能安全的SMを追加する，最後に安全アーキを考慮しながらCS方策を検討する

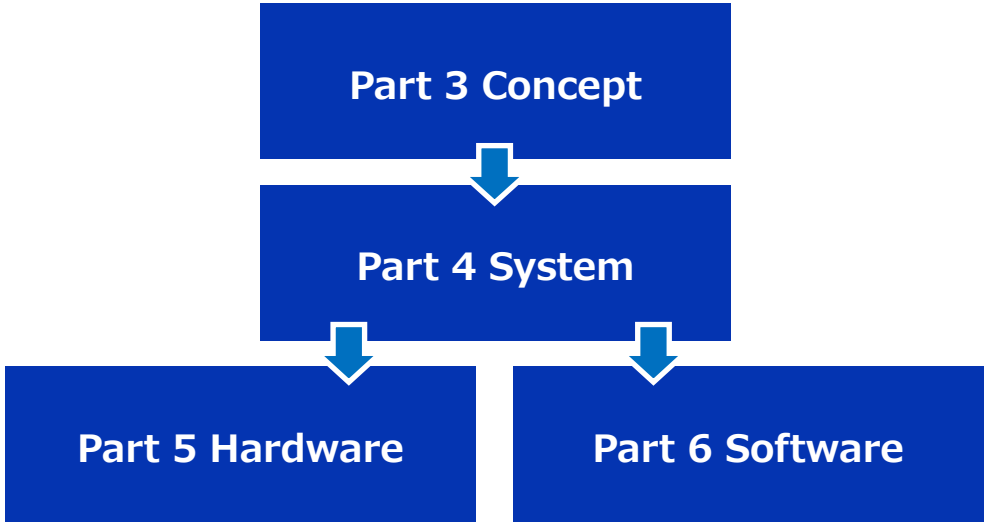
・規格の名前では　ISO 21448➡ISO 26262➡ISO 21434

レイヤフェイズモデル

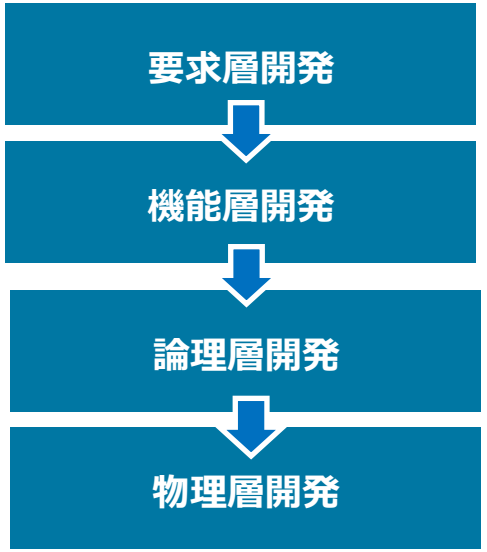
LPM（レイヤフェイズモデル）：設計レイヤを開発フェイズ定義に用いたプロセスモデル

・FSの コンセプト・システム・HW/SW のプロセスモデルがこれにあたる

・SE領域では 要求層・機能層・論理層・物理層 というモデルも知られている



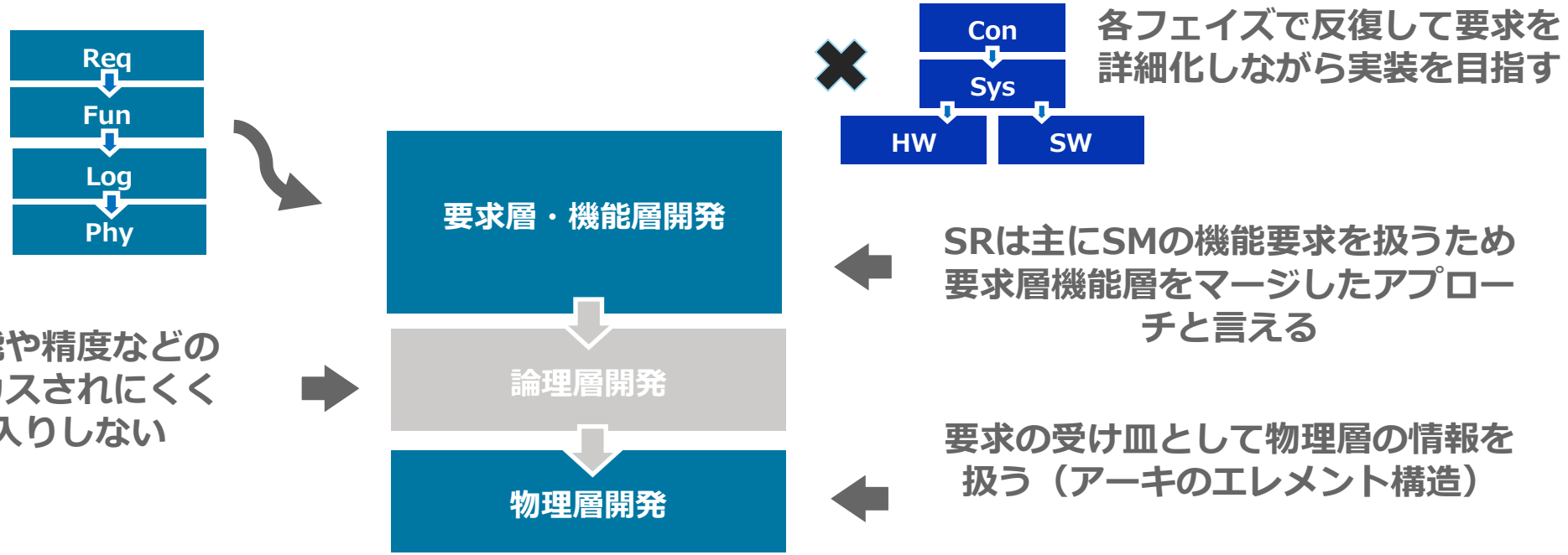
ISO 26262のLPM



SEのLPM

FS(ISO 26262)のレイヤフェイズモデル

FSにおける安全要求SRのエレメントへの配置は SEフェイズで考えると物理層を一部考慮しながら要求層・機能層をマージしたアプローチといえる. 規格ではこれをコンセプト～HW/SWまで反復する

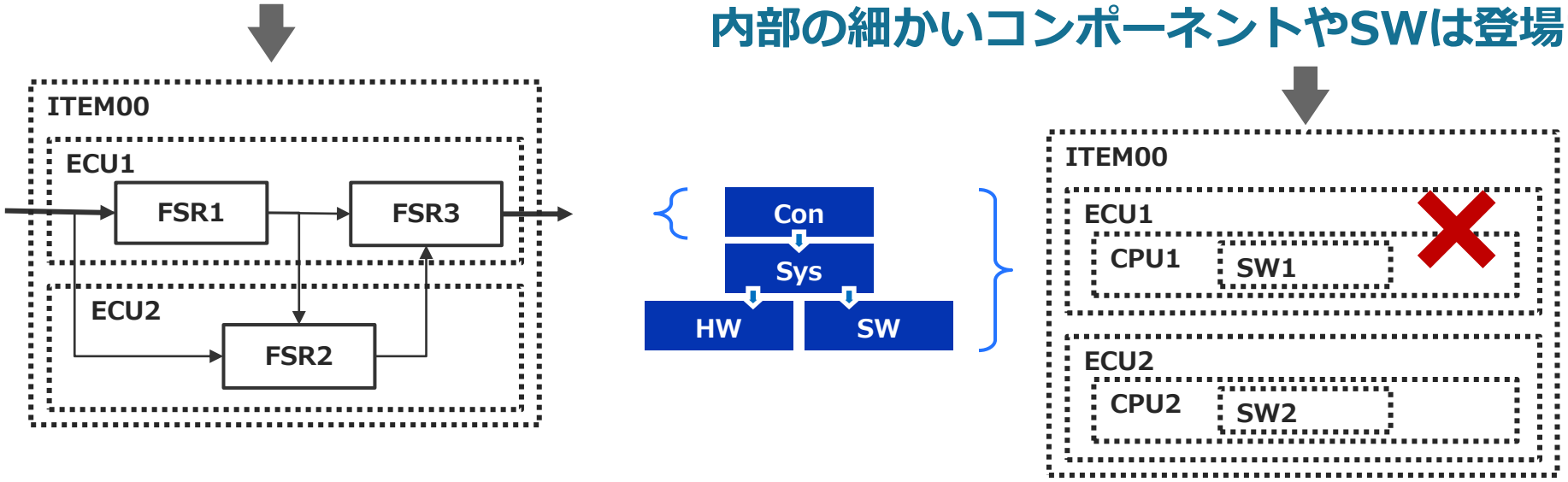


FSアプローチの特徴

レイヤを跨がないことでSR粒度をコントロールする：

例えばFSCでは典型的にはECUレベルのエレメントだけを登場させる

内部の細かいコンポーネントやSWは登場させない



ただし多くの場合 実態としては 開発初期から詳細アーキ（SAD）が検討される

→　トップダウンアプローチは 説明（＝安全論証）の為のロジックと言える

SOTIF(ISO 21448)のレイヤフェイズモデル

活動は主にIFの性能や精度を論じる→機能の性能要求→論理層での作りこみ にフォーカスしたものになる：

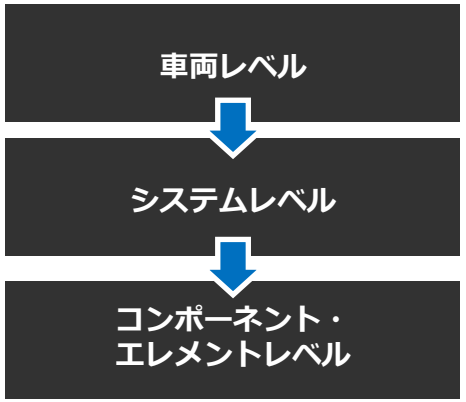
・車両～システム～コンポーネント, システム～エレメント，OEM～Tier N 等のレイヤ概念が混在する

・要求切り口では SG→FSR/TSRに相当する VLSSから’SOTIF(関連)要求’が導出されると理解される

EE実装関連のWPとしてはクローズ5の’仕様と設計‘が相当する

・中身は 要求仕様・機能仕様・設計仕様とされている

・SOTIF的緩和策仕様は冗長構成などFSのSMと関連するためFSC/TSCと合冊される場合があるとされる

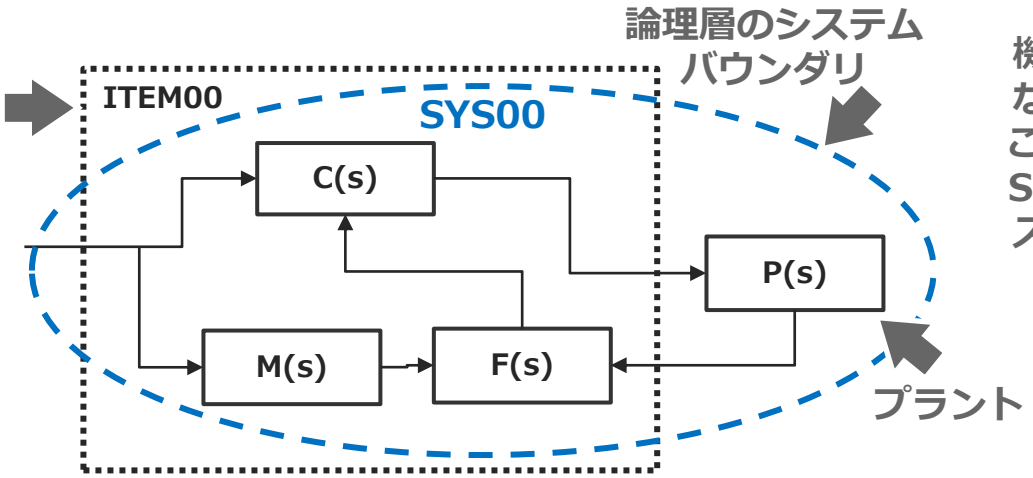


SOTIFアプローチの特徴

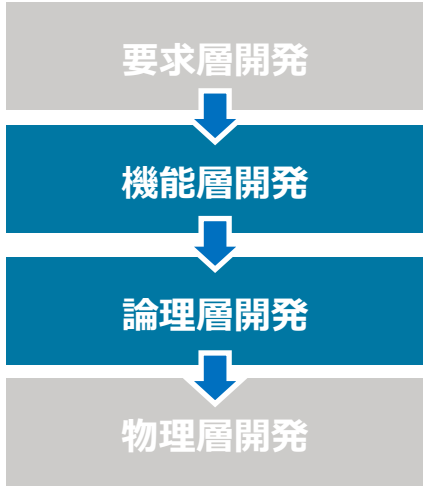
システムやコンポーネントのバウンダリは分散開発における性能分担で配慮されるが 関心事の中心は機能層・論理層の作り込み. この立場のエンジニアから見るとシステムはプラント(制御対象)を含む絵になり 規格でもFSを参照するとき以外はアイテムの語は使われない

- IFの機能仕様が分析対象
- この機能にまつわる性能や精度を論じる→アルゴリズムが勝負
- 性能未達となった場合には機能追加や部品追加も考える

車両レベル機能が複数アイテムに跨る場合がある という扱いになっている



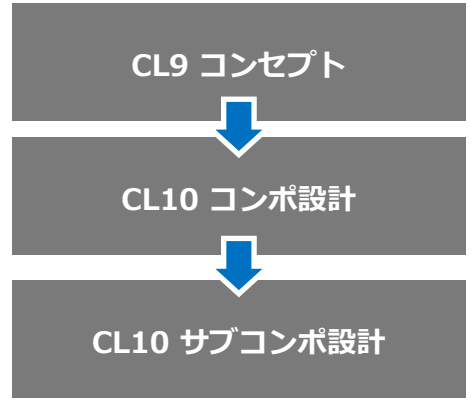
機能の性能・精度要求などから論理層の作りこみ活動が中心になる. SOTIF的対策としてシステムアーキの更新に及ぶケースもある

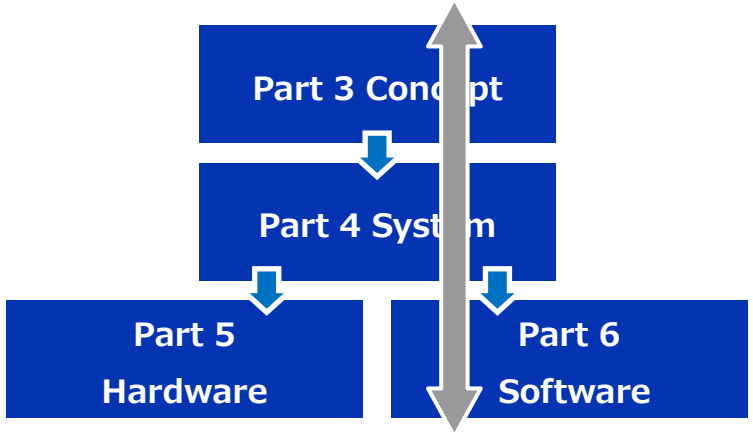


CS(ISO 21434)のレイヤフェイズモデル

LPMはコンセプト～サブコンポの表現で与えられている

・分析や方策を論じる対象は環境含む広い概念. 一方で最終攻撃対象は 典型的にはSWであり 大きくレイヤを跨いでの分析となる





・CSコンセプトはアイテムレベルのCSRとCSコントロールなどを含む上位概念. CSスペック (=CSR+アーキ設計) がFSのコンセプトに相当する

・アイテム定義は運用環境記述を含む. 環境そのものとアイテムとのインタラクションが脅威シナリオ・攻撃パス特定に用いられる

・アーキの構成要素はコンポーネントの語に統一されている. FSのエレメントと異なり 機能や論理の単位で扱われる場合もある

CSアプローチの特徴

SC対策の CSG→CSRのうちEEに実装されるものについては FSアプローチと同様のトップダウンの要求詳細化の取り扱いが有効といえる

一方で

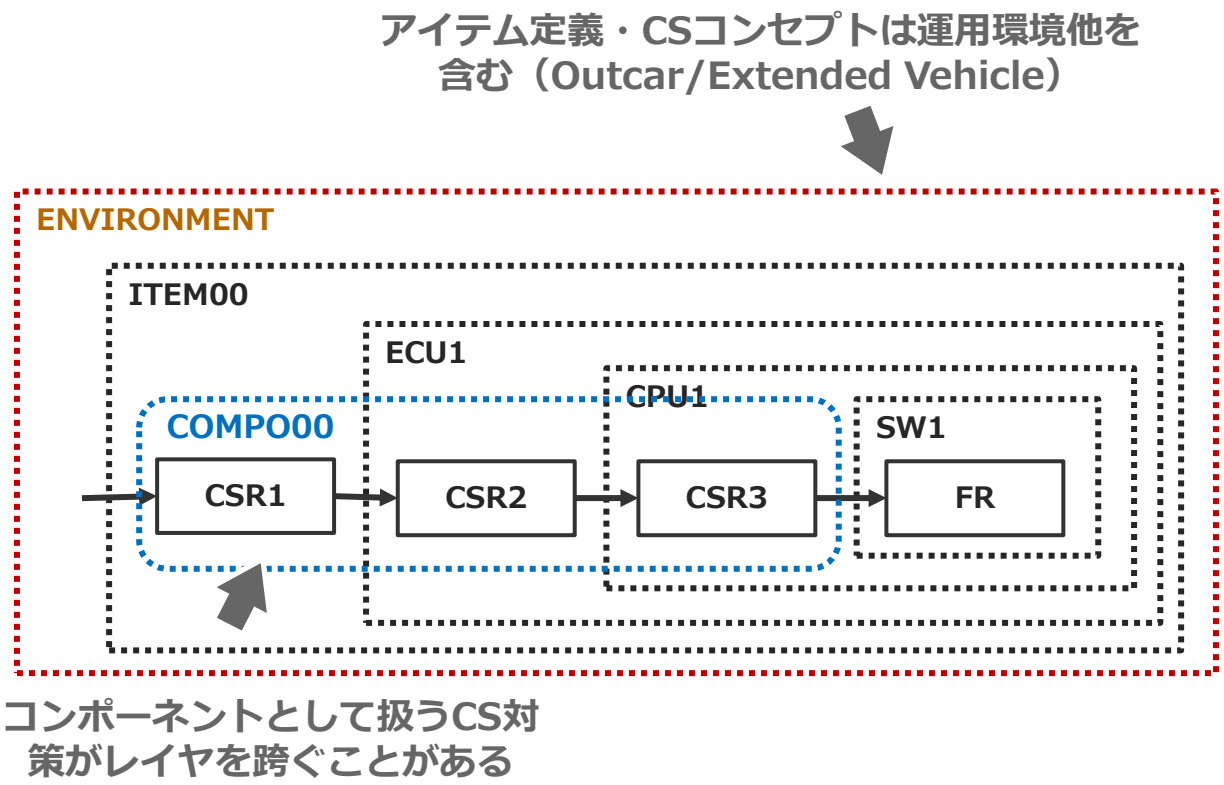
・既存コンポをカタログ買いする

・機能・論理コンポとして対策を論じる

・多層防御型のCSメカニズムを検討する

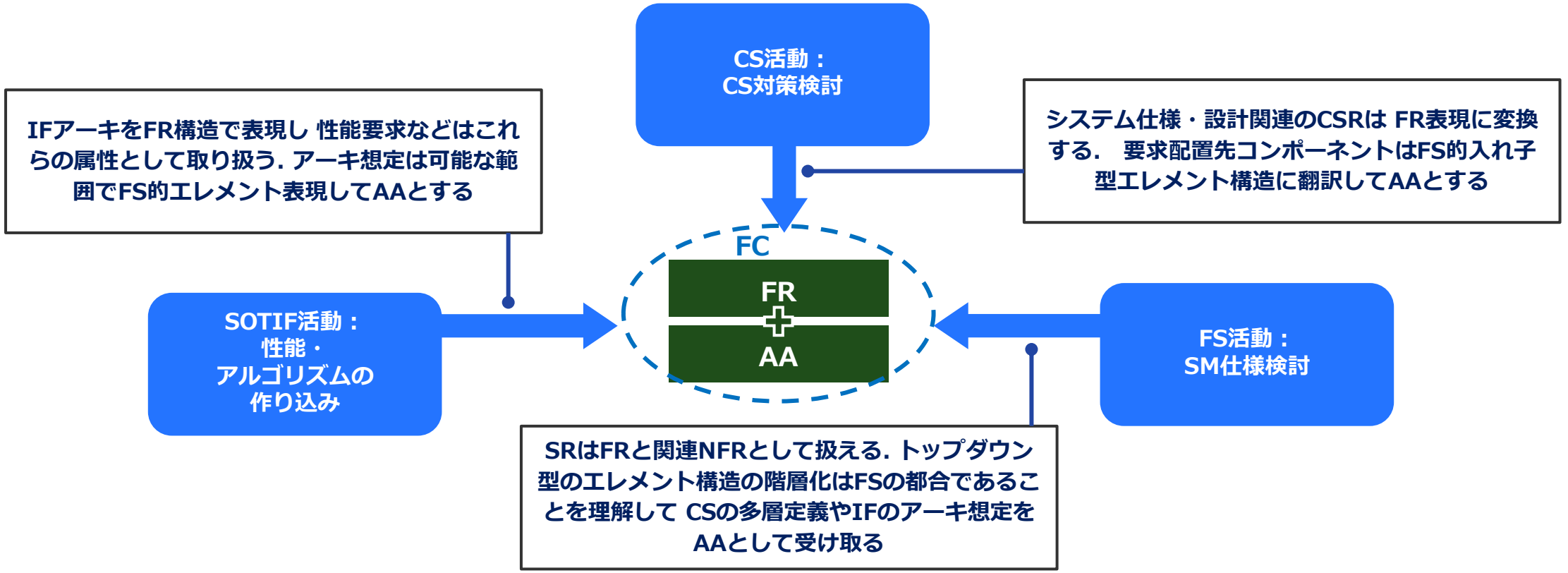
などのケースではいずれも 大きく

エレメントのレイヤを跨ぐ議論になる



三規格仕様整合におけるFCの役割

三規格はそれぞれのフォーカスが異なり共通のLPMは描きにくい. しかし ここまで見てきたとおり システム設計仕様に関する三規格共通項として 機能コンセプト（FC）= 機能要求（FR）+ エレメントアーキ想定（AA）がコミュニケーションツールの候補に挙げられる



FC(機能コンセプト)の概念復習

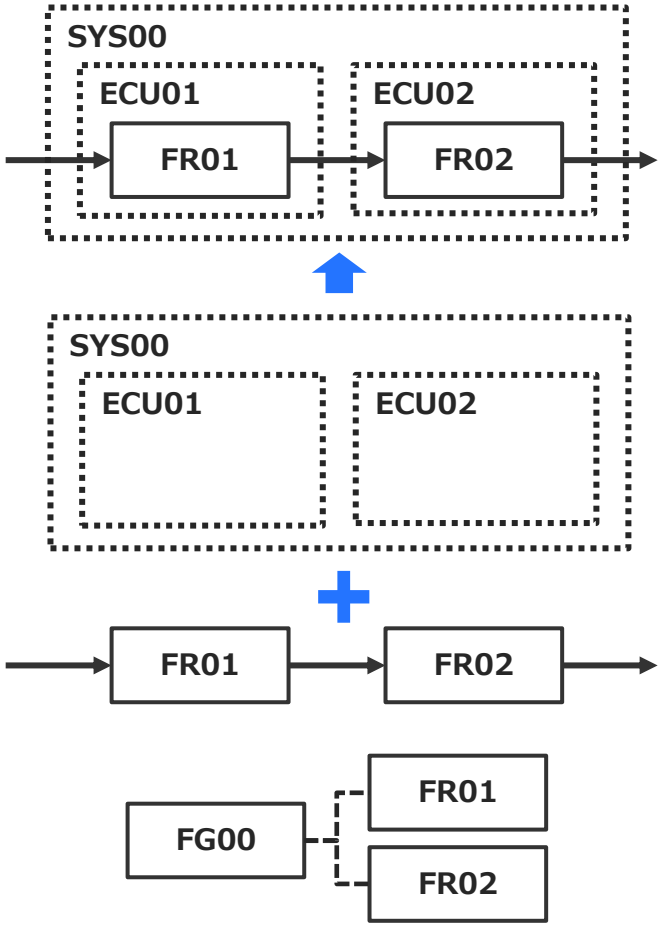
三規格間のコミュニケーションに有効と考えられるFC（機能コンセプト）は ISO 26262のFCやPAAと類似の概念であり SAD（システムアーキ設）の一部とみなすことができる：

・FC＝FR+AA：機能要求をアーキ想定に配置したもの. FR構造をエレメントから構成されるAAに配置することで 物理レイヤにおける 機能的な役割分担と依存関係を示すことになる

ここで

・AA(アーキテクチャ想定)：物理アーキの想定を指す. エレメント切り口の構造を中心に 通信ネットワーク仕様や電源構成の情報などを含む

・FR(機能要求)：各要求の仕様と それらのつながり すなわち構造からなる. 構造は一般的な機能ブロックダイアグラムで示すことができる範囲のものを指す. 要求として上位要求とのトレーサビリティなども重要



三規格時代こそSCDLの役割が重要になる

本日の内容

★アブストラクト----------

　ISO 26262，ISO 21448，ISO 21434が求めるWPの特性を理解することで　各規格間の連携時にSCDLが果たすべき役割を見出すことができる：各方面でご好評をいただいているFCワイズアプローチ概要を紹介する

➡　SG活動方向性見直しアナウンス

SWG構成見直し

'SysMLにダメ出しするわけにいかない'という反語表現でダメ出ししながら10年間議論してきたがそろそろ融和の時代か：SysMLユーザにSCDLを使ってもらう方向に舵を切りたい

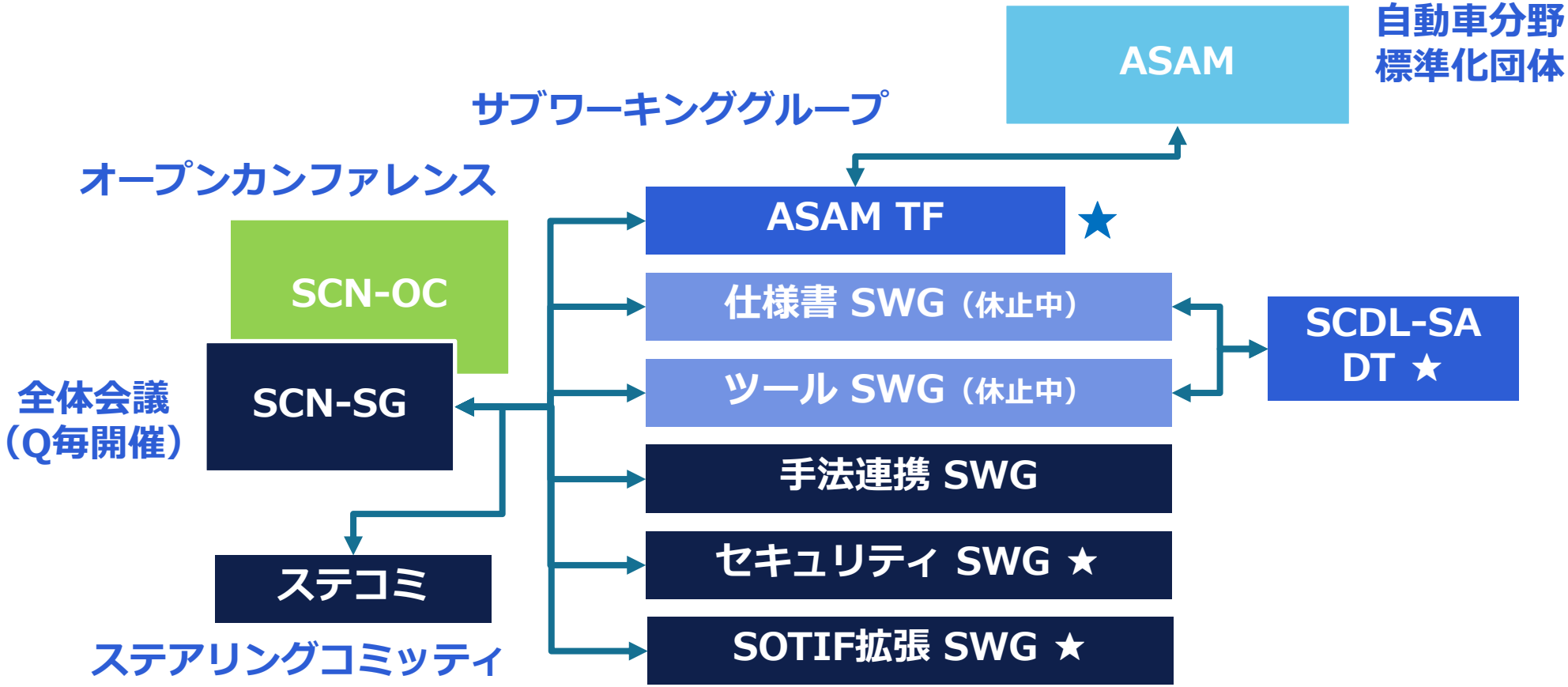
ASAMのNEXT GENの取り組みの一つとしてSA-DTで議論してきたダイアグラム簡素化がもたらす恩恵の一つが SysMLとの親和性向上といえる：
例：デコポンの要求Gr・ペアリングをSRVAで提示するなどのダイアグラム取り回し向上策
（ただし1.6の表現を廃止するわけでは無い：互換性を確保し，トレーニング用，オーサリング時のGUI，レビュー時のダイナミックドキュメント向け表現として発展させる方向）

➡ 対応案
・トヨタ関さんをリーダーとするSCDL 2.0 SWGを新設する（次頁）
・SCDL仕様改訂の作業母体を本SWGとしASAMプロジェクトプロポーザルの計画を練り直す
・活動の主題の一つとして 'SysMLのSCDL拡張プロファイルを定義する' を掲げる
・SA-DTと手法連携SWG，および休止中SWGを再構成する
・本日SCN-OC以降追加メンバ募集を行う
・年明けキックオフ？活動形態や出口戦略はSWGの中で相談する

SCN-SGの組織（2022.11時点）

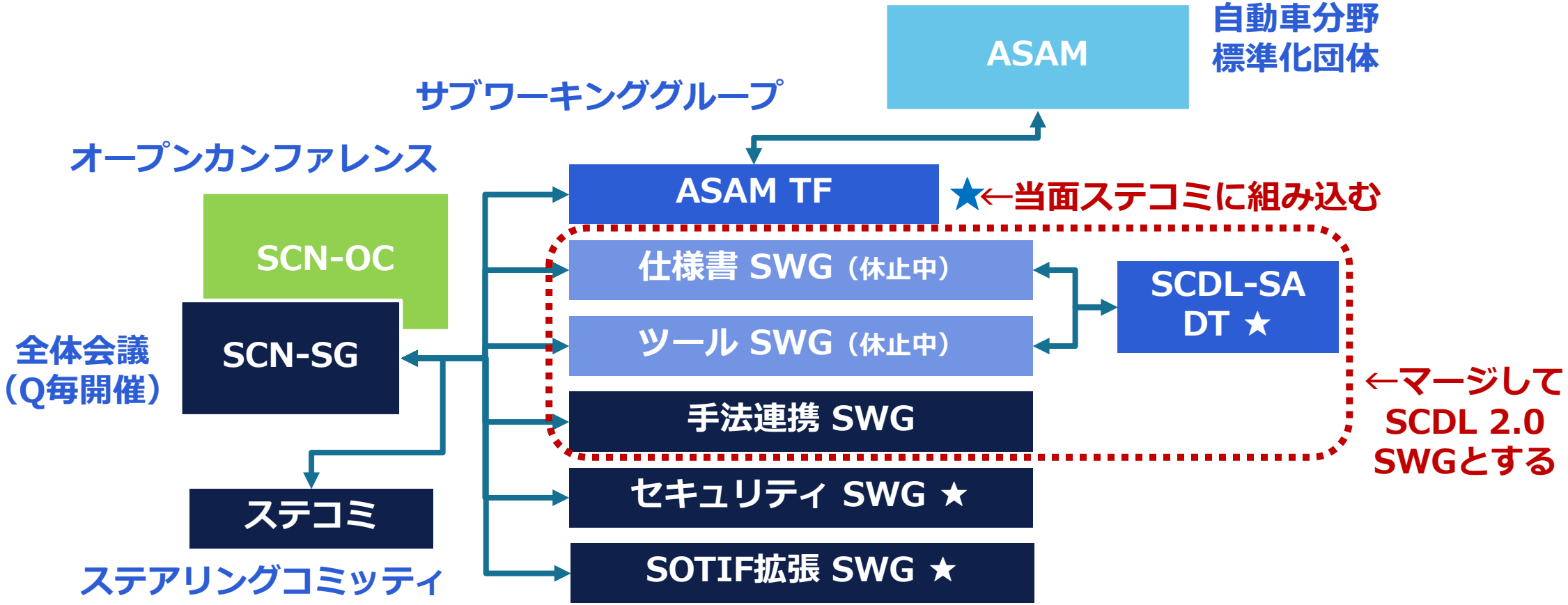
- 本年より SOTIF拡張SWG，SCDL-SA DT，ASAM TF 新設

★：ASAM SCDL 1.7.0提案に向けて活動中



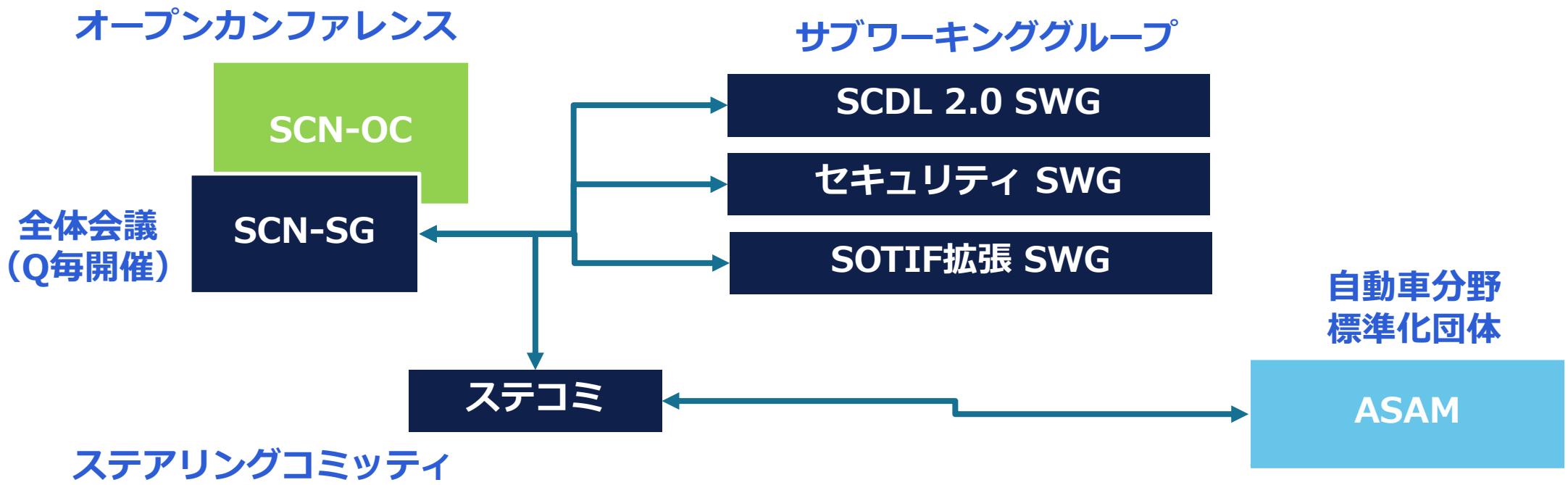
SCN-SGの組織（2023.12時点）見直し案

- ASAM-TFはステコミに組み込む
- 休止中SWGなどを発展的に解消してワンチームとする



SCN-SGの組織（2024.01以降）案

- SOTIFとセキュリティは活動を継続する
- それ以外の休止中SWGなどは発展的に解消してワンチームとする
- みなさまの参加お待ちしております



本日の内容

★アブストラクト----------

　ISO 26262，ISO 21448，ISO 21434が求めるWPの特性を理解することで　各規格間の連携時にSCDLが果たすべき役割を見出すことができる：各方面でご好評をいただいているFCワイズアプローチ概要を紹介する

ご清聴ありがとうございました

➡　SG活動方向性見直しアナウンス