SCN-SG Safety Concept Notation Study Group

SCDL Safety Concept Description Language

SCDL Cybersecurity Expansion

日本語版

SCN-SG Security-SWG

プレゼン：DNV 山下修平　(チームリーダ名古屋大学倉地先生の代行として)

Sept. 19th, 2023

ASAM Association for Standardization of Automation and Measuring Systems

SCDL
Safety Concept Description Language

Agenda

1	Motivation
2	’Safecomp Case Study’ & additional discussion
3	Outcomes from the case study
4	CSM expression
5	CAL expression
6	Communication network expression

Agenda

1	Motivation

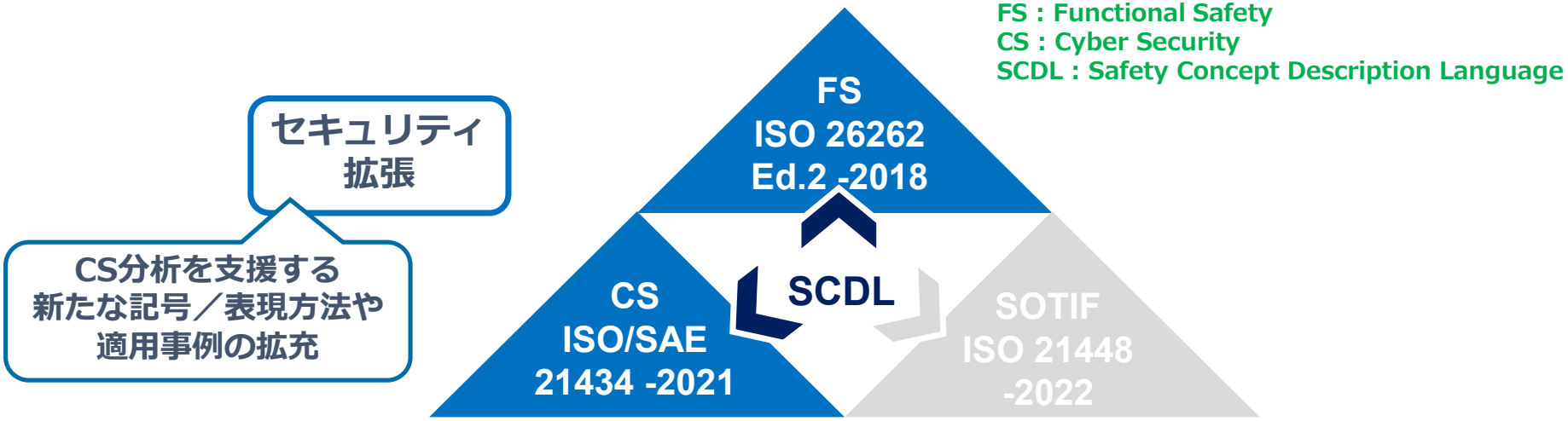
SCDL Safety Concept Description Language

提案の動機

機能安全・サイバセキュリティ両規格のコミュニケーションを

SCDLで効果的にサポートしたい

➡ このために 適用事例の充実と ここから見えてくる文法のアップデートを行う



SCDL
Safety Concept Description Language

Agenda

1	Motivation
2	’Safecomp Case Study’ & additional discussion

SCDL Safety Concept Description Language

Safecomp事例と原設計に対するCSM追加のケーススタディ

ISO 21434の取り組みではSFOPに関するセキュリティ確保の十分性を説明しなければならない　一方

このSFOPの中の最重要トピックである安全に関しては ISO 26262の安全コンセプトがアーキテクチャ的情報を提供する　すなわち安全コンセプトはサイバセキュリティ対策・メカニズムを論じる際の重要入力になると言える

この観点からSCDLが両規格間のコミュニケーションをサポートする事例を作成した

➡　Safecompケーススタディ：

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

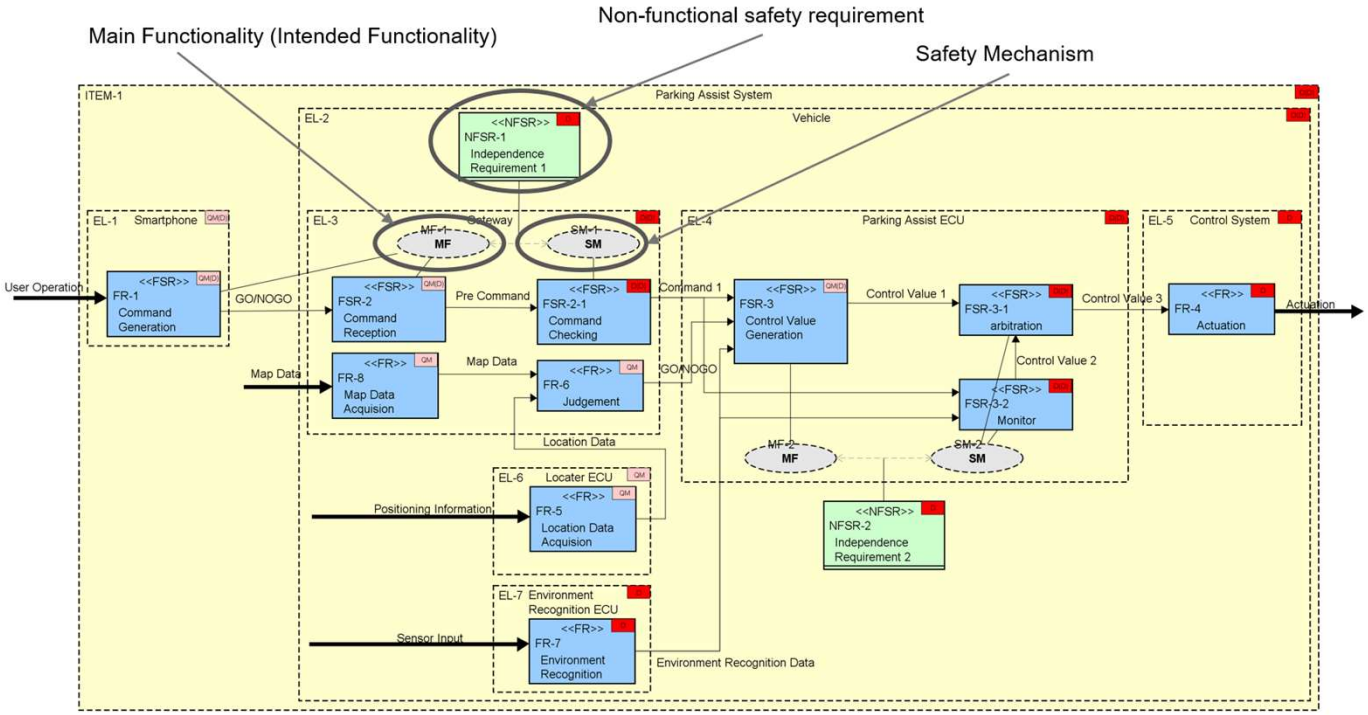
SFOP : Safety – Finance - Operability - Privacy
CSM : Cyber Security Mechanism

SCDL Safety Concept Description Language

Safecomp Case Study

“Threat Analysis Framework for Safety Architectures in SCDL” @SafeComp2020 で用いたSCDL記述されたシステムモデルの例

- Parking Assist System (ITEM-1) = Smartphone (EL-1) + Vehicle (EL-2)
- Vehicle (EL-2) = Gateway (EL-3) + Parking Assist ECU (EL-4) + Control System (EL-5) + Locator ECU (EL-6) + Environment Recognition (EL-7)



SCDL Safety Concept Description Language

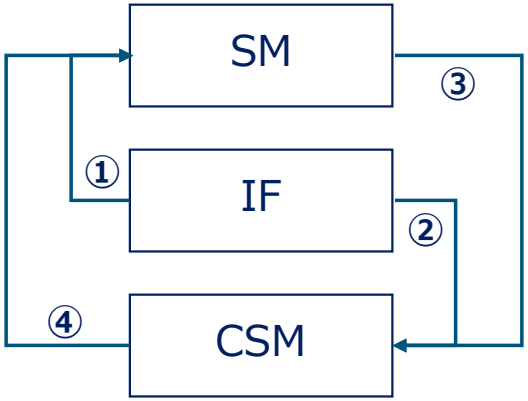
Safecomp事例におけるCSM検討プロセス

意図機能（IF）に対して安全メカニズム（SM）とサイバセキュリティメカニズム（CSM）を考える場合に例えば
以下のような手順が想定される

Step.1 IFにSMを追加する①
Step.2 IF＋SM（＝SC）にCSMを追加する②③
Step.3 CSMにSMを追加する④

さらにこの際，以下のような議論を考慮することになる
・SMがCSMを兼ねる場合がある①vs②
・SMとCSMがコンフリクトする場合は調停必要①vs②
・CSMはS以外のFOPの対策も必要になる②③

Safecompの事例ではこのうちのstep.1とstep.2を扱った
この後さらにstep.3の議論の追加を検討中



CSM : Cyber Security Mechanism
IF : Intended Functionality
SM : Safety Mechanism
SC : Safety Concept
SFOP : Safety – Finance - Operability - Privacy

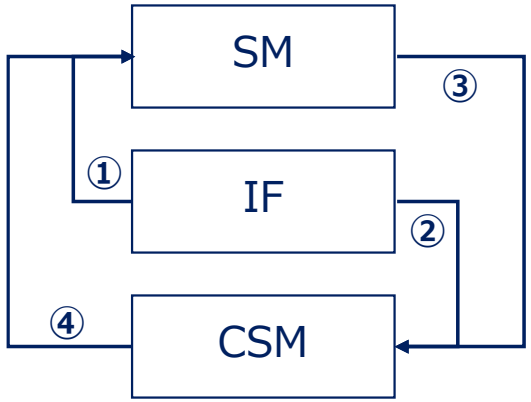
SCDL Safety Concept Description Language

CSM検討プロセス：原設計にCSMを追加するケース

Safecomp事例とは異なるアプローチとして 意図機能（IF）に対して安全メカニズム（SM）とサイバセキュリティメカニズム（CSM）をそれぞれ検討してマージする手順が可能なのかをスタディ中：

Step.1 IFにSMとCSMをそれぞれ追加する①②
Step.2 SMにはCSMを，CSMにはSMの 追加要否を検討する③④

SCDLのモデルを用いて二つのアプローチの比較を行い，プロセス最適化などにも有効であることを検証したい



CSM : Cyber Security Mechanism
IF : Intended Functionality
SM : Safety Mechanism
SC : Safety Concept
SFOP : Safety – Finance - Operability - Privacy

SCDL Safety Concept Description Language

Agenda

1	Motivation
2	Safecomp case study & additional discussion
3	**Outcomes from the case studies**

SCDL Safety Concept Description Language

これまでのスタディから見えたきたこと

Safecomp事例など これまでのSCDLによる機能安全・サイバーセキュリティ間のコミュニケーションのケーススタディの結果 少なくとも以下の検討が必要であることが分かった

・サイバセキュリティメカニズムの機能・論理コンポーネント表示：サイバセキュリティの議論においての'コンポーネント'は機能安全のエレメントのバウンダリを跨ぐことがありSCDLが提供しているエレメント表示に適さない

・サイバセキュリティ要求等のCAL表示：サイバセキュリティにおけるCALもしくはこれに相当するリスクレベル/保障レベルの表示を機能安全におけるASILと並行して行いたいが現行SCDLは対応していない

・通信ネットワーク表示：脅威分析における攻撃界面・攻撃径路の特定に必要なネットワークなどの接続先の表現法が定義されていない

以下項目毎に論じる

CAL : Cybersecurity Assurance Level
ASIL : Automotive Safety Integrity Level

SCDL Safety Concept Description Language

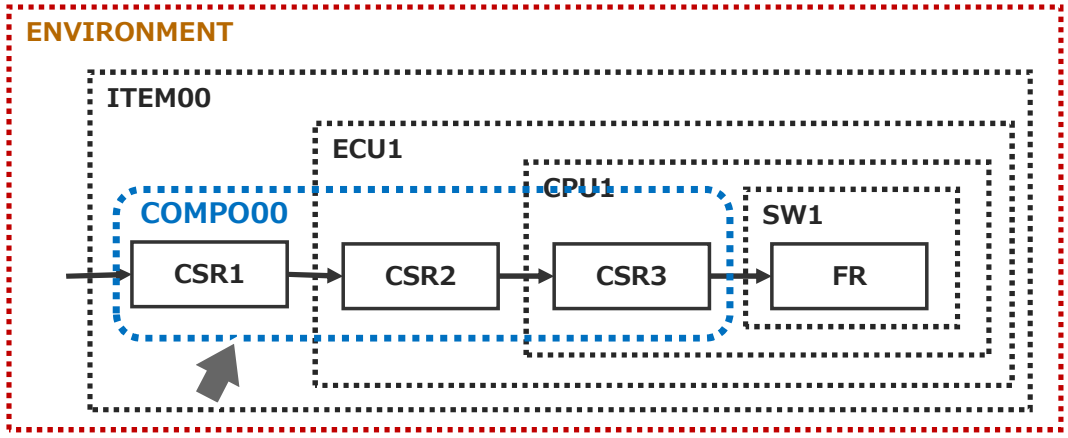
Agenda

1	Motivation
2	Safecomp case study & additional discussion
3	Outcome from the case study
4	CSM expression

SCDL Safety Concept Description Language

サイバセキュリティメカニズムの機能・論理コンポーネント表示

サイバセキュリティ対策・メカニズムが複数エレメントのレイヤを跨ぐことがある
このような場合 機能コンポーネント・論理コンポーネントによるサイバセキュリティメカニズムの提示が行われる これらはSCDL 1.6における要求グループとして取り扱うことで表記・分析・詳細化に供することが可能と考えられる



コンポーネントとして扱うサイバセキュリティメカニズムが
異なる粒度のエレメントレイヤを跨ぐことがある

Agenda

1	Motivation
2	Safecomp case study & additional discussion
3	Outcome from the case study
4	CSM expression
5	CAL expression

SCDL Safety Concept Description Language

サイバセキュリティ要求等のCAL表示

サイバセキュリティ要求およびエレメント・コンポーネントにはCALもしくはCALに相当するリスクレベルを表示可能とする　これにより
- 当該機能要求に関連するサイバセキュリティゴールの存在が識別可能となる
- サイバセキュリティ要求が配置されたエレメントであることが識別可能となる
- 予め定められた設計ルールなどに基づくサイバセキュリティ対策の検討が可能となる

CAL : Cybersecurity Assurance Level
ASIL : Automotive Safety Integrity Level

表示法は下表に示す通りとする
- ASIL下段にCALの欄を設ける，ただしCALは省略できる (1.6互換)
- CALを単独表示する場合はブランクのASIL欄とともに表示する
- エレメントもこれらに準じる
- サイバセキュリティコンポーネントは要求Grで表現する，ASIL/CALの扱いは要求，エレメントに準じる

	要求	エレメント	要求Gr （論理/機能コンポーネント）
ASAM SCDL 1.6	ASIL SR-ID and/or SR-NAME	ASIL ELE-ID and/or ELE-NAME	REQ-GR-ID and/or REQ-GR-NAME
SCDL NEXT GEN	ASIL CAL SR/CSR-ID and/or SR/CSR-NAME	ASIL CAL ELE-ID and/or ELE-NAME	ASIL CAL REQ-GR-ID and/or REQ-GR-NAME

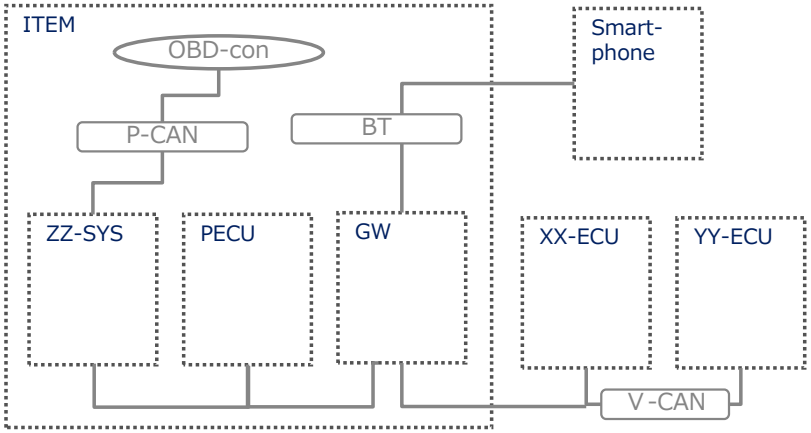
Agenda

1	Motivation
2	Safecomp case study & additional discussion
3	Outcome from the case study
4	CSM expression
5	CAL expression
6	Communication network expression

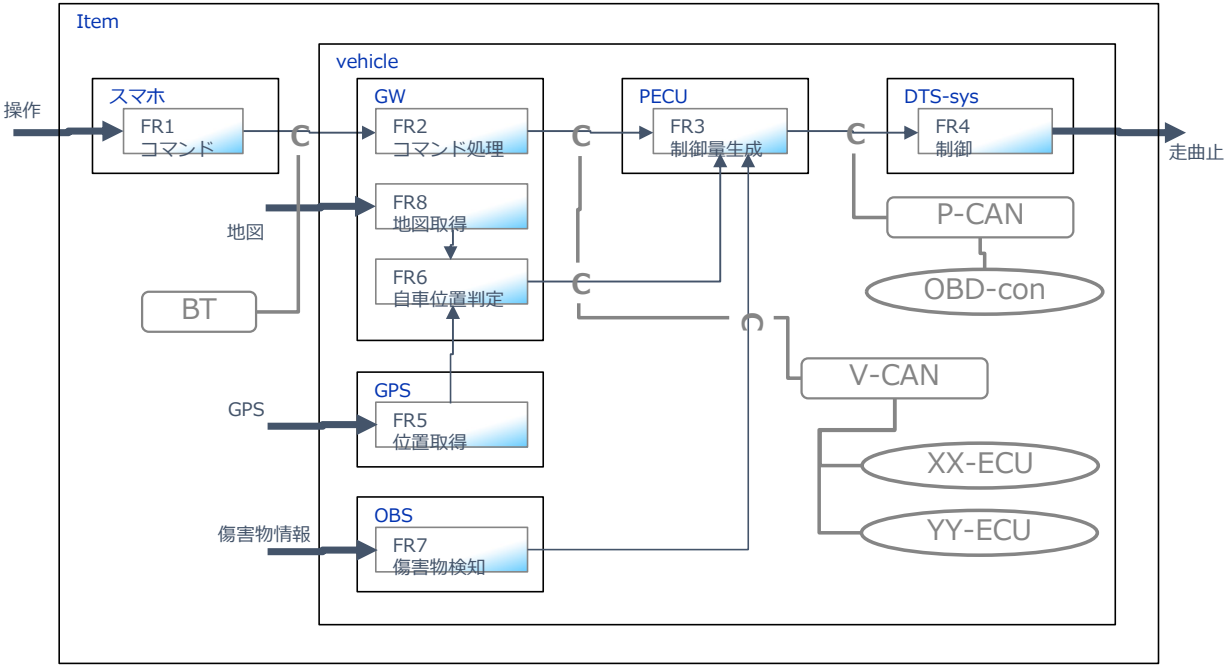
SCDL Safety Concept Description Language

通信ネットワークの表示

・現行SCDLによる安全コンセプト図で不足するものとして攻撃界面・攻撃径路に結び付く接続手段やシステム外の接続先情報がある　この為の記号を追加する： エレメントレベルの接続図を定義する（Type1）またコンセプト図のインタラクション（矢印）の接続手段を個々に表記，さらにこれにつながる他のエレメントなども表記できることとする（Type2）
・なお　SCDL記述された安全コンセプト図では 機能資産は安全/機能要求，情報資産はインタラクション，物理資産はエレメントで表現されるのでこれらに対する記号追加は不要，安全非関連の各種資産（e.g.サービス機能）についても同様



Type1：エレメント構造レベルのネットワーク表記例



Type2: 安全コンセプト上のネットワーク表記例

Summary

Summary

SCDL Safety Concept Description Language

Summary

SCDL NEXT GENプロジェクトにおけるサイバセキュリティ関連活動として以下を提案する

1．FSとCSの連携事例の充実：

・Safecomp事例のリファインと対比プロセスの検討によるSCDLの有効性の検証を行う

・この中で必要記号類の追加検討を行う

・これら両規格連携におけるSCDL適用事例をASAM SCDL 2.0（仮称）仕様書の付録として提案する

2．SCDL文法のアップデート案検討：

・現時点で明らかになっている　CAL追加，機能・論理コンポーネント対応，通信ネットワーク表示追加の仕様書案を作成する

➡　みなさまの合流をお待ちしております

Thank you for your attention

Question?