SCN-SG Safety Concept Notation Study Group

SCDL
Safety Concept Description Language

SCDL Cybersecurity Expansion

In English

SCN-SG Security-SWG

Presentation : DNV Shuhei Yamashita

(on behalf of Associate Professor Ph.D. Ryo Kurachi in Nagoya University)

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

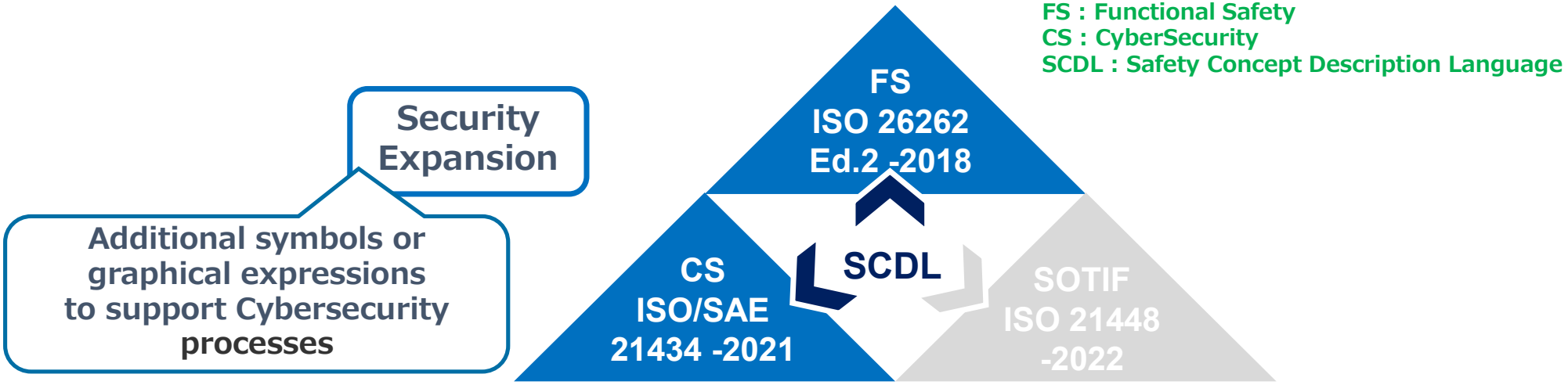
1	Motivation

SCDL
Safety Concept Description Language

Motivation

We aim to effectively support communication between functional safety and cybersecurity standards using SCDL. To achieve this, we plan to enhance our application examples and make necessary grammar updates based on the insights gained from these cases.

FS : Functional Safety
CS : CyberSecurity
SCDL : Safety Concept Description Language



SCDL
Safety Concept Description Language

Agenda

1	Motivation
2	’Safecomp Case Study’ & additional discussion

SCDL
Safety Concept Description Language

‘Safecomp Case Study’ and additional one

In the context of ISO 21434 compliance efforts, it is necessary to explain the adequacy of security assurance regarding SFOP . On the other hand, for the most critical topic within SFOP, which is safety, ISO 26262 provides architectural information through safety concepts. Therefore, safety concepts can be considered important inputs when discussing cyber security measures and mechanisms.

From this perspective, a case study has been created to demonstrate how SCDL supports communication between both standards.

SFOP : Safety – Finance - Operability - Privacy

➡ Safecomp case study :

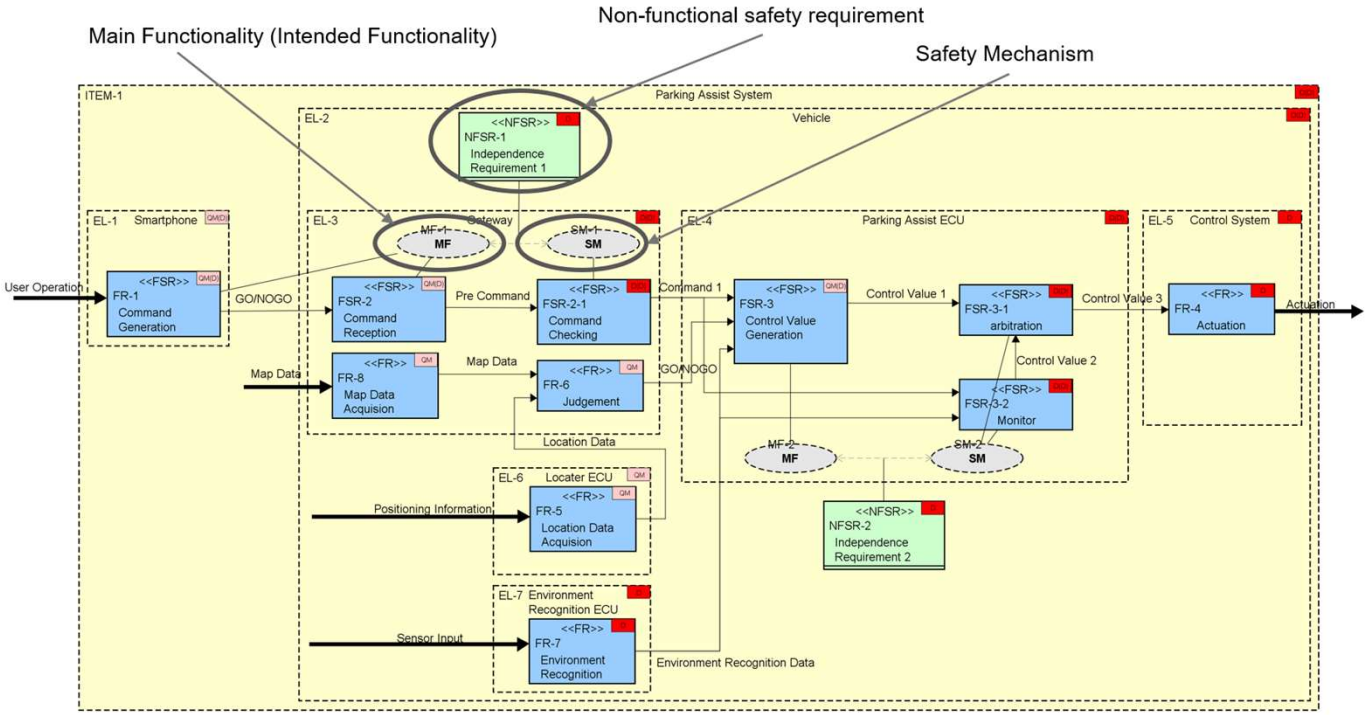
“Threat Analysis Framework for Safety Architectures in SCDL” @SafeComp2020

SCDL Safety Concept Description Language

Safecomp Case Study

The example of a system model in SCDL from “Threat Analysis Framework for Safety Architectures in SCDL” @SafeComp2020

- 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)

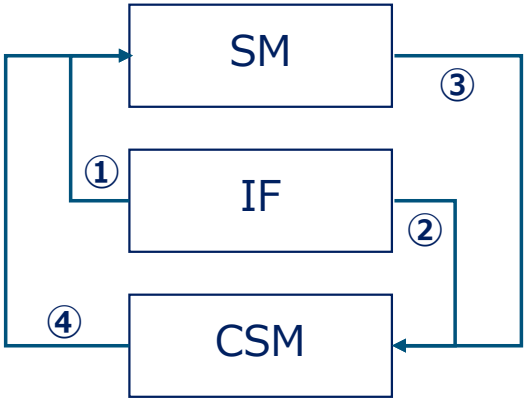


SCDL Safety Concept Description Language

CSM consideration process in Safecomp case studies

When considering safety mechanisms (SM) and cyber security mechanisms (CSM) for Intended Functionalities (IF), the following steps are assumed, for example:

- Step 1: Adding SM to IF (①).
- Step 2: Adding CSM to IF+SM (= SC) (② and ③).
- Step 3: Adding SM to CSM (④).



Furthermore, during this process, the following discussions need to be taken into consideration:

- The possibility of SM also serving as CSM (① vs. ②).
- Arbitration may be necessary in cases where SM and CSM conflict (① vs. ②).
- CSM may require measures for FOPs other than S (② and ③).

Safecomp's case studies have covered steps 1 and 2, and we are currently considering adding discussions related to step 3.

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

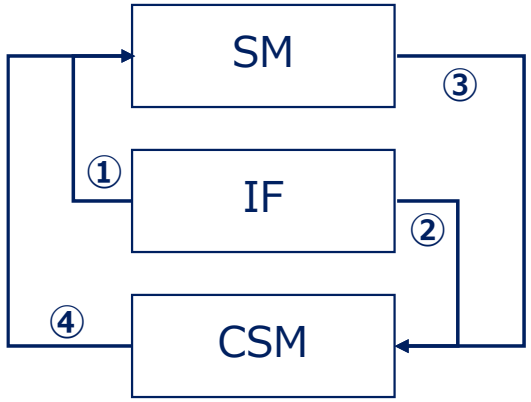
SCDL
Safety Concept Description Language

CSM consideration process : a different one from Safecomp case studies

We are currently studying the possibility of an alternative approach, where safety mechanisms (SM) and cyber security mechanisms (CSM) are individually considered for Intended Functionalities (IF) and then merged. The steps for this approach are as follows:

Step 1: Adding SM and CSM separately to IF (① and ②).
Step 2: Considering the necessity of adding SM to CSM and vice versa (③ and ④).

The studies is aimed to compare these two approaches using SCDL models and verify their effectiveness, particularly in terms of process optimization.



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

Outcomes from the case studies

Based on the results of previous case studies on communication between functional safety and cyber security using SCDL, it has become clear that at least the following considerations are necessary:

・Representation of Cyber Security Mechanism (as Functional/Logical Components) : In cyber security discussions, the concept of ‘components’ may span the boundaries of functional safety elements, making the element representation provided by SCDL unsuitable.

・Representation of CAL for the Cyber Security Requirements and other elements : In the context of cyber security, there is a need to represent CAL or equivalent risk levels alongside ASIL used in functional safety. However, the current SCDL does not provide support for this parallel representation.

・Communication Network Representation: SCDL does not define a representation method for connecting endpoints such as networks, which is necessary for identifying attack interfaces and attack paths in threat analysis.

Each of these considerations in more detail is provided in the following pages.

CAL : Cybersecurity Assurance Levels
ASIL : Automotive Safety Integrity Level

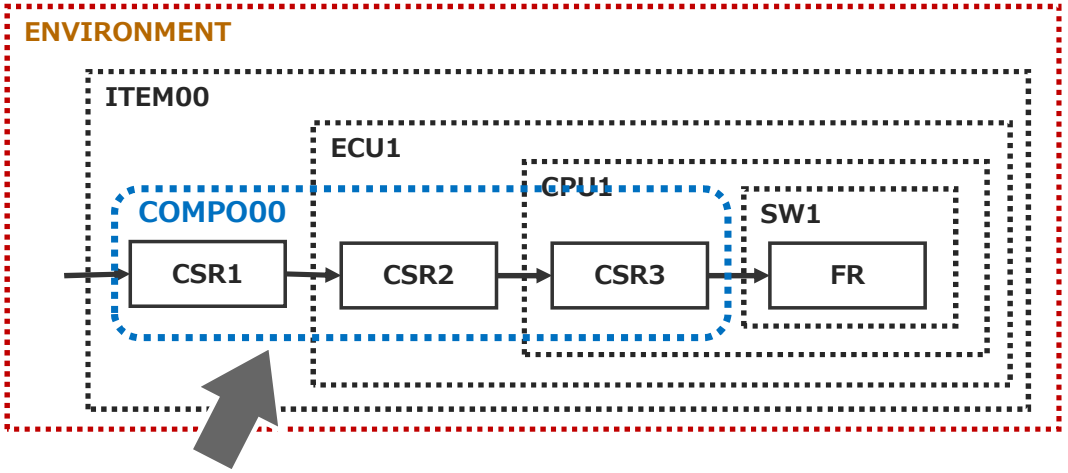
SCDL Safety Concept Description Language

Agenda

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

Representation of Cyber Security Mechanisms as Functional/Logical Components

Cyber security measures and mechanisms may span multiple layers of elements. In such cases, the presentation of cyber security mechanisms can be carried out through functional components and/or logical components. These can be handled as requirement groups in SCDL 1.6, enabling their representation, analysis, and detailed elaboration.



Cyber security mechanisms treated as components may span elements at different levels of granularity within the layer.

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

Representation of CAL for CSR and for others

CAL or an equivalent risk level can be displayed for cyber security requirements and elements/components. This enables:

- Identification of the presence of cyber security goals related to specific CSR/FR.
- Recognition of elements/components where cyber security requirements are allocated.
- Facilitation of considerations for cyber security measures based on predetermined design rules, etc.

CAL : Cybersecurity Assurance Level
ASIL : Automotive Safety Integrity Level

The representation method is as follows:

- Create a CAL placeholder beneath the ASIL column, allowing for the omission of CAL (compatible with SCDL 1.6).
- When displaying CAL independently, it should be presented alongside a blank ASIL column.
- Elements should follow a similar format.
- Cyber security components should be represented within requirement groups, and the treatment of ASIL/CAL should align with that of requirements and elements.

	Requirement	Element	Requirement Gr (Logical / Functional component)
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

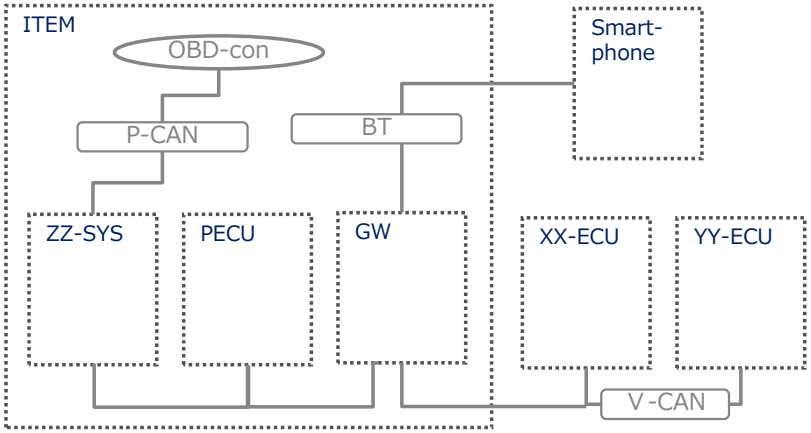
Communication network expression

To address the deficiencies in the current SCDL for safety concept diagrams in CS use, symbols need to be added for connecting means associated with attack surfaces and attack paths, as well as information about external system interfaces. This will involve:

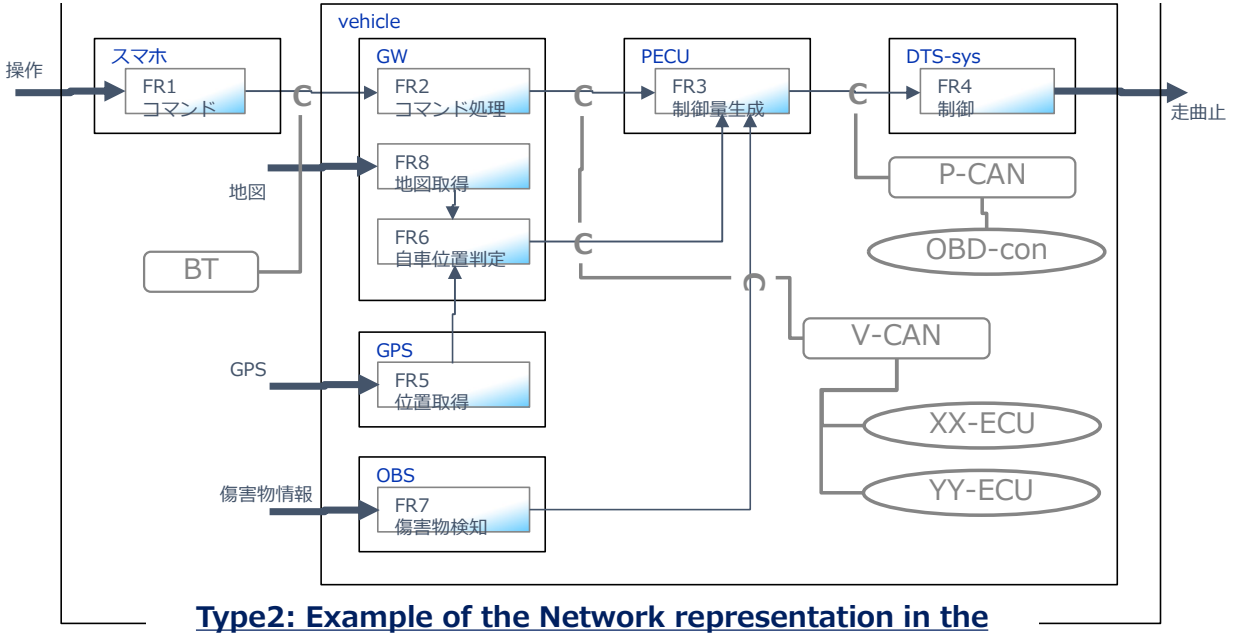
・Defining an element-level connectivity diagram (Type 1).

・Individually indicating the connecting means of interactions (arrows) in concept diagrams, with the ability to represent other connected elements, etc. (Type 2).

It's important to note that in safety concept diagrams described in SCDL, functional assets are represented by safety/functional requirements, information assets by interactions, and physical assets by elements. Therefore, there is no need to add symbols for these categories. The same applies to various non-safety-related assets, such as service functions.



Type1 : Example of the Element-level connectivity diagram



Type2: Example of the Network representation in the safety concept diagram

Summary

Summary

SCDL
Safety Concept Description Language

Summary

As part of the SCDL NEXT GEN project's activities, we propose the following for the Cybersecurity topics :

1. Enhancement for the case study of communication between FS and CS :

・To refine the Safecomp case studies and compare it with another approach to evaluate the effectiveness of SCDL. During this process, we will consider the addition of necessary symbols.
・To propose SCDL application examples in the context of collaboration between both standards as an appendix to the ASAM SCDL 2.0 (tentative) specification.

2. Consideration of SCDL Grammar Updates:

・To propose specification drafts for known updates to the SCDL grammar, including the addition of CAL, support for functional/logical components, and the inclusion of communication network representation.

We look forward to welcoming your participation in these efforts.

Thank you for your attention

Question?