Association for Standardization of
Automation and Measuring Systems

英和対訳版

ASAM SCDL

Safety Concept Description Language

安全コンセプト記述言語

Part 2 of 3

Practical Example

取り組み事例

Version 1.6.0

Date: 2021-11-09

Base Standard

標準ドキュメント

この日本語版はオリジナルの英語版の翻訳であり、情報提供のみを目的としている。齟齬がある場合、英語版のASAM SCDL Practical Example Version 1.6.0 標準ドキュメントが優先される。

The Japanese version is a translation of the original in English for information purposes only. In case of a discrepancy, the English version of the ASAM SCDL Practical Example Version 1.6.0 standard document shall prevail.

目次

まえがき

SCDL は、ISO 26262 の文脈と意味に基づいた、単一の安全コンセプト仕様の表記法である。ISO 26262 では準形式記法が推奨されており、SCDL は準形式記法を提供する。また、SCDL は、安全コンセプトの仕様化、分析、レビューに必要な直感的な表現力を備えている。本書では、取り組み事例を説明する。例題には、設計されたアーキテクチャ図、要求表、エレメント表が含まれている。本書を通じて、SCDL の表記法を理解することができる。

1 取り組み事例

1.1 概要

本章では、ASAM SCDL 表記仕様に準拠したアーキテクチャ図の例を示す。本例は、ドライバの操作量により車両制御をおこなうシステムである。このシステムで想定している安全目標は「意図に反した過大出力なきこと」である。この安全目標を達成するための安全アーキテクチャを、２つの例で示す。１つは、Figure 1 に示した冗長設計による安全アーキテクチャである。もう１つは、Figure 2 に示した上限値制限設計による安全アーキテクチャである。

1.2 要求表およびエレメント表によるアーキテクチャ図の補足

Figure1 および Figure2 のアーキテクチャ図は、要求表およびエレメント表にて補足される。SCDL は、これらの表をどのように活用するかは規定していない。しかしながら、これらの表を活用することで、アーキテクチャ図の理解が深まることが期待される。Figure 1 のアーキテクチャ図に表記されている要求、制約条件、エレメントについては、Table1～4 で、Figure2 については Table5～8 にてそれぞれ説明する。

1.3 冗長設計による安全アーキテクチャの例

1.3.1 アーキテクチャ図

入力デバイス E-1 では、ドライバ操作検知要求 MFR-1 とドライバ操作冗長検知要求 SR-11 により、ドライバ操作量が冗長に検知される。その検知結果に基づいて、セレクトロー要求 SR-12 により選択がおこなわれる。制御量の算出は、コントローラ E-2 の制御量演算要求 MFR-2 および制御量冗長演算要求 SR-21 により冗長に実施される。そして、異常時駆動制限要求 SR-22 により、制御量演算結果が異常かどうかを判断し、必要に応じて制御量を調整する。出力デバイス E-3 の駆動要件 MFR-3 により、制御量に応じてモータが駆動される。出力デバイス E-3 には、駆動モニタ要求 SR-31 があり、動作角検知要求 SR-32 へ入力される動作角および駆動要求 MFR-3 への入力を監視している。監視結果に基づいて、調停要求 SR-33 がモータ駆動を調整する。本アーキテクチャを実現するための制約条件としては、NFSR-1、NFSR-2、NFSR-3 が規定されている。要求グループ間には独立要求があり、それらは制約条件として示されている。要求、制約条件、エレメントに割り当てられた重み付けは、それぞれに与えられた ASIL を表す。

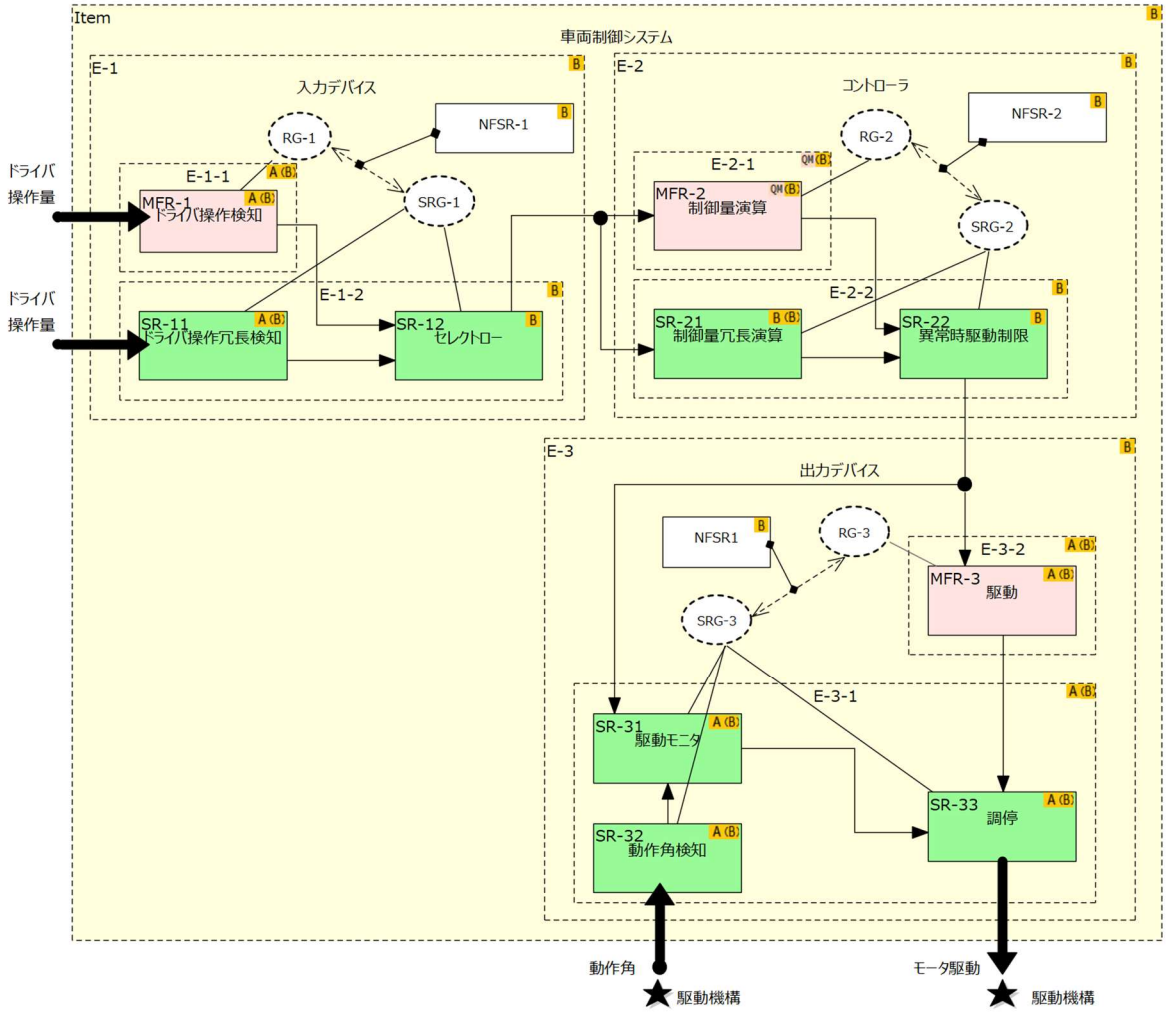

Figure 1 SCDL によるアーキテクチャ図

1.3.2 要求表

Table 1 意図機能要求

ID	名称	要求グループ	意図機能要求に由来する安全要求
MFR-1	ドライバ操作検知	RG-1	ドライバの操作量を検知する
MFR-2	制御量演算	RG-2	ドライバの操作量に従った制御量を演算する
MFR-3	駆動	RG-3	演算値に応じてモータを駆動する

Table 2 安全要求

ID	名称	要求グループ	安全要求
SR-11	ドライバ操作冗長検知	SRG-1	ドライバの操作量を検知する
SR-12	セレクトロー		2 つのドライバ操作量から操作量が低い方を選択する
SR-21	制御量冗長演算	SRG-2	ドライバの操作量に従った制御量を演算する
SR-22	異常時駆動制限		2 つの演算値の比較結果に応じて、制御量を制限する
SR-31	駆動モニタ	SRG-3	制御量と駆動量を比較する
SR-32	動作角検知		動作角より駆動量を検知する
SR-33	調停		比較結果に応じてモータ駆動を調整する

Table 3 制約条件

ID	独立要求
NFSR-1	RG-1 および SRG-1 が同時侵害となるような従属故障なきこと
NFSR-2	RG-2 および SRG-2 が同時侵害となるような従属故障なきこと
NFSR-3	RG-3 および SRG-3 が同時侵害となるような従属故障なきこと

1.3.3 エレメント表

Table 4 エレメント表

ID	名称
ITEM	車両制御システム
E-1	入力デバイス
E-1-1	ドライバ操作検知デバイス 1
E-1-2	ドライバ操作検知デバイス 2
E-2	コントローラ
E-2-1	制御量演算デバイス 1
E-2-2	制御量演算デバイス 2
E-3	出力デバイス
E-3-1	駆動モニタデバイス
E-3-2	駆動デバイス

1.4 上限値制限設計による安全アーキテクチャの例

1.4.1 アーキテクチャ図

車両に入力されたドライバ操作量を入力デバイス E-1 のドライバ操作検知要求 MFR-1 で検知する。制御量は、コントローラ E-2 の制御量演算要求 MFR-2 で算出される。そして、制御量は、制御量上域制限要求 SR-21 により上限値が制限される。その後、計算結果に基づき、出力デバイス E-3 の駆動要求 MFR-3 によりモータが駆動される。出力デバイス E-3 には、駆動モニタ要求 SR-31 があり、動作角を監視する動作角検知要求 SR-32 および駆動要求 MFR-3 への入力を監視している。その結果により、調停要求 SR-33 がモータ駆動を調整する。本アーキテクチャを達成するための要求としては、制約条件 NFSR-1、NFSR-2 が規定されている。要求グループ間には独立要求があり、それらは制約条件として示されている。要求、制約条件、エレメントに割り当てられた重み付けは、それぞれに与えられた ASIL を表す。

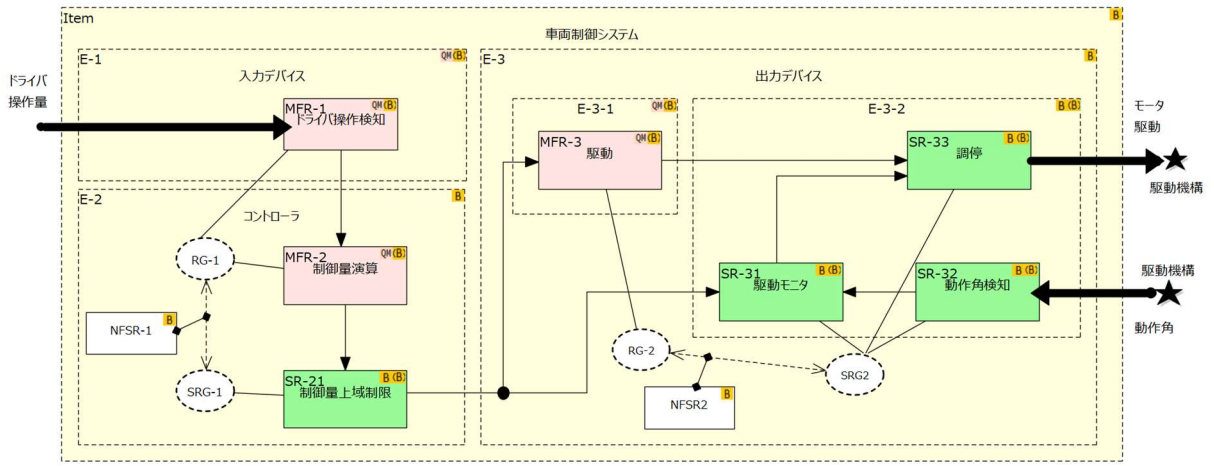

Figure 2 SCDL によるアーキテクチャ図

1.4.2 要求表

Table 5 意図機能要求

ID	名称	要求グループ	意図機能要求に由来する安全要求
MFR-1	ドライバ操作検知	RG-1	ドライバの操作量を検知する
MFR-2	制御量演算		ドライバの操作量に従った制御量を演算する
MFR-3	駆動	RG-2	演算値に応じてモータを駆動する

Table 6 安全要求

ID	名称	要求グループ	安全要求
SR-21	制御量上域制限	SRG-1	制御量を上限値で制限する
SR-31	駆動モニタ	SRG-2	制御量と駆動量を比較する
SR-32	動作角検知		動作角より駆動量を検知する
SR-33	調停		比較結果に応じてモータ駆動を調整する

Table 7 制約条件

ID	独立要求
NFSR-1	RG-1 および SRG-1 が同時侵害となるような従属故障なきこと
NFSR-2	RG-2 および SRG-2 が同時侵害となるような従属故障なきこと

1.4.3 エレメント

Table 8 エレメント表

ID	名称
ITEM	車両制御システム
E-1	入力デバイス
E-2	コントローラ
E-3	出力デバイス
E-3-1	駆動モニタデバイス
E-3-2	駆動デバイス

2 参考文献

ASAM SCDL Specification Version 1.6.0 ASAM e.V.,
ISO 26262：2018. Road Vehicles -- Functional Safety.

図一覧

表一覧

E-mail: support@asam.net
Web: www.asam.net