Association for Standardization of
Automation and Measuring Systems

ASAM SCDL

Safety Concept Description Language

Part 2 of 3

Practical Examples

Version 1.6.0

Date: 2021-11-09

Base Standard

Table of Contents

Foreword

SCDL is a single safety concept specification notation based on ISO 26262 context and semantics. ISO 26262 recommends semi-formal notation, and it is a solution. In addition, it has intuitive comprehension necessary for the specification, analysis, and review of safety concepts.
Practical examples are described in this document. An example contains the title which means designed architecture, architectural diagram, requirement table, and element table. Thus, notation of SCDL can be understood by this document.

1 Practical Examples

1.1 Overview

This document provides examples of architectural diagrams which are compliant with ASAM SCDL specifications. The specified system in the examples performs vehicle control based on the degree of driver operation. The safety goal assumed for this system is “Unintended excessive output shall not occur”. There are two examples provided for the safety architecture to demonstrate achievement of this safety goal. One is the safety architecture by redundancy design described in Figure 1. The other is the safety architecture by upper- limit design described in Figure 2.

1.2 Requirement tables and element tables to complement architecture diagrams

The architectural diagrams in Figure 1 and Figure 2 are complemented by requirement tables and element tables. The SCDL does not specify how to use these tables. However, it is expected that these tables facilitate a better understanding of the architectural diagrams.
Requirements/constraints/elements notated in the architectural diagram in Figure 1 are explained in Table 1 through 4, and those noted in Figure 2 are explained in Table 5 through 8.

1.3 Example of safety architecture by redundancy design

1.3.1 Architectural diagram

The degree of driver operation is detected redundantly by Driver operation detection requirement MFR-1 and by Driver operation redundant detection requirement SR-11 in the Input device E-1. Selection is then performed by Select low requirement SR-12, based on the detection result. Calculation of the control amount is also performed redundantly by Control amount calculation requirement MFR-2 and by Control amount redundant calculation requirement SR-21 in the Controller E-2. Drive limit at fault requirement SR-22 then determines if the result of the control amount calculation is faulty or not, and the control amount is adjusted as needed. Motor is driven according to the control amount by Drive requirement MFR-3 in the Output device E-3. The Output device E-3 also has Drive monitor requirement SR-31 which monitors input to Operating angle detection requirement SR-32 which monitors actuation amount, and input to Drive requirement MFR-3. Based on the monitoring result Arbitration requirement SR-33 adjusts motor drive. Constraints NFSR-1, NFSR-2, and NFSR-3 are specified as requirements to realize this architecture. There are independence requirements between requirement groups, which are indicated as constraints. Weighting assigned to each requirement, constraint, and element represents its ASIL.

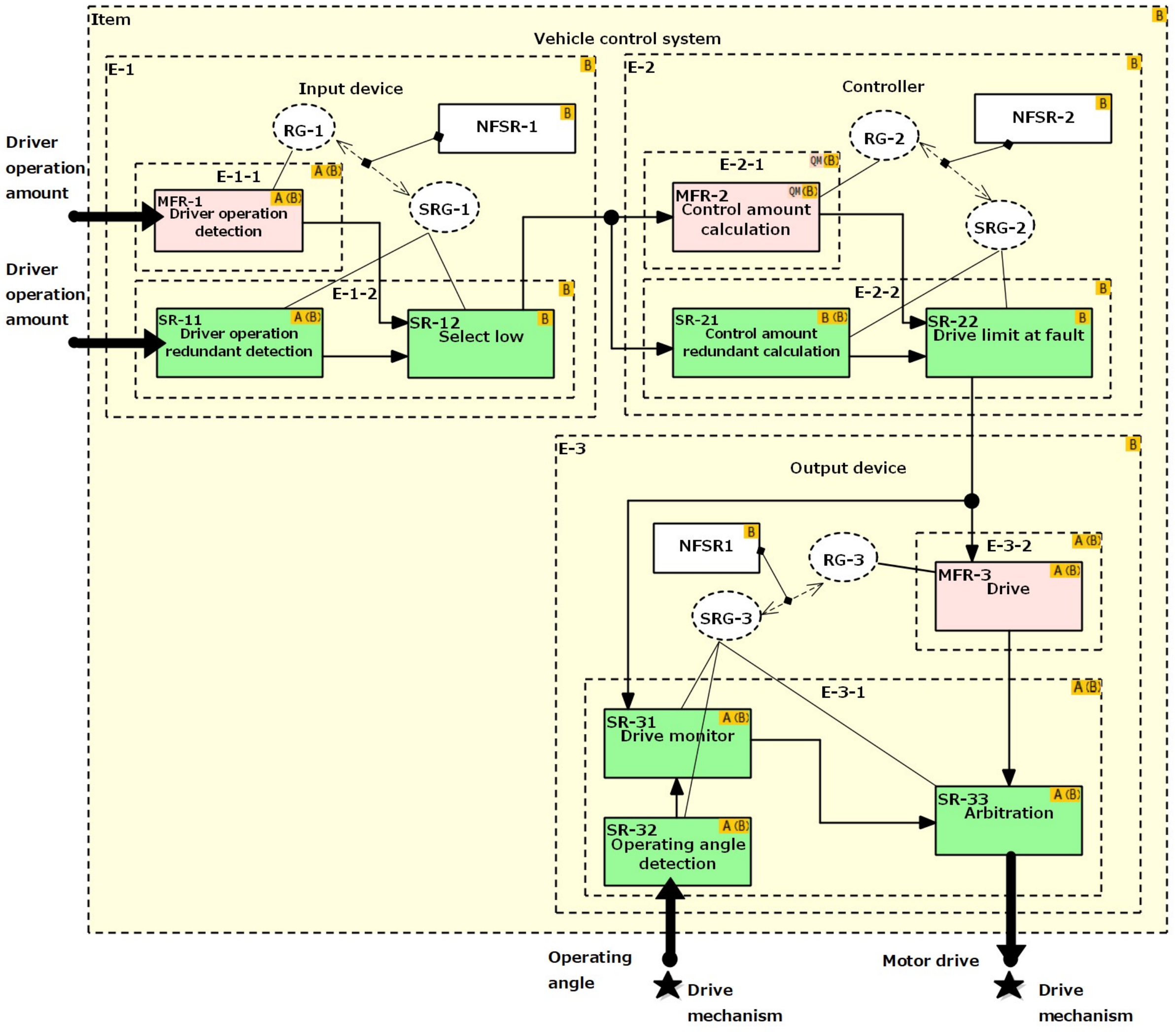

Figure 1 Architectural diagram using SCDL

1.3.2 Requirement table

Table 1 Intended functional requirements

ID	Name	Requirement Group	Safety requirements derived from intended functional requirements
MFR-1	Driver operation detection	RG-1	Detect the degree of driver operation
MFR-2	Control amount calculation	RG-2	Calculate control amount according to the degree of driver operation
MFR-3	Drive	RG-3	Drive motor according to the control amount

Table 2 Safety requirements

ID	Name	Requirement Group	Safety requirement
SR-11	Driver operation redundant detection	SRG-1	Detect the degree of driver operation
SR-12	Select low		Select the lower of the two different degree of driver operations
SR-21	Control amount redundant calculation	SRG-2	Calculate control amount according to the degree of driver operation
SR-22	Drive limit at fault		Limit the control amount according to the result of comparison of two control amounts
SR-31	Drive monitor	SRG-3	Compare the control amount and the actuation amount
SR-32	Operating angle detection		Calculate the actuation amount of the operating angle
SR-33	Arbitration		Adjust motor drive according to the result of comparison

Table 3 Constraints

ID	Independence requirement
NFSR-1	Dependent failure which may simultaneously violate both RG-1 and SRG-1 shall not occur
NFSR-2	Dependent failure which may simultaneously violate both of RG-2 and SRG-2 shall not occur
NFSR-3	Dependent failure which may simultaneously violate both of RG-3 and SRG-3 shall not occur

1.3.3 Element table

Table 4 Element table

ID	Name
ITEM	Vehicle control system
E-1	Input device
E-1-1	Driver operation detection device 1
E-1-2	Driver operation detection device 2
E-2	Controller
E-2-1	Control amount calculation device 1
E-2-2	Control amount calculation device 2
E-3	Output device
E-3-1	Drive monitor device
E-3-2	Drive device

1.4 Example of safety architecture by upper-limit design

1.4.1 Architectural diagram

The degree of driver operation that was input to the vehicle is detected by Driver operation detection requirement MFR-1 in the Input device E-1. Control amount is calculated by Control amount calculation requirement MFR-2 in the Controller E-2. The control amount is then limited by the upper-limit value by Control amount limit by upper-value SR-21. Based on the calculation result, the motor is driven by Drive requirement MFR-3 in the Output device E-3. The output device E-3 also has Drive monitor requirement SR-31 to monitor input to Operating angle detection requirement SR-32 which monitors actuation amount, and input to drive requirement MFR-3. Based on the monitoring result, Arbitration requirement SR-33 adjusts motor drive. Constraints NFSR-1 and NFSR-2 are specified as requirements to realize this architecture. There are independence requirements between requirement groups, which are indicated as constraints. Weighting for each requirement, constraint, and element represents its ASIL.

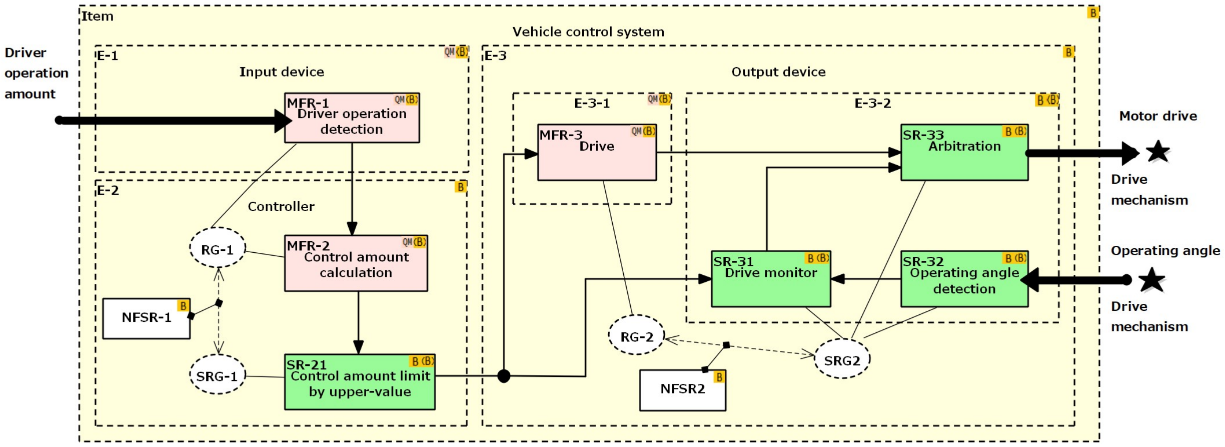

Figure 2 Architectural diagram using SCDL

1.4.2 Requirement table

Table 5 Intended functional requirements

ID	Name	Requirement Group	Safety requirements derived from intended functional requirements
MFR-1	Driver operation detection	RG-1	Detect the degree of driver operation
MFR-2	Control amount calculation		Calculate control amount according to the degree of driver operation
MFR-3	Drive	RG-2	Drive motor according to the control amount

Table 6 Safety requirements

ID	Name	Requirement Group	Safety requirements
SR-21	Control amount limit by upper-value	SRG-1	Limit control amount by the upper-limit value
SR-31	Drive monitor	SRG-2	Compare the control amount and the actuation amount
SR-32	Operation angle detection		Calculate the actuation amount of the operating angle
SR-33	Arbitration		Adjust motor drive according to the comparison result

Table 7 Constraints

ID	Independence requirement
NFSR-1	Dependent failure which may simultaneously violate both RG-1 and SRG-1 shall not occur
NFSR-2	Dependent failure which may simultaneously violate both RG-2 and SRG-2 shall not occur

1.4.3 Element table

Table 8 Element table

ID	Name
ITEM	Vehicle control system
E-1	Input device
E-2	Controller
E-3	Output device
E-3-1	Drive monitor device
E-3-2	Drive device

2 Bibliography

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

Figure Directory

Table Directory

ASAM

Association for Standardization of
Automation and Measuring Systems

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