Consideration of the Effectiveness of

D-Case and SysML Collaboration

Table of Contents

Revision History

Revised Date	Description
2014/01/27	Created

1 Scope

This document describes the consideration of the effectiveness of D-Case and SysML collaboration.

2 Related Work

As part of existing work into Collaboration between assurance case, safety case, or D-Case and system development environment like UML or SysML, some trials are carried out. This section summarizes similarities, differences, and appeal points of this method against 5 references.

2.1 Comparison to Reference [1]

Reference [1]:

- Stefen Wagner et al, A Case Study on Safety Cases in the Automotive Domain: Modules, Patterns, and Models, In Proc. of ISSRE2010

Similarities:

- Propose goal structure of safety case

Differences:

- Propose Notation guide for D-Case node and template to collaborate D-Case and SysML model description
- Improve efficiency of D-Case and SysML model development by controlling development flow

Appeal point of Reference:

- Apply safety case to functional safety in the automotive system
- Apply ASCET SD and Matlab/Simulink models to safety case

2.2 Comparison to Reference [2]

Reference [2]:

- John Birch, Roger Rivett, Ibrahim Habli, Ben Bradshaw, John Botham, Dave Higham, Peter Jesty, Helen Monkhouse, Robert Palin: Safety Cases and their Role in ISO 26262 Functional Safety Assessment. In the proceedings of the 32nd International Conference on Computer Safety, Reliability and Security (SAFECOMP), Toulouse, France, September 2013.

Similarities:

- Propose goal structure of safety case

Differences:

- Propose Notation guide for D-Case node and template to collaborate D-Case and SysML model description
- Improve efficiency of D-Case and SysML model development by controlling development flow

Appeal point of Reference:

- Apply safety case to functional safety in the automotive system
- Apply works products in system development to safety case

2.3 Comparison to Reference [3]

Reference [3]:

- Ewen Denney, Ganesh Pai, Ibrahim Habli: Perspectives on software safety case development for unmanned aircraft. DSN 2012: 1-8

Similarities:

- Propose goal structure of safety case

Differences:

- Propose Notation guide for D-Case node and template to collaborate D-Case and SysML model description
- Improve efficiency of D-Case and SysML model development by controlling development flow

Appeal point of Reference:

- Apply safety case to safety assurance in an unmanned aircraft system
- Apply works products in system development to safety case

2.4 Comparison to Reference [4]

Reference [4]:

- (In Japanese) 名古屋大学山本研究室、産総研 D-Case と SysML/UML 連携の実証実験

  (In English) Nagoya Univ., IPA: Experiment of collaboration between D-Case and

SysML/UML

- http://www.dcase.jp/pdf/yamamoto20130419.pdf

Similarities:

- Propose goal structure of assurance case

Differences:

- Propose Notation guide for D-Case node and template to collaborate D-Case and SysML model description
- Improve efficiency of D-Case and SysML model development by controlling development flow

Appeal point of Reference:

- Apply assurance case to UML/SysML development environment
- Collaborating between D-Case and UML or SysML, effectiveness on understanding of D-Case, and control Modeling work products on D-Case

2.5 Comparison to Reference [5]

Referece[5]:

- Patrick J. Graydon, John Knight, Elisabeth A. Strunk, Assurance Based Development of Critical Systems, In Proc. IEEE DSN 2007

Similarities:

- Propose goal structure of assurance case

Differences:

- Propose Notation guide for D-Case node and template to collaborate D-Case and SysML model description
- Improve efficiency of D-Case and SysML model development by controlling development flow

Appeal point of Reference:

- Propose goal structure of assurance case

3 Evaluation Plan

3.1 Target

3.1.1 Background

Previous model of the cruise control (CC) system was developed half a year ago. Derivational development is applied to new CC model of cruise control system based on specifications of previous CC model. New CC model has differences to adding functions of ISO26262 functional safety. The development target of this evaluation is set on new CC model of cruise control system.

3.1.2 Work Products

Work products below are prepared by the development of new model.

- D-Case
- Use case diagram
- Requirement diagram
- Block definition diagram
- Parametric diagram
- Internal block diagram
- State machine diagram
- Verification scenario

3.1.3 Evaluation Term

Development term is structured by items in Table 1. Evaluation is conducted in point of man-hour for each item.

Table 1 Evaluation Term

ID	Term	Description
1	Item Definition	Define item using D-Case and SysML models for previous model.
2	Identification of Hazard	Hazard analysis using HAZOP, FTA, FMEA.
3	Decomposition Based on Functional Safety Requirements	Decompose D-Case goal based on functional safety requirements.
4	Update Use case and Requirement Diagram	Update use case and requirement diagram.
5	Decomposition Based on	Decompose D-Case goal based on technical safety

	Technical Safety Requirements	requirements.
6	Update Block Definition and Parametric Diagram	Update block definition, parametric, internal block, and state machine diagram. Associate model elements to D-Case.
7	Guaranty by Verification Results	Associate verification scenario to D-Case.
8	Model Simulation	Execute verification scenario.

3.1.4 Evaluator

A development engineer is the same person who developed previous model. Other one person is a reviewer.

3.2 Evaluation Item

Compare man-hour to develop D-Case and SysML models for new CC model.[1]

Case 1: No modeling guide and no template are applied

Case 2: All modeling guides and templates are applied

- D-Case Modeling Guide for Target System
- SysML Modeling Guide for Target System
- D-Case Template
- SysML Template

[1] Note that the target for comparison here is not “with D-Case versus without D-Case”, but “with modeling guides and templates versus without them” in this evaluation.

4 Evaluation Result

4.1 Work Products

Work Products on new CC Model development are listed up in Table 2, Table 3, and Table 4.

Table 2 Work Products

Model	No. of pcs
D-Case	1
Use case diagram	1
Requirement diagram	1
Block definition diagram	2
Parametric diagram	2
Internal block diagram	1
State machine diagram	13
Verification scenario	1

Table 3 D-Case Node

Node	No. of pcs
Goal	24
Strategy	10
Context	74
Evidence	14
SolvedBy	47
InContextOf	74

Table 4 Elements of SysML Model

Model	Elements	No. of pcs
Use case diagram	Actor	3
	Use case	11
	Association	21
	Subject	1
	Association to D-Case	8
Requirement diagram	Functional Requirement	13
	Non-functional Requirement	8

	Association	34
	Association to D-Case	12
Block definition diagram (design)	Block	16
	Association	34
	Association to D-Case	12
Parametric diagram	Block	12
	Connector	25
	Association to D-Case	4
Internal block diagram	Block	3
	Connector	4
Block definition diagram (Implementation)	Block	16
	Association	32
State machine diagram	State	100
	Transition	113
Verification scenario	Scenario	1
	Verification	1
	Association to D-Case	12

4.2 Sample of Work Products

This section describes samples of work products developed in new CC model.

4.2.1 D-Case

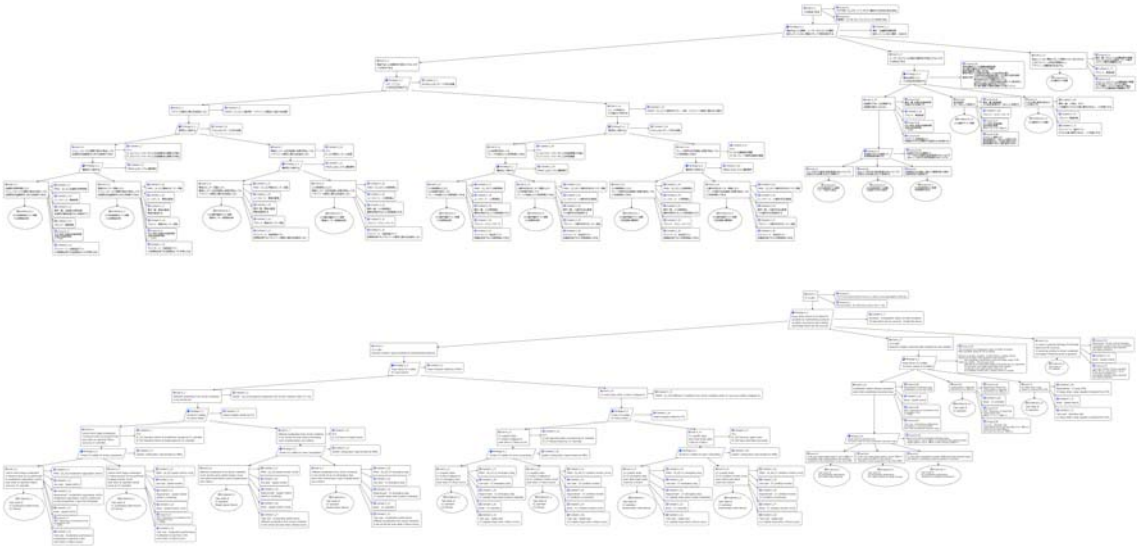
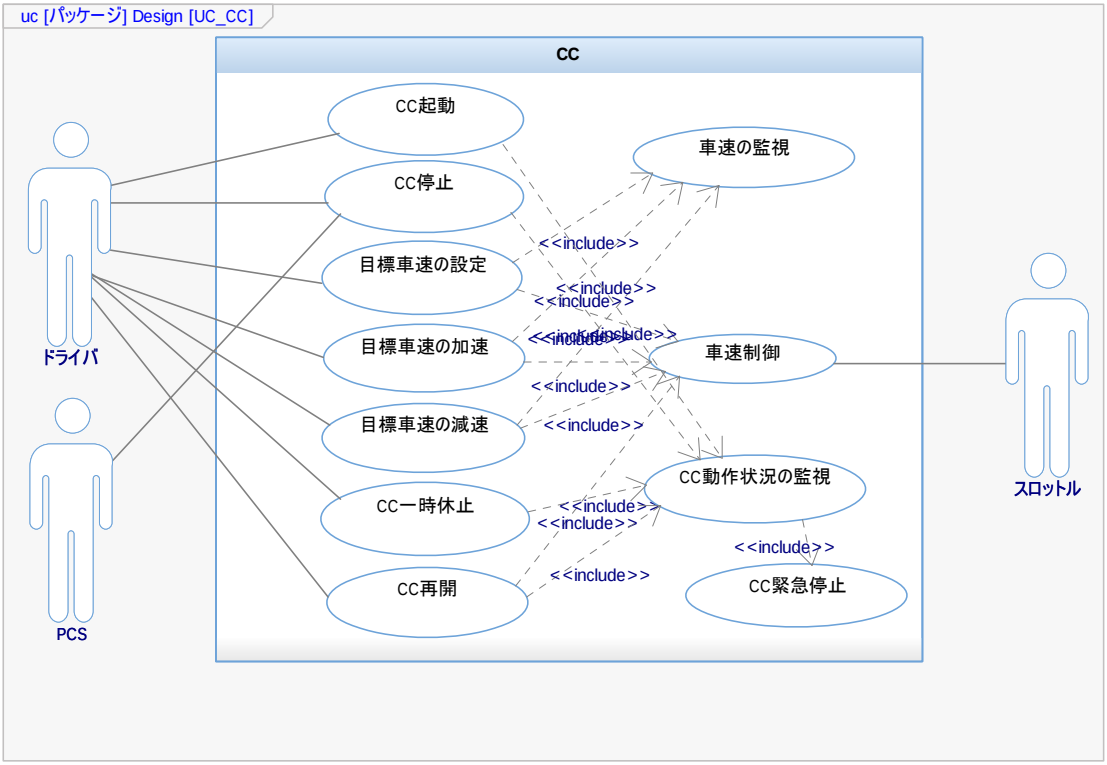


Figure 4-1 D-Case (Original D-Case is in Japanese)

4.2.2 Use case diagram



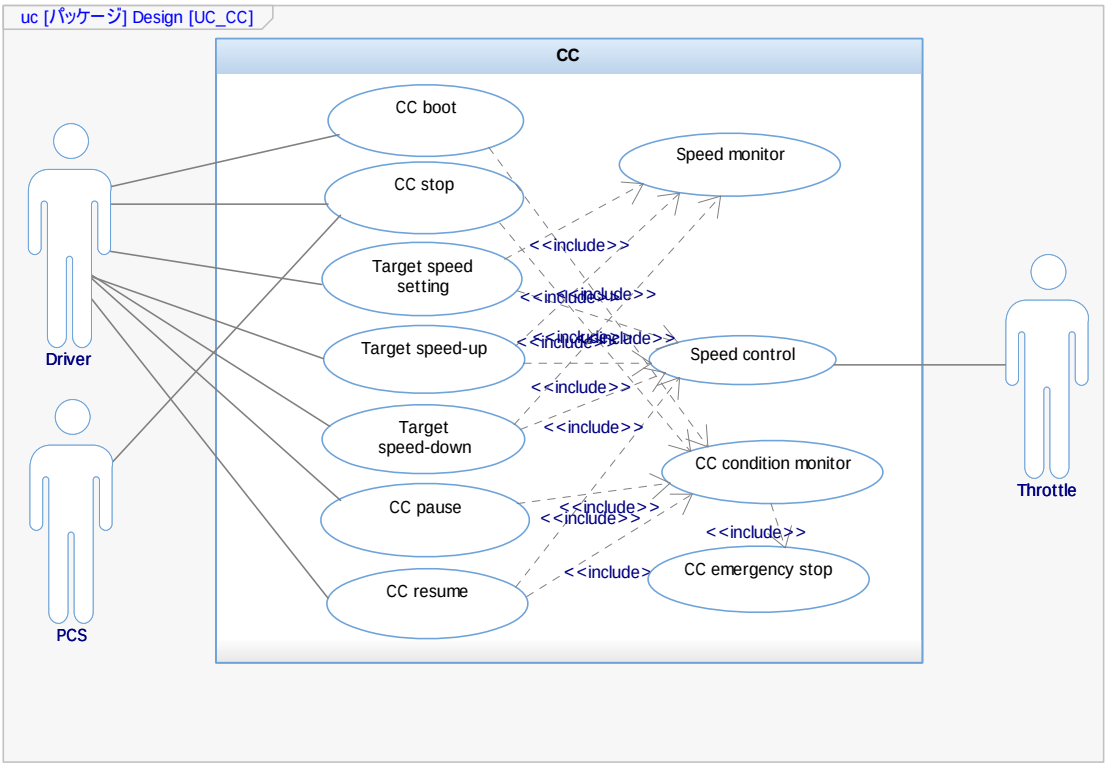


Figure 4-2 Use case diagram (Original diagram is in Japanese)

4.2.3 Requirement diagram

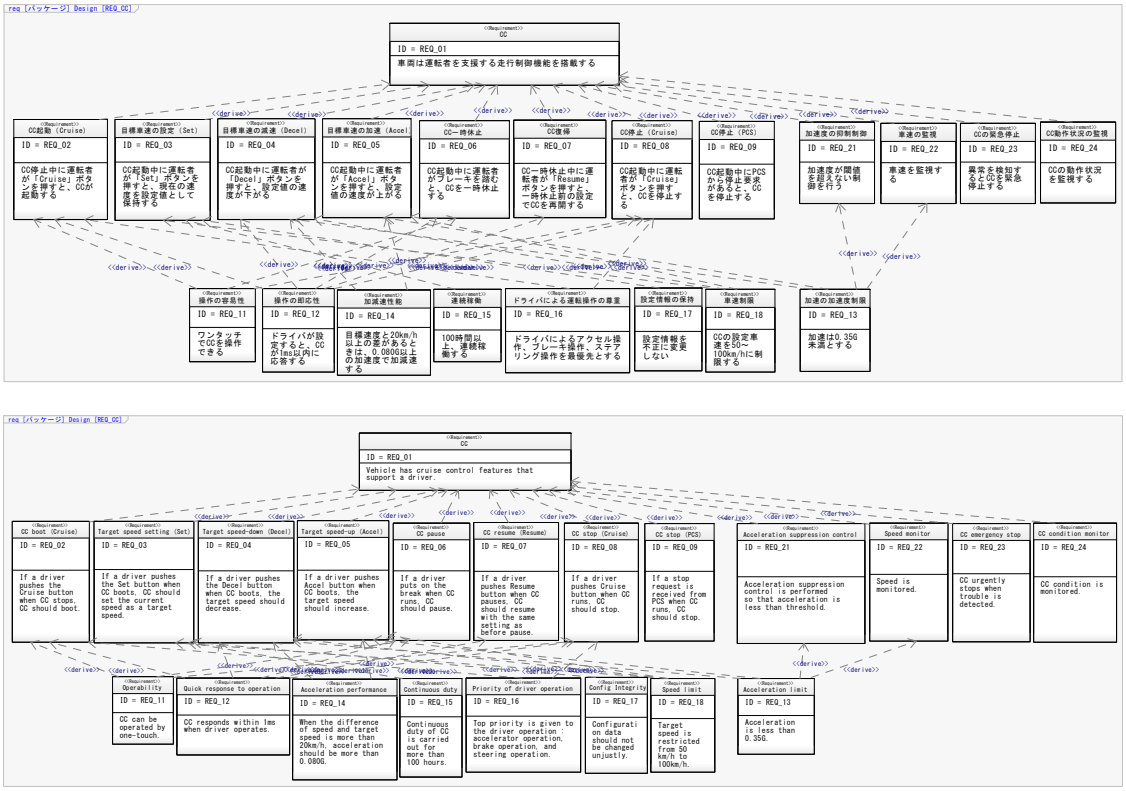


Figure 4-3 Requirement diagram (Original diagram is in Japanese)

4.2.4 Block definition diagram (design)

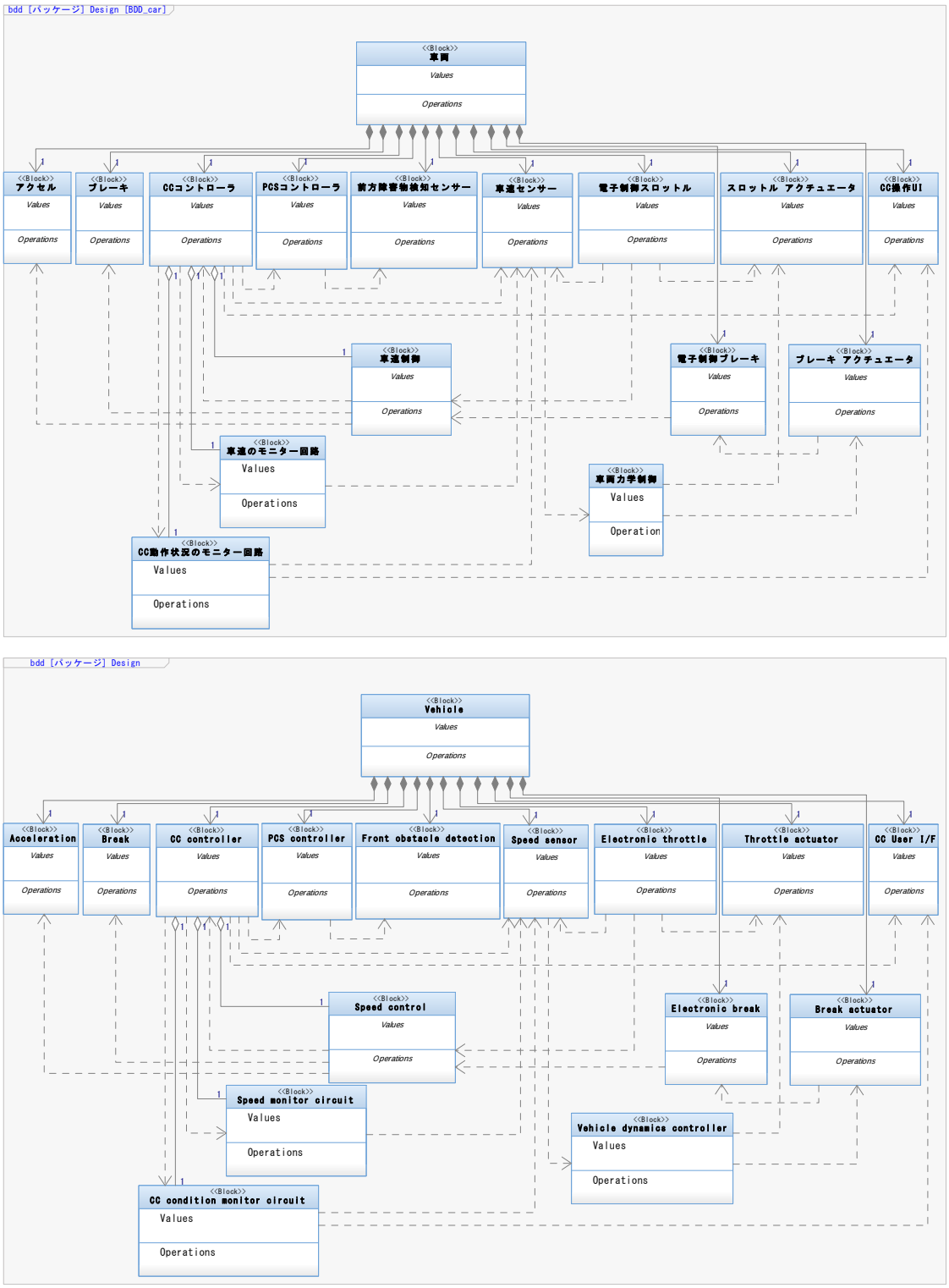


Figure 4-4 Block definition diagram (Original diagram is in Japanese)

4.2.5 Parametric diagram

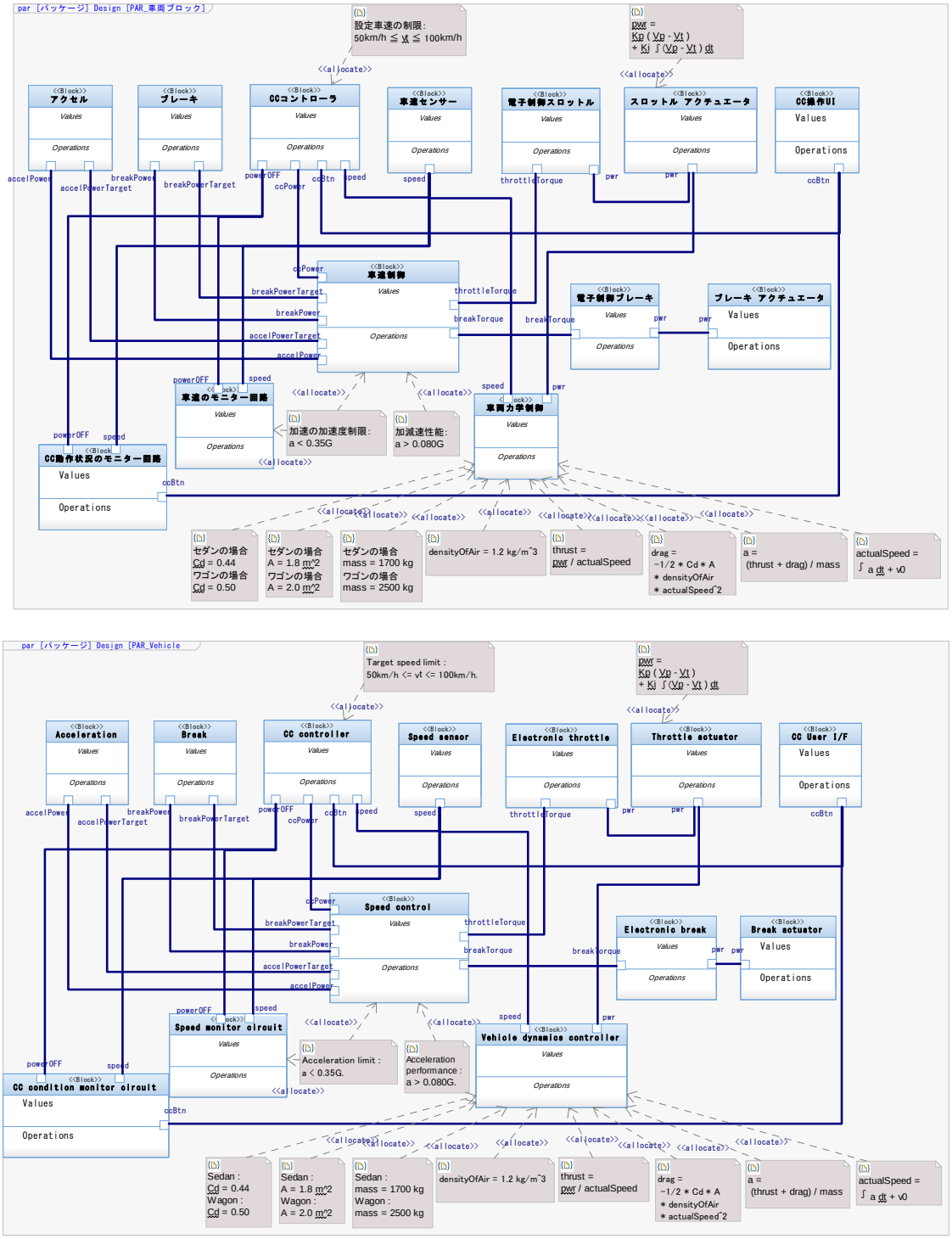
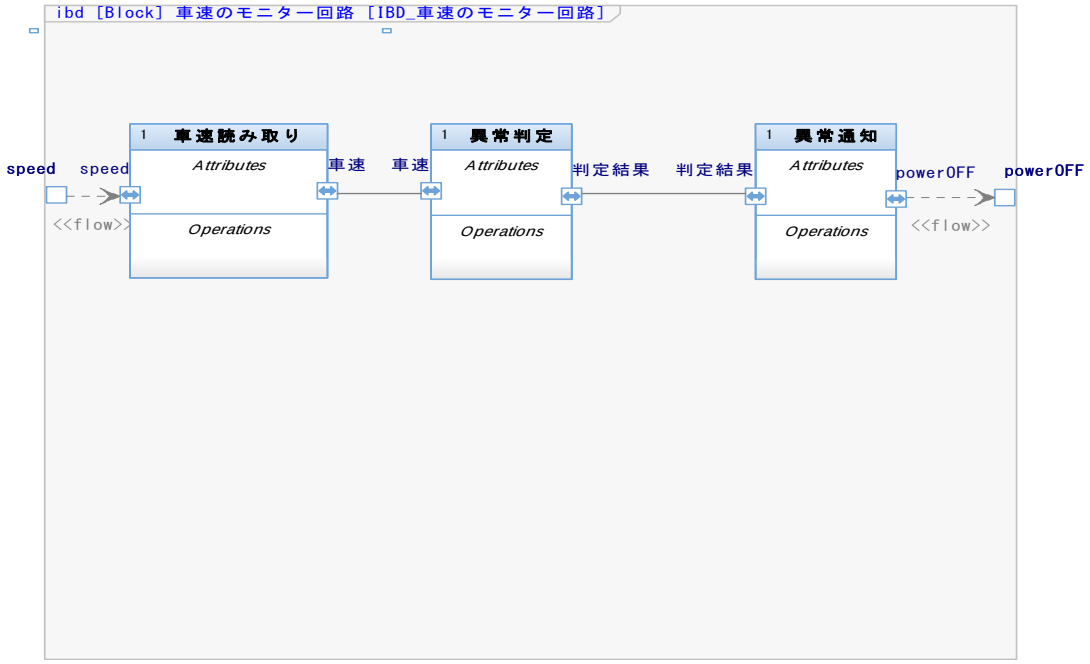


Figure 4-5 Parametric diagram (Original diagram is in Japanese)

4.2.6 Internal block diagram



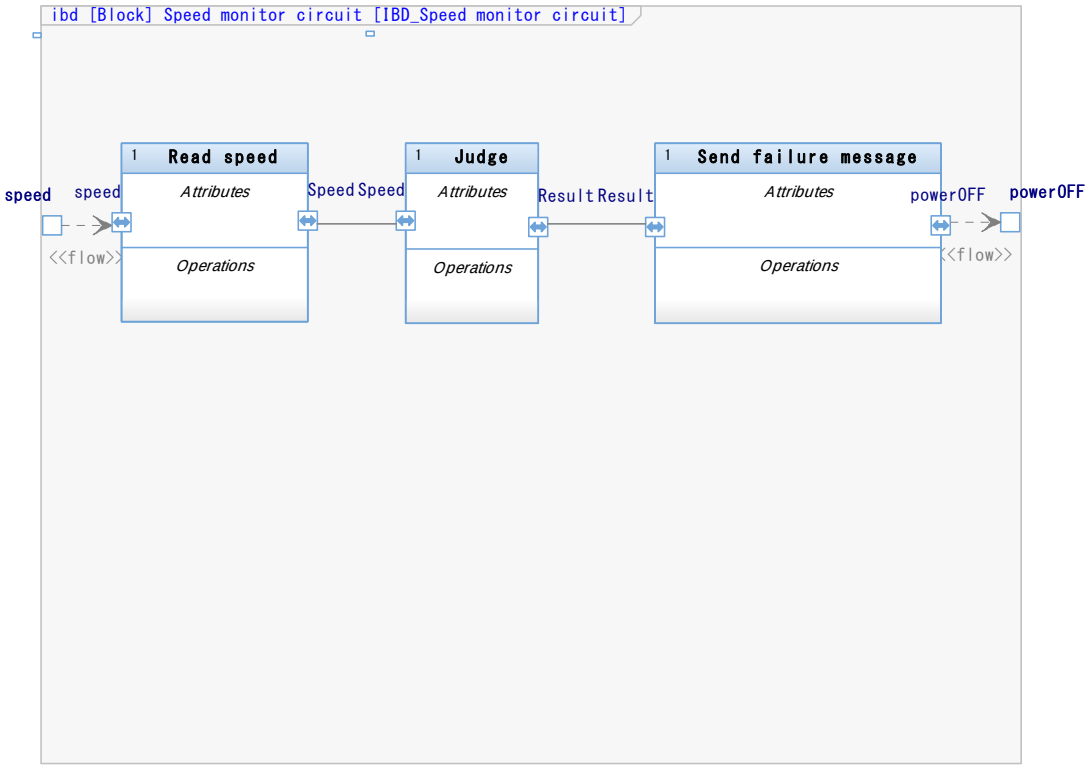


Figure 4-6 Internal block diagram (Original diagram is in Japanese)

4.2.7 Block definition diagram (Implementation)

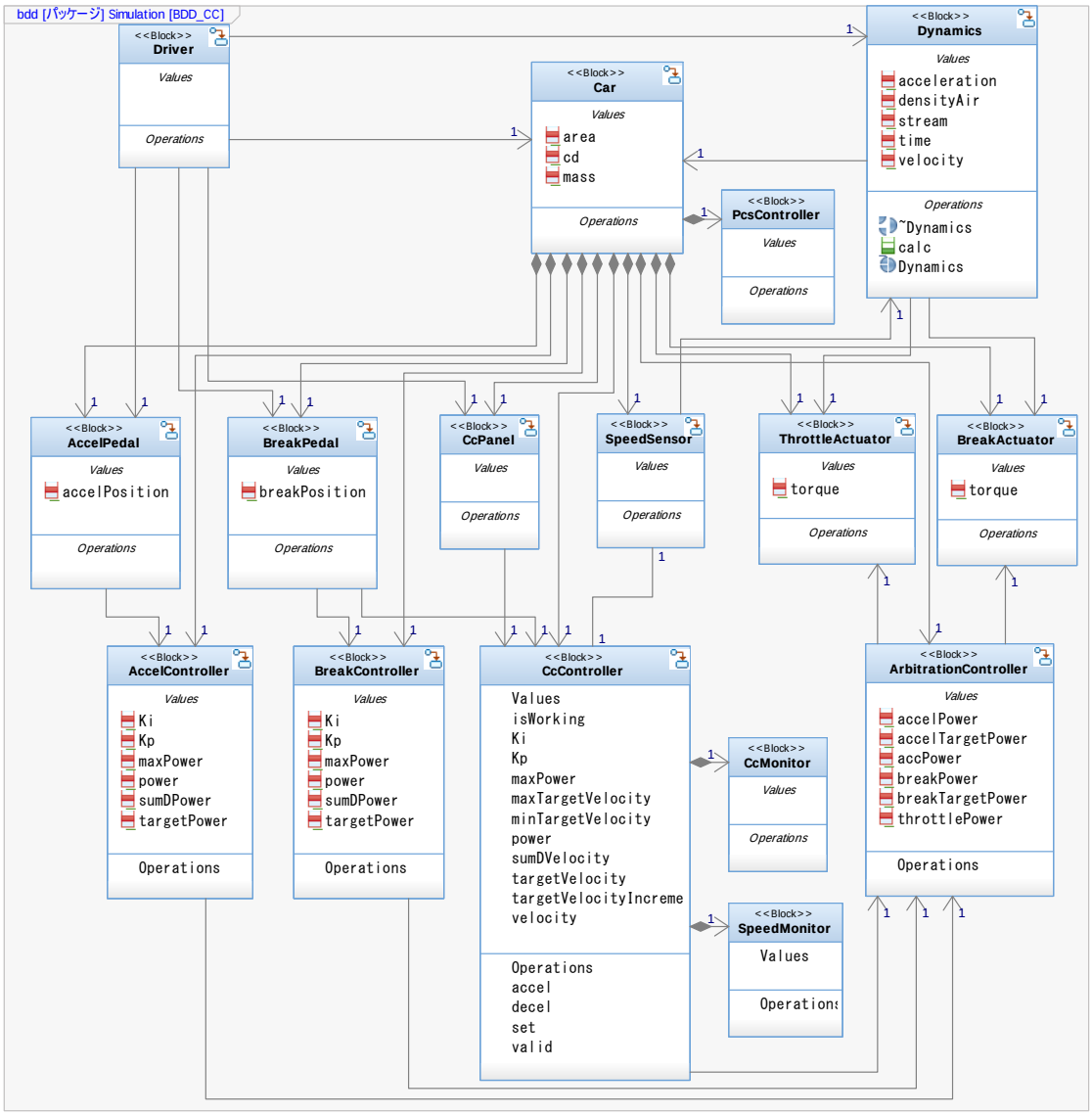


Figure 4-7 Block definition diagram (Implementation)

4.2.8 State machine diagram

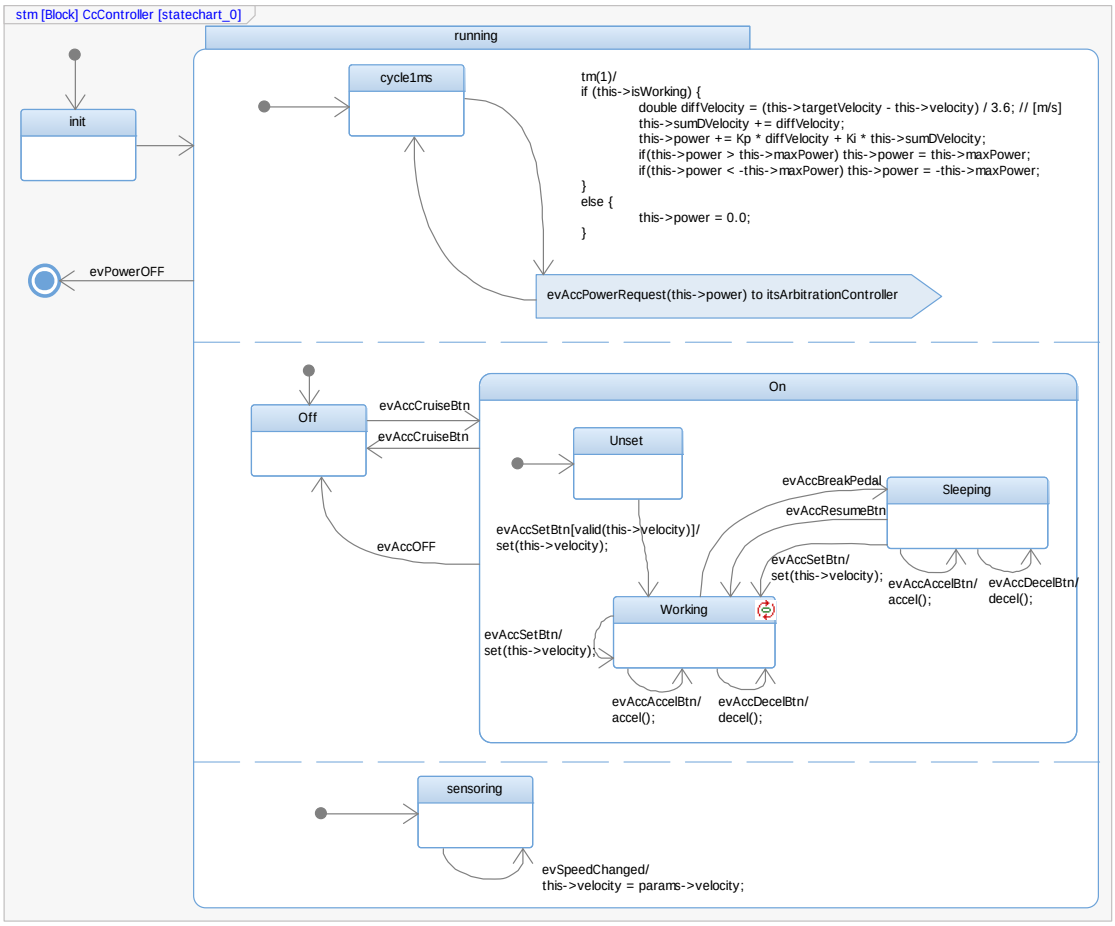


Figure 4-8 State machine diagram

4.2.9 Verification scenario

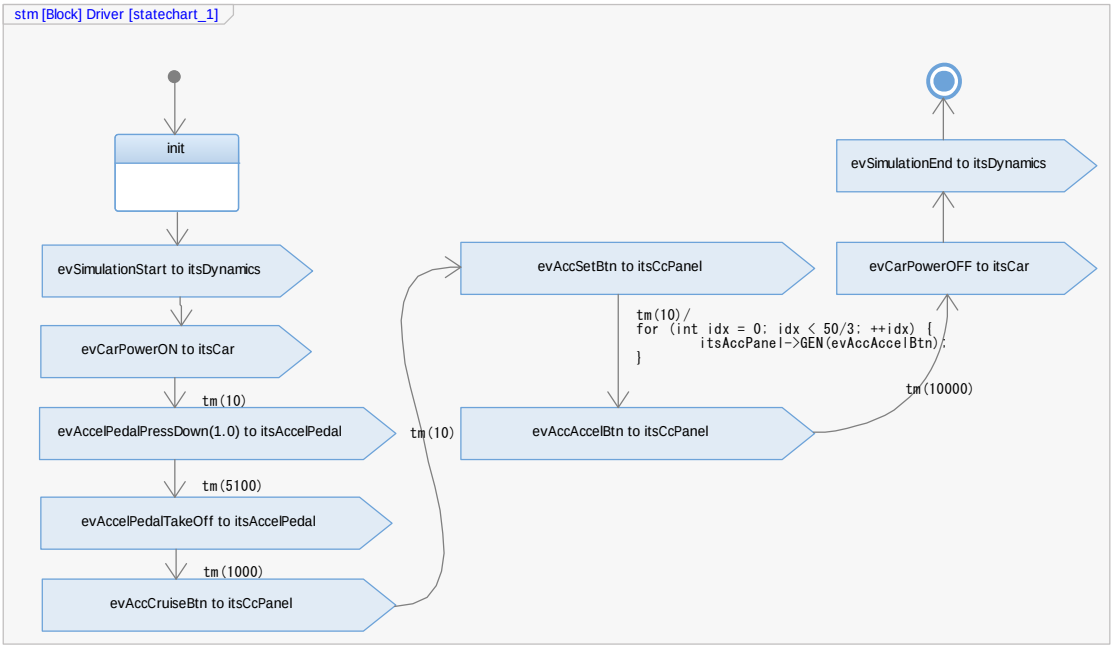


Figure 4-9 Verification scenario

4.3 Result

Table 5 and Table 6 show measurement results of man-hour to develop.

Case 1: No modeling guide and no template are applied

Case 2: All modeling guides and templates are applied

Table 5 Case 1: No modeling guide and no template are applied

ID	Term	man –hour (h)	Review (No. of times)
1	Item Definition	4.5	2
2	Identification of Hazard	30	6
3	Decomposition Based on Functional Safety Requirements	20	3
4	Update Use case and Requirements Diagram	11.5	5
5	Decomposition Based on Technical Safety Requirements	3	2
6	Update Block Definition and Parametric Diagram	12	3
7	Guaranty by Verification Results	1	1
8	Model Simulation	1	1

	Total	83	23

Table 6 Case 2: All modeling guides and templates are applied

ID	Term	man –hour (h)	Review (No. of times)
1	Item Definition	4.5	2
2	Identification of Hazard	30	6
3	Decomposition Based on Functional Safety Requirements	6	3
4	Update Use case and Requirements Diagram	6.5	2
5	Decomposition Based on Technical Safety Requirements	1	1
6	Update Block Definition and Parametric Diagram	7.5	2
7	Guaranty by Verification Results	1	1
8	Model Simulation	1	1
	Total	57.5	18

4.4 Comparison

Figure 4-10 shows the comparison of man-hour in case 1 and in case 2.

Figure 4-11 shows the comparison of number of review in case 1 and in case 2.

Case 1: No modeling guide and no template are applied

Case 2: All modeling guides and templates are applied

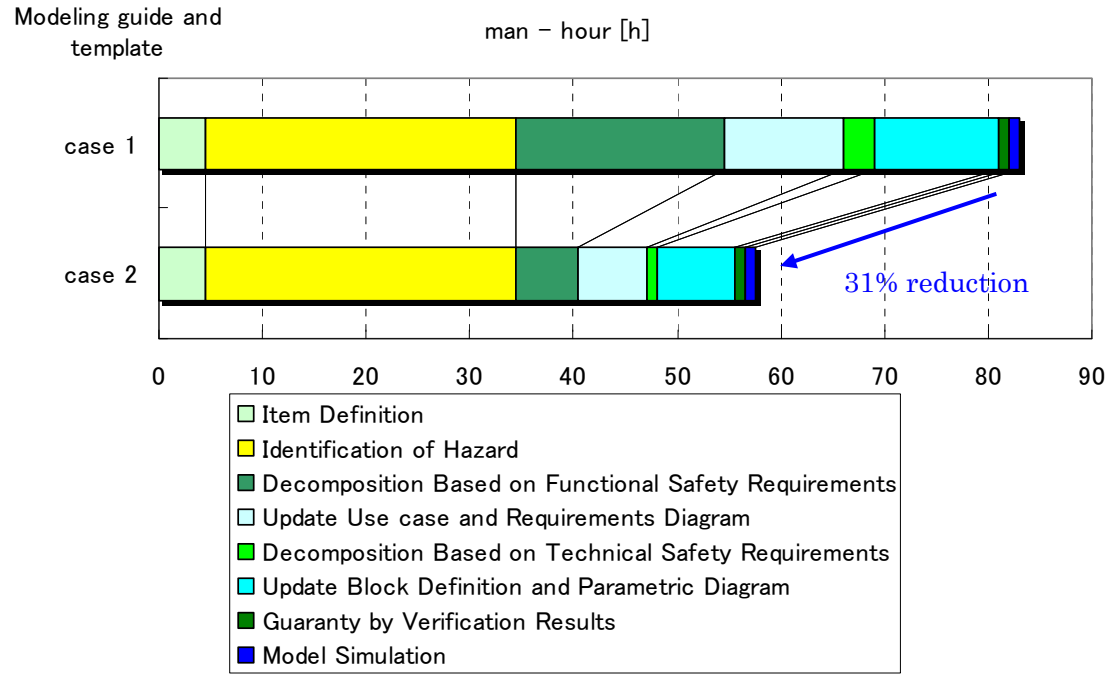


Figure 4-10 Man-hour

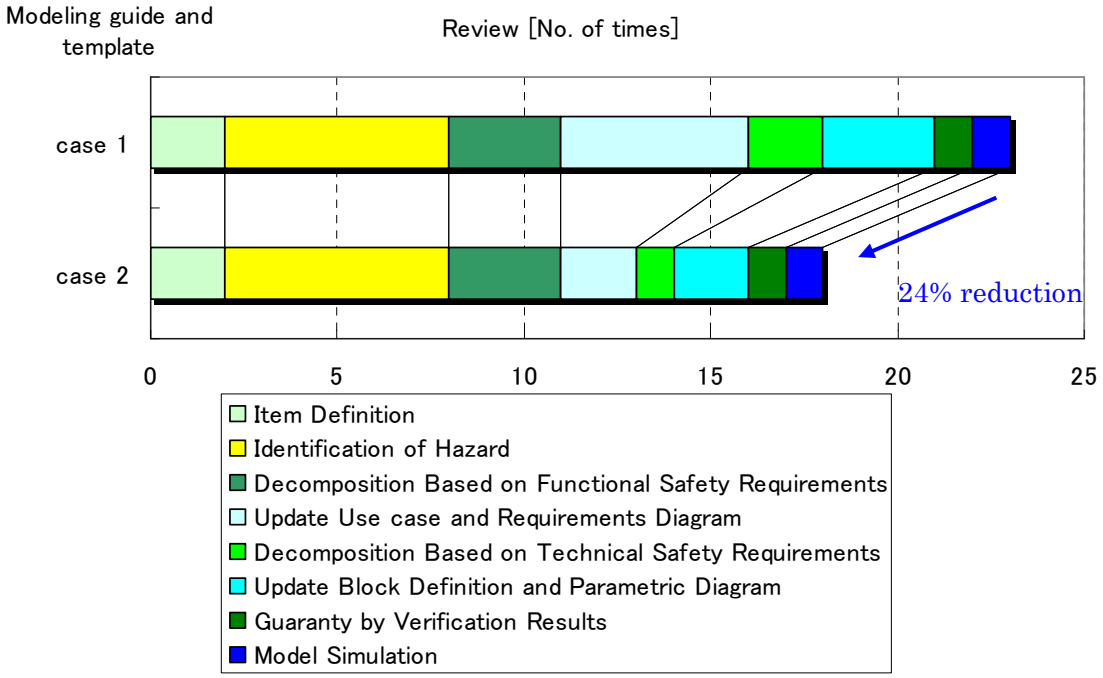


Figure 4-11 Number of reviews

According to Figure 4-10 and Figure 4-11, applying modeling guides and templates reduce 31% of man-hour and 24% of number of reviews.
For decomposition based on functional safety requirements, update use case and requirements diagram, decomposition based on technical safety requirements, and update block definition and parametric diagram, Applying template is effective.
Item definition and identification of hazards are not depends on templates.

5 Consideration

As the description in the previous chapter, Applying modeling guides and templates reduce 31% of man-hour and 24% of number of review.
factors of these effectiveness are below.

- D-Case template prepares goal structure, and it reduced the number of rewriting strategy and goal node in D-Case.
- Association with D-Case and SysML requirement diagram about functional safety requirements reduced man-hour to requirements definition.
- Association with D-Case and SysML block definition diagram reduced man-hour to architecture design.
- Association with D-Case and SysML parametric diagram about restriction reduced man-hour to extract restriction.

These results show that modeling guides and templates are effective on the system development.