Challenges of Assurance Case Description Method in Japan

Nobuyuki KOBAYASHIa *, Kohei TANAKAb, Nasa YOSHIOKAc, Aki NAKAMOTOd, Seiko SHIRASAKAc

“Development Administration Department, KATO WORKS CO., LTD. 1-9-37 Higashioi, Shinagawa-ku, Tokyo 140-0011 Japan
bSOKENDAI(The Graduate University for Advanced Studies), School of Physical Sciences, 3-1-1 Yoshinodai, Chuo-ku, Sagamihara-shi, Kanagawa 252-5210 Japan
cGraduate School of System Design and Management, Keio University, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8526, Japan
dThe System Design and Management Research Institute of Graduate School of System Design and Management, Keio University, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8526 Japan

Abstract

Assurance cases standardized by ISO have come to draw a lot of attention. With the aim of identifying challenges of assurance case description method in Japanese organizations, this study evaluates assurance cases created by beginners. The objectives of this study are three folds. First, we aim to show, based on the test and questionnaire survey, the challenges which have not been identified in previous studies regarding assurance case description. Though teaching the description method of assurance cases is necessary, each organization in the industries conforming to international standards find it difficult to educate the employees on how to describe appropriate assurance cases. Second, we aim to confirm for which of visualizing strengths and visualizing weaknesses of the contents described in assurance cases work better. With this in mind, assurance case instructors could suggest the participants which of strengths and weaknesses they are likely to visualize in creating assurance cases. It will also help beginners create assurance cases. Third, this study aims to demonstrate the number of trainees who made mistakes in the test after the training with a view to disclosing the proportion of trainees who created assurance cases correctly after the training. This study concludes with presenting challenges of assurance case description method in Japanese organizations.

Key words: Assurance Case, Goal Structuring Notation, Dependability-Case

1. Introduction

Assurance cases standardized by international standards of ISO 26262 [1], ISO 15026 [2] and others have come to draw a lot of attention. The assurance case can be applied to manage documents and processes regarding Systems Engineering. Kobayashi et al. discusses that assurance case is useful in the fields including management. [3] [4]

Yamamoto et al. however states that there are challenges in creating assurance cases correctly [5]. This study therefore evaluates assurance cases created by beginners, with the aim of identifying challenges of assurance case description method.

The objectives of this study are three folds. First, we aim to show, based on the test and questionnaire survey, the challenges which have not been identified in previous studies regarding assurance case description.

Yamamoto et al. pointed out the following “four common mistakes beginners make.” [5]:

(1) Write in a wrong node of “Strategy” instead of “Goal”
(2) Goal is not mentioned as a proposition but as an execution statement or a function statement.
(3) Strategy is misunderstood as a judgment branching.
(4) Decompose by not discussion but the order of function.

Though teaching the description method of assurance cases is necessary, each organization in the industries conforming to international standards find it difficult to educate the employees on how to describe appropriate assurance cases.

This study thus aims to identify other challenges of assurance case description method in Japanese organizations than the four common mistakes mentioned above.

Second, we aim to confirm for which of visualizing strengths and visualizing weaknesses of the contents described in assurance cases work better. With this in mind, assurance case instructors could suggest the participants which of strengths and weaknesses they are
likely to visualize in creating assurance cases. It will also help beginners create assurance cases.

Third, this study aims to demonstrate the number of trainees who made mistakes in the test after the training with a view to disclosing the proportion of trainees who created assurance cases correctly after the training. Though having revealed issues in assurance case description, previous studies including Yamamoto et al. [5] have not shown how many of the trainees were able to create appropriate assurance cases after the training, which is therefore presented in this study.

2. Previous Studies

2.1 Assurance Case

Safety cases were proposed by Kelly et al. [6] in 1998 as a means of conducting a clear, complete and reasonable discussion. Using safety cases helps the stakeholders confirm that the developed system can operate at an acceptable level in terms of safety. Assurance cases [7] extend the discussion to the whole quality of the system discussed, including “safety”, which is focused in safety cases. In this study, we mainly used for training the Goal Structuring Notation (GSN) [8] proposed by Tim et al, as well as extended GSN, namely the Dependability-Case (D-Case) [9], and the GSN also for evaluating the description method.

2.2 Nodes of Dependability Case

In this study, we used mainly five nodes. The basic description rules are as follows. “Goal” describes what to assure, with a combination of a subject and predicate. “Context” describes the state, environment and conditions of the system, and shows ways to lead to the Goal and Strategy. “Strategy” describes how to divide the Goal into sub-goals leading to the lower layer. “Evidence” eventually assures that we can reach the Goal, and shows ways to lead to the Goal. “Undeveloped” shows the status that there is no Evidence or discussion supporting the Goal.

3. Experiment Design

This section describes the experiment design of this study, as shown in Figure 1.

90 minute-lecture

A 90 minute-lecture on assurance cases was given at Graduate School of System Design and Management, Keio University. The lecture covered the history of assurance cases and the description method. We used GSN description for assurance case description. [9] In addition, we showed “four common mistakes beginners make” and how to avoid the mistakes as follows:

1. Write in a wrong node of “Strategy” instead of “Goal”.
   We checked the participants with a quiz if they understood or not how to use each node.
2. Goal is not mentioned as a proposition but as an execution statement or a function statement.
   We showed a proper description to the participants after the they created their assurance cases.
3. Strategy is misunderstood as a judgment branching.
   We showed poor examples to help the participants avoid their misunderstanding.
4. Decompose by not discussion but the order of function.
   Mistake (4) however is accepted in some situations. There are cases where describing functions in details entail decomposition by the order of function.

A pre-test questionnaire

A pre-test questionnaire on assurance cases was carried out before the participants take the test. Responses were given on a five-point ordinal scale; from -2 (disagree), 0 (neither agree nor disagree) to +2 (agree). The questionnaire included free descriptive answers to write their situations so that the data of the free descriptive answers can be used for analysis in this study.

Test

In order to confirm whether the beginners were able to create assurance cases, we had the participants describe the contents that they propose to the stakeholders, and intend to assure (hereinafter referred to as “contents described in assurance cases”).

A post-test questionnaire

A post-test questionnaire was carried out after the participants took the test. Same as the pre-test questionnaire, responses were given on a five-point ordinal scale, and the questionnaire included free descriptive answers to write their situations so that the data from the free descriptive answers can be used for analysis in this study.

Test scoring

The test results were scored by three assurance case researchers.

4. Evaluation

4.1 Evaluation Method

We took different approaches to evaluate the created assurance cases and the questionnaire answers.

Evaluation method for the created assurance cases

Three assurance case researchers evaluated the assurance cases created by the participants, and
categorized the mistakes, if any, into “four common mistakes beginners make”, and “other mistakes in creating assurance cases”. In case that a mistake found in the assurance case created is relevant to multiple categories, we categorized the mistake into all the relevant categories. We set the Pass/Fail criteria as follows: An assurance case described without a mistake: Pass; An assurance case described with mistake(s): Fail.

In addition, the three researchers evaluated the assurance cases created in terms of Understanding and Utility. Responses were given on a three-point ordinal scale; “1 Hard to understand, 2 Understandable, 3 Easy to understand”, and “1 Hard to use, 2 Usable, 3 Easy to use”.

Evaluation method for questionnaires
Questions in this study requested the participants to provide free descriptive answers, and responses on a five-point ordinal scale. The pre-test questionnaire and the post-test questionnaire asked five questions each.
This study evaluated two points, analyzing the above-mentioned answers.

First, we used paired t-test to assess if assurance cases make it easy to find strengths and weaknesses of the contents described in assurance cases. The reason being that previous research has not shown for which of visualizing strengths and visualizing weaknesses assurance cases work better. This study compared the answers to the following questions:
Weaknesses: Did you think assurance cases are effective for finding weaknesses of the contents you propose?
Strengths: Did you think assurance cases are effective for finding strengths of the contents you propose?

Second, we compared the advantages and disadvantages of creating assurance cases, using the free descriptive answers in the pre- and post-test questionnaires. The reason being that the participants are likely to describe, in the free descriptive answers, challenges in assurance case description if any. In addition, a larger number of disadvantages than advantages would suggest more significance of the challenge, and a larger number of advantages than disadvantages would suggest less significance of the challenge.

The concrete analysis method of this study, using qualitative coding method [10], is as follows;
Step 1: Pick up, from the free descriptive answers, those related to advantages and disadvantages of creating assurance cases. Set a viewpoint for creating an affinity diagram (Step 2). This study set “advantages and disadvantages of creating assurance cases” as the viewpoint, in order to identify challenges in assurance case description.
Step 2: Categorize the comments from the viewpoint above by creating an affinity diagram.
Step 3: Give a name to each category group with a slightly higher abstraction level. (hereinafter referred to as “Open coding results”)

Step 4: With regard to free descriptive answers, count the number of sentences related to Open coding results, as well as the number of participants who wrote the sentences.
This study ensured the validity of analysis through the three assurance case researchers’ review on the Open coding results and the totaled results. [11]

4.2 Evaluation Results
Table 1 is a list of participants.
Table 1: List of participants
| Age | Participants |
|-----|--------------|
| 20’s| L, M         |
| 30’s| B, C, E, J, N|
| 40’s| A, D, F, K   |
| 50’s-| G, H, I      |

Table 2 shows the number of nodes made by each participant.
Table 2: Number of nodes made by each participant

|        | Goal | Strategy | Context | Evidence | Total |
|--------|------|----------|---------|----------|-------|
| A      | 13   | 3        | 25      | 82       |
| B      | 15   | 6        | 13      | 74       |
| C      | 9    | 1        | 13      | 56       |
| D      | 16   | 2        | 9       | 71       |
| E      | 13   | 6        | 8       | 34       |
| F      | 22   | 3        | 19      | 86       |
| G      | 14   | 8        | 14      | 6        | 42    |
| H      | 16   | 19       | 10      | 61       |
| I      | 15   | 3        | 8       | 38       |
| J      | 11   | 13       | 3       | 67       |
| K      | 9    | 4        | 22      | 75       |
| L      | 19   | 4        | 2       | 29       |
| M      | 13   | 13       | 1       | 67       |
| N      | 16   | 1       | 26      | 85       |

Analysis on the free descriptive answers revealed issues in assurance case description, which have not been pointed out in the previous studies. In addition, the results showed that no branching was set in the Context. We therefore set the following eight viewpoints for evaluating the assurance cases created by the participant A to N (hereinafter referred to as “Mistake (1) to (8)”).
1. Write in a wrong node of “Strategy” instead of “Goal”
2. Goal is not mentioned as a proposition but as an execution statement or a function statement.
3. Strategy is misunderstood as a judgment branching.
4. Decompose by not discussion but the order of function.
5. Use case is created in the Goal and the Strategy.
6. Strategy is decomposed using vague words such as “etc.”
7. Goal is described using a noun, changed from a sentence.
8. Multiple Strategies are set for the Goal.

We set the Pass/Fail criteria as follows: An assurance case described without a mistake: Pass; An assurance case described with mistake(s): Fail.
Table 3 shows the results of each participant’s evaluation on Understanding and Utility.

As shown in Table 3, 35.7% (5 of 14) of the participants’ assurance case description was appropriate. One out of the five participants took a table-top lecture and the other four took an e-learning lecture. We thus consider that creating assurance cases is straightforward enough to understand without a lecture in person, but not necessarily easy.

Table 3: Results of each participant’s evaluation

|   | Understanding | Utility |
|---|---------------|---------|
| A | Pass          | Fail    |
| B | Fail          | Fail    |
| C | Pass          | Pass    |
| D | Fail          | Fail    |
| E | Fail          | Pass    |
| F | Fail          | Fail    |
| G | Fail          | Fail    |
| H | Fail          | Fail    |
| I | Pass          | Fail    |
| J | Pass          | Fail    |
| K | Pass          | Pass    |
| L | Pass          | Fail    |
| M | Pass          | Pass    |
| N | Pass          | Pass    |
| % | 21.4%         | 0.0%    |

Table 4 shows the results of paired t-test on the strengths and weaknesses of the contents described in assurance cases, which were visualized by the created assurance cases. For the strengths and weaknesses of the contents described in assurance cases, which were visualized by the created assurance cases, the difference was confirmed to be statistically significant as to the average value, with p = 0.027 as shown in Table 4. Table 5 shows Open coding results of the free descriptive answers.

Table 4: Results of paired t-test

|   | Average p value (two-tailed test) |
|---|----------------------------------|
| Weaknesses | 1.3077 | 0.027 |
| Strengths  | 0.8462 |        |

With the disadvantage of “Need to set appropriate conditions for description, depending on the contents to be assured” being ranked the 3rd in Table 5 (the 3rd as to both the number of relevant sentences and the participants who wrote the sentences; 10 of 14 participants), we consider creating assurance cases is not necessarily easy.

4.3 Discussion

Three assurance case researchers in total evaluated the results in order to avoid personal evaluation by a single researcher.

Evaluation results of created assurance cases

This section discusses the evaluation results of created assurance cases from the perspective of Mistake (5) to (8) first, followed by Mistake (1) to (4).

Mistake (7) Goal is described using a noun, changed from a sentence: As shown in Table 3, 50% (7 of 14) of the participants made this mistake. We presume that the participants tended to write only the breakdown results (noun) in order to avoid duplicate description because they have described what to assure in the Goal, which was set initially. A future study therefore could propose a description method based on this description rule using nouns.

Mistake (5) Use case is created in the Goal and the Strategy: As shown in Table 3, 21.4% (3 of 14) of the participants made this mistake. They presumably had an understanding that they could describe the Goal using a noun after having had written what to assure in the Strategy.

Mistake (8) Multiple Strategies are set for the Goal: Based on the assurance case description rule, it is a mistake to set multiple Strategies for the Goal. However, if assurance case users intend to assure the contents described in assurance cases by decomposing the Goal from multiple viewpoints, it is effective to change the rule accordingly, which is the case of the participants of this study who made Mistake (8).

Mistake (6) Strategy is decomposed using vague words such as “etc.”: This mistake needs to be pointed out and corrected to assure the contents described in
assurance cases. Vague words such as “etc.” make the decomposition unclear as to what to include and what not to include.

Evaluation results from the perspective of Mistake (7), (5), and (8) therefore suggest future study could propose an assurance case description rule based on the rules those participants wrongly followed, instead of the current description rule.

Next, we discuss the evaluation results of created assurance cases in terms of the “four common mistakes beginners make” in creating assurance cases (Mistake (1) to (4)). The participants of this study did not make mistakes in relation to Mistake (2) Goal is not mentioned as a proposition but as an execution statement or a function statement, and (4) Decomposed by not discussion but the execution order of function.

Mistake (1) Write in a wrong node of “Strategy” instead of “Goal”: The participants who made this mistake wrote a noun in the Goal and a verb (e.g., Assure) in the Strategy, which makes sense in the Japanese language with the combination of the Strategy and the Goal making a phrase. The wrong description leads to easiness to understand the created assurance case, which results in this mistake.

Mistake (3) Strategy is misunderstood as a judgment branching: As Yamamoto et al. [5] also pointed out, this mistake is caused by decomposition misunderstood as making judgment in flow charts.

Based on the discussion above, a description rule easy for beginners to use is required for helping them create assurance cases without mistakes. If the beginners need to memorize all the rules to create assurance cases, creating assurance cases becomes more difficult. Future study thus could propose a new description method based on the rules the participants of this study wrongly followed, instead of the current assurance case description rule. Mistakes in description suggests that the existing description method is difficult for people without knowledge on assurance cases to understand, as shown in the evaluation results of created assurance cases. Areas of future study also include proposing a description rule for each node, which at the same time takes into account the linkage of nodes.

Understanding and Utility

This section discusses the evaluation results of the created assurance cases in terms of Understanding and Utility (Table 3).

Among the created assurance cases, those given a “Pass” grade were rated relatively high, while those given a “Fail” grade were rated lower but not necessarily “Hard to understand”/ “Hard to use”. The results therefore suggested that mistakes in creating assurance cases do not always negatively impact Understanding and Utility. We suppose it necessary to set an appropriate description rule depending on the contents to be assured.

Results of paired t-test

As shown in Table 1, this study failed to collect a statistically significant number of questionnaires, and thus made the assessment based on descriptive study. [12] In Table 4, both average of weaknesses=1.3077 and average of strengths=0.8462 are positive values. We consider therefore assurance cases are effective for identifying strengths and weaknesses of the contents described in assurance cases. For the weaknesses and strengths, the difference was confirmed to be statistically significant as to the average value, with p = 0.027 as shown in Table 4. The descriptive study thus showed that assurance cases visualize weaknesses of the contents described in assurance cases more easily than strengths.

Open coding results

This section discusses the Open coding results (Table 5) first in terms of the advantages of creating assurance cases, followed by the disadvantages.

“Show the weaknesses of the contents described in assurance cases with the assured range being clarified”: This advantage infers that creating assurance cases clarifies the assured range of the contents described in assurance cases as a result of assurance case users’ confirming the Evidence of the Goal. The weakness of the contents described in assurance cases is namely the Goal without Evidences described. Table 4 also supports this discussion.

“Show the validity of the contents described in assurance cases”: This perception is similar to the above-mentioned advantage of “Show the weaknesses of the contents described in assurance cases with the assured range being clarified”. This advantage infers that creating assurance cases enables the users to see the validity through confirming the Evidences of the Goal.

“Sort out the current situation logically”: This advantage infers that creating assurance cases enables the users to break down the current situation in a Mutually Exclusive and Collectively Exhaustive (MECE) way, and thereby sort out the situation by themselves.

“Helpful to identify issues of the contents described in assurance cases”: This perception is similar to the above-mentioned advantage of “Show the weaknesses of the contents described in assurance cases with the assured range being clarified”. This advantage infers that creating assurance cases enables the users to recognize what they failed to indicate in the assurance case created. For instance, users may find unexpected situation in relation to the contents described in assurance cases while setting Strategies, which decompose the Goal.

“Assure the strengths of the contents described in assurance cases”: This perception is similar to the above-mentioned advantage of “Show the weaknesses of the contents described in assurance cases with the assured range being clarified”. Assurance case users may have an understanding that assurance cases assure the contents described in assurance cases by setting the Goal with Evidences as a strength, which is conversely a weakness of the contents described in assurance cases. With Table 4 also supporting this discussion, this descriptive study showed that assurance cases work better for visualizing
weaknesses of the contents described in assurance cases than visualizing the strengths.

Based on the above-mentioned advantages, we consider creating assurance cases is helpful for grasping the current situation related to the contents described in assurance cases, as well as identifying issues, weaknesses and strengths of the contents described in assurance cases.

Next, we discuss the disadvantages of creating assurance cases.

“Need to set appropriate conditions for description, depending on the contents to be assured”: This disadvantage suggests the necessity of developing a description rule easy for beginners to use as we discussed earlier. We suppose assurance cases need to be created depending on the contents to be assured.

“Difficult to develop the Strategy”: Participants of this study pointed out the difficulty of decomposing in a MECE and complete way, and considering the range of decomposition. We thus need to provide guidelines of decomposition for setting Strategies.

“Need to change the abstraction level of description depending on the stakeholders”: This perception is similar to the above-mentioned disadvantage of “Difficult to develop the Strategy”, and focuses more on decomposition in creating assurance cases. Participants of this study pointed out, for instance, the necessity of adjusting the abstraction level of description to the stakeholders, depending on what information the user is to provide to the stakeholders. We therefore need to take account of stakeholders in considering guidelines of decomposition for creating assurance cases.

The Open coding results of these three disadvantages mentioned here are in line with our discussion earlier on evaluation results of created assurance cases, as well as Understanding and Utility.

This study therefore drew two conclusions. First, future study needs to propose a description rule for creating assurance cases, as well as the relevant guidelines, which take in account the characteristics of the contents to be assured, and the stakeholders to use the created assurance cases. Our argument is in line with the results of this study pointed out the necessity of a description rule for creating assurance cases as well as the relevant guidelines, which take in account the characteristics of the contents to be assured, and the stakeholders to use the created assurance cases.

Based on the discussion above and the previous studies, challenges of assurance case description method in Japanese organizations include the followings:

(1) Write in a wrong node of “Strategy” instead of “Goal”
(2) Goal is not mentioned as a proposition but as an execution statement or a function statement.
(3) Strategy is misunderstood as a judgment branching.
(4) Decompose by not discussion but the order of function
(5) Use case is created in the Goal and the Strategy.
(6) Strategy is decomposed using vague words such as “etc.”
(7) Goal is described using a noun, changed from a sentence.
(8) Multiple Strategies are set for the Goal.

Future study therefore needs to develop description rules and guidelines for creating assurance cases to address the eight challenges. The results of this study will contribute to improvement in the usage of assurance cases in the management field.

Acknowledgments

We appreciate FONT Co., Ltd. (http://osakahonyaku.com/) for its collaboration with us to conduct this study. Nobuyuki Kobayashi was supported by Doctoral Student Aid Program of Keio University.

References

[1] ISO 26262-10-2012(E)-Road vehicles-Functional safety-Part 10: Guideline on ISO26262
Challenges of Assurance Case Description Method in Japan

[2] ISO 15026-2-2011. Systems and Software engineering Part2: Assurance case

[3] N.Kobayashi, M.Kawase, S.Shirosaka: A Proposal for an Assurance Case Description Method -Aiming to Tackle Challenges in Work-Related Communication-, Journal of Japan Association for Management Systems, Vol. 33, No.2, (2016), 91-107,

[4] N.Kobayashi, A.Nakamoto, M.Kawase, S.Shirosaka: Comparison of Two Quantitative Evaluation Methods for Assurance Cases, International Journal of Japan Association for Management Systems, Vol. 8 No.1, (2016), 27-34

[5] S.Yamamoto, Y.Matsuno: A Consideration on Developing Dependability Case., IEICE technical report. KBSE, The Institute of Electronics, Information and Communication Engineers. Vol.112, No.165, (2012), 61-66

[6] Tim Kelly: Arguing Safety – A Systematic Approach to Managing Safety Case, Ph.D. Thesis, University of York, (1998)

[7] Catherine Menon, Richard Hawkins, John McDermid: Defence Standard 00-56 Issue 4: Towards Evidence-Based Safety Standards., Proceedings of the Seventeenth Safety-Critical Systems Symposium, (2009), 223-243.

[8] GSN Community.: GSN COMMUNITY STANDARD VERSION 1, Origin Consulting (York), (2011)

[9] Y.Matsuno, T.Takai, S.Yamamoto: D-Case NYUUMONN Dependability Case WO KAIITEMIYOU!(D-Case Introduction. -Let's write a dependability case!-), Daitec Holding Co., Ltd. (2012), 67-82

[10] A.Strauss and J. Corbin.: Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory, third edition, London, Sage Publications., (2008)

[11] N.Golafshani.: Understanding Reliability and Validity in Qualitative Research, The Qualitative Report Vol. 8 No.4 December 2003, (2003), pp.597-607.

[12] D. F. Polit, B. P. Hungler: Nursing Research: Principles and Methods (6th Ed.), (Philadelphia, Lippincott, 1999).

[13] S.Kobayashi, S.Yamamoto: A Proposal on Service Deployment Decision Method using Assurance Case., IEICE technical report. KBSE, The Institute of Electronics, Information and Communication Engineers. Vol.111, No.489, (2012), 7-12.

[14] T.Kaneko: CC-Case: An Integrated Method of Security Analysis and Assurance. , Institute of Information Security, Ph.D. Thesis., (2014)
