Four-Layered Assurance Case Description Method Using D-Case

Nobuyuki KOBAYASHI^{a*}, Aki NAKAMOTO^b, Maki KAWASE^c,
Fiona SUSSAN^d, Makoto IOKI^b, Seiko SHIRASAKA^b

^aDevelopment Administration Department, KATO WORKS CO., LTD.

1-9-37 Higashioi, Shinagawa-ku, Tokyo 140-0011 Japan

^bGraduate School of System Design and Management,

Keio University, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8526 Japan

^cCenter for Collaborative Research and Community Cooperation,

Hiroshima University, 2-313 Kagamiyama, Higashi-Hiroshima-shi, Hiroshima 739-8527 Japan

^dCenter for Global Business and Information Technology Research, University of Phoenix, School of Advanced Studies, John Sperling Center for Educational Innovation, 4025 S. Riverpoint Pkwy, Phoenix, AZ 85040, USA

Abstract

Recently, assurance cases standardized by ISO have received a lot of attention from researchers. A previous study showed that it is appropriate to use assurance case to demonstrate the improved feasibility of accomplishing management vision and management strategy using four models (Management vision model, Management strategy model, Business process model, and IT system model). However, in the previous study, concrete description methods were not discussed.

Filling this gap of knowledge, this study aims to show a detailed four-layered assurance case description method using D-Case approach to connect multiple layers of the hierarchical structure of an assurance case. This is an improvement from the previous in that it now focuses on one layer for improving the feasibility of accomplishing both management vision and management strategy. As a result, this study contributes to the existing literature by adding a description method for a four-layered assurance case that includes 30 steps and uses D-Case. This study concludes with future research topics.

Keywords: Assurance Case, Goal Structuring Notation, D-Case, Four-layered Assurance case

1. Introduction

Assurance cases standardized by international standards of ISO 15026-2-2011 [1], ISO 26262 [2], and others have received a lot of attention from researchers. Recently, researchers have reported that assurance cases can be applied to managing documents and processes in systems engineering. Kobayashi et al. showed an improved feasibility of accomplishing management vision and management strategy by comparing a total of eight models which were described in an assurance case (ISO 15026-2-2011) [1]. The eight models are a repeated measure of a set of four models (Management vision model, Management strategy model, Business process model, and IT system model), with one set before and one set after the implementation of an organization's management strategy [3].

The results of their research concluded that assurance cases are useful in the various fields including management [4] [5]. Kobayashi et al. [3] however stopped short of showing a description method for describing four models of the Management vision model, Management strategy model, Business process model, and IT system model. This study therefore aims to show a description method for four-layered assurance cases with an aim to describe the four models.

There are various description methods with regard to assurance cases. Kaneko [6] briefly demonstrated models relevant to assurance cases. Kobayashi et al. proposed three description methods for describing 1) the layers between management vision and business process [7], 2) the layer of business process [4], and 3) the layers between business process and IT system [8]. The novelty of this study therefore is to show a four-layered assurance case description method using D-Case through connecting four layers of the hierarchical structure of an assurance case, instead of focusing on one layer, in order to improve the feasibility of accomplishing both management vision and management strategy.

Section 2 summarizes assurance case (D-Case) description methods. Section 3 describes the proposed description method. Section 4 shows description results using the description method proposed in Section 3. Section 5 concludes with future research directions.

2. Previous Studies

Safety cases were proposed by Kelly et al. [9] in 1998 as a means of conducting a clear, complete and reasonable discussion. The argument is that using the safety case will help operations to reach an acceptable level of safety among stakeholders. An assurance case [10] extends the

*Corresponding author: n-kobayashi@kato-works.co.jp

discussion area to the whole quality of the discussed system including “safety” as proposed in the safety case. An assurance case (D-Case) is mainly a description method using six nodes, including Goal, Context, Strategy, Evidence, Monitoring, and Undeveloped [11] [12]. These six nodes are shown in Table 1.

Table 1: Explanation of Six nodes for D-Case

Node	Figure	Explanation
Goal		Goal describes what to assure, with a combination of a subject and predicate.
Strategy		Strategy describes how to break down the Goal into sub-goals leading to the lower layer.
Context		Context describes the state, or environment and conditions of the System, and shows ways to lead to the Goal and Strategy.
Evidence		Evidence eventually assures that we can reach the Goal, and shows ways to lead to the Goal.
Monitoring		Monitoring is intended to represent Evidence available at runtime, corresponding to the target values of in-operation ranges.
Undeveloped		Undeveloped shows the status that there is no Evidence or Monitoring, or discussion supporting the Goal.

3. Description Method for a Four-Layered Assurance Case

In this chapter, we will describe the four models, which Kobayashi et al. [3] showed. This study uses the four models as the description method for a four-layered assurance case.

3.2 Management vision model

The Management vision model is a layer of an assurance case, which describes the activities to set numerical targets linking the management vision and the management strategy.

3.3 Management strategy model

The Management strategy model is a layer of an assurance case, which describes the activities that are relevant to the details of management strategy based on the numerical targets identified in order to reach

management vision. This model describes management strategy only, and does not include business process.

3.4 Business process model

The Business process model is a layer of an assurance case, which describes concrete activities in the business process to implement the management strategy. As this model details the business process, it clarifies who is in charge of each activity in the business process, and who has assured the business process. Thus, personnel placement and business improvement will be needed in proportion to the workload.

3.5 IT system model

The IT system model is a layer of an assurance case, which describes the IT system corresponding to the business process. This model defines the business process the IT system supports, and the business process operated manually, which as a result clarifies the range of the IT system.

4. Proposed method by using D-Case

In the following part, we will present our proposed method for describing four-layered assurance cases by using D-Case.

4.1 Steps of describing management vision model

- Step 1: Set Goal node.
- Step 2: Set Context node as sub-goals by dividing the Goal into sub-goals.
- Step 3: Set priorities, if any, in the Context node when the priority of sub-goals is important.
- Step 4: For the Strategy node, divide the Goal into sub-goals (in prioritized order, if any).
- Step 5: Set the sub-goals (in prioritized order if any) underneath the Strategy node.
- Step 6: Set Evidence nodes if the sub-goals need to be prioritized.
- Assume Step 5 to be Step 1, and repeat this process until sub-goal nodes are completely decomposed.
- Step 7: For the Strategy node, divide the Goal node below into management vision and management strategy.

4.2 Steps of describing management strategy model

- Step 8: Set Goal nodes respectively for management vision and management strategy.
- Step 9: Set Evidence nodes for Goal nodes of management vision.
- Step 10: Set Evidence nodes as Context nodes since they are prerequisites of Goal nodes of management strategy.
- Step 11: Set priorities, if any, in the Context node when the priority of sub-strategies is important.

As with the management vision model, and repeat this process until sub-goal nodes are completely decomposed.

Step 12: For Strategy node, divide the Goal node below into management strategy and business process for implementing management strategy.

Step 13: Set Evidence nodes for Goal nodes of management strategy.

Step 14: Set Evidence nodes as Context nodes since they are prerequisites of Goal nodes of sub-strategy.

Step 15: Management strategy set Evidence nodes or Monitoring nodes as Context nodes since they are prerequisites of Goal nodes of business process for implementing management strategy.

4.3 Steps of describing business process model

Step 16: Set Goal node of business process for implementing management strategy.

Step 17: Set Context node as sub-functions by dividing the Goal into sub-functions.

Step 18: Set priorities, if any, in the Context node when the priority of sub-functions is important.

Step 19: For Strategy node, divide the Goal into sub-functions (in prioritized order, if any).

Step 20: Set the sub-goals (in prioritized order if any) underneath the Strategy node.

Step 21: Set Evidence nodes if the sub-goals need to be prioritized.

Assume Step 20 to be Step 16, and repeat this process until sub-goal nodes are completely decomposed.

Step 22: Set Context nodes as operating conditions (which department carries out what is written in the Goal) for each goal.

Step 23: For Strategy node, divide the Goal node below into the one at the time of business process design, and the one at the time of business process implementation.

Step 24: Set Goal nodes respectively for the time of business process design, and the time of business process implementation.

Step 25: For Strategy node, divide the Goal node at the time of business process design into the business process tier and the application tier.

Step 26: Set Evidence nodes for Goal nodes of the business process tier.

Step 27: Set Evidence nodes of the business process tier as Context nodes of the application tier.

4.4 Steps of describing IT system model

Step 28: For Strategy node, divide the Goal node of the application tier below into functions needed to information system applications.

Step 29: Set Evidence nodes for sub-Goal nodes of each function.

Step 30: Set Monitor nodes for Goal nodes at the time of business process implementation.

Next, we summarize the above-mentioned steps. Kobayashi et al. [7] presented the steps of describing the management vision model. Step 1-Step 7 of this study shows the procedure to decompose the goals set as a management vision until the top goal of management strategy. The evidence nodes given to the goal nodes set within the management vision model can be considered a prerequisite for considering the management strategy. The lowest goal of the management vision model can also be called the top goal of the management strategy model.

Kobayashi et al. [7] presented the steps of describing the management strategy model. Step 8-Step 15 of this study shows the procedure to decompose “the top goal of the management strategy” into “the management strategy linked to the business process”. The evidence nodes given to the goal nodes set within the management strategy model can be considered a prerequisite for considering the business process.

Kobayashi et al. [4] presented the description steps of describing the business process model. Kobayashi et al. [4] divided the business process model into three layers. This study also calls the three layers “the business process model”. Step 16-Step 27 of this study is shown the procedure to decompose “the business process” into “the business process that the person in charge can decide”. The evidence nodes given to the goal nodes set within the business process model can be considered a prerequisite for considering the IT system.

Kobayashi et al. [8] presented the steps of describing the IT system model. Kobayashi et al. [8] divided the IT system model into two layers. This study also calls the two layers “the IT system model”. Steps 28-Step 30 of this study shows the procedure for the decomposing goals node of IT system into necessary functions for IT system. In addition, it means that what you decide within the IT system model will determine the items to be monitored by affecting the business process. The four-layered assurance case description method proposed in this study thereby integrates the description steps presented in the previous studies [4] [7] [8].

5. Results and Discussion

This study shows description results using the description method proposed in Section 4. Specifically, collaborating with a Japanese manufacturing company of construction machinery, we created the management vision model, the management strategy model, the business process model, and IT system model. Figures 1- Figure 4 as a whole presents an example of description using the proposed description method.

Figure 1 shows Step 1 to Step 7, which mainly describe the management vision model. The top goal of the management vision is shown as “At least, achieve contribution to the society through excellent products” in Figure 1. Subsequently, when dividing the management vision into the management strategy, we set “sales JPY100 bil” and “overseas ratio 50%” as sub-goals of the management vision in Figure 1. In addition, “Document of medium-term management plan” that is set in the

evidence node of the management vision is a prerequisite for the management strategy. The description results of

the assurance case description method proposed in the previous study [7] correspond to Figure 1.

Figure 1 Steps of describing Management vision model (Step 1-7)

Figure 2 Steps of describing Management strategy model (Step 8-15)

Four-Layered Assurance Case Description Method Using D-Case

Figure 3 Steps of describing Business process model (Step 16-27)

Figure 4 Steps of describing IT system model (Step 28-30)

Figure 2 shows Step 8 to Step 15, which mainly describe the management strategy model. Based on "Document of medium-term management plan", we divide the management strategy into "Sales strategy" and "Production strategy" in Figure 2. Figure 2 shows that the document set in the evidence node of the management strategy are a prerequisite for the business process. The description results of the assurance case description method proposed in the previous study [7] correspond to Figure 2.

Figure 3 shows Step 16 to Step 27, which mainly describes the business process model. Figure 3 shows that the business process is divided into sub-goals of "Sales process", "Manufacturing process", "Procurement process", and "Maintenance process". In addition, Figure 3 shows that "Procurement process" is further divided and connected to sub-goal of the business process. The description results of the assurance case description method proposed in the previous studies [4] [7] correspond to Figure 3. Figure 3 shows that the Overseas materials department "Sends order information" which is the sub-goal of "Procurement process". In Figure 3, the sub-goal of the business process is divided into the business process tier and the application tier. The document set in the evidence node of business process tier are a prerequisite for the IT system. The description results of the assurance case description method proposed in the previous study [8] correspond to Figure 3.

Figure 4 shows Step 28 to Step 30, which mainly describes the IT system model. Figure 4 shows the application tier that "Overseas materials department sends order information at the time of business process design", and the evidence node for the sub-goal of the application tier. Figure 4 also shows that the evidence node for the sub-goal of the application tier is a prerequisite for the monitoring at the time of business process implementation. The description results of the assurance case description method proposed in the previous study [8] correspond to Figure 4. Figure 1-4 thereby show the description results using the proposed description method,

which integrated the description methods of the previous studies [4] [7] [8].

In the following part, we will discuss why the proposed description method used the steps mentioned above. The reason being that this study allowed the stakeholders to define the scope of each layer—the management vision, the management strategy, the business process, and the IT system—and to what extent they describe each layer in detail. By definition, an assurance case is a method to assure the stakeholders' acceptable level of quality. Companies use various expressions and perspectives to refer to each layer: for example, management vision, management philosophy, mission, strategy, measures, business processes to refer to management vision. Thus, each company can define each layer, which is the ground of Step 1 to Step 30 in this study. Future research topic therefore assesses whether other users of the proposed description method can make their own definition of the four layers.

Next, we will describe the relevance of this study to the previous studies. The proposed method in this study integrated the description methods of the previous studies [4] [7] [8]. Kobayashi et al. [7] proposed a method to solve a communication challenge, which was:

1) Companies fail to share the management vision (purpose) sufficiently.

Kobayashi et al. [4] proposed a method to solve three communication challenges, which were:

2) Employees fail to smoothly collaborate with other departments and groups because they do not grasp the connection of the work they engage in, and the other work.

3) Employees are not motivated with the work they engage in, and do not contemplate the purpose of the work.

4) There are many cases business improvement proposed by employees are not accepted because conventional ways are preferred.

Kobayashi et al. [8] proposed a method to solve two communication challenges, which were:

5) Organizations fail to assess the functions required for IT systems sufficiently.

6) Organizations need to handle the new requirements for IT systems.

Since the proposed method integrated the three description methods [4] [7] [8], this study therefore suggests that the proposed method solves the six communication challenges at the same time. The reason being that, as shown in previous studies [4] [7] [8], six communication challenges were solved in each model before the three description methods were integrated. In addition, Kobayashi et al. [3] stated that using the four-layered assurance case is likely to increase the feasibility of accomplishing the management vision and the management strategy. Summarizing the discussion above, we conclude that the four-layered assurance case description method solves the six communication challenges, and increases the feasibility of accomplishing the management vision and the management strategy.

6. Conclusions

This study aimed to show a four-layered assurance case description method for describing four models of the Management vision model, Management strategy model, Business process model, and IT system model. This study showed description examples by the proposed description method. Thus the four-layered assurance case can be described to increase the feasibility of accomplishing management vision and management strategy by using D-Case.

Future research topics include:

- Assist the users' understanding of the description rule for assurance cases.
- Examine how an assurance case grows, and how to manage it when a company uses it for several years.
- Increase the number of applications of the proposed method.
- Assess whether other users of the proposed description method can make their own definition of the four layers.

References

- [1] ISO15026-2-2011. Systems and Software engineering Part2: Assurance case
- [2] ISO26262-10-2012(E)-Road vehicles-Functional safety-Part 10: Guideline on ISO26262
- [3] N. Kobayashi, A. Nakamoto, M. Kawase, F. Sussan, S. Shirasaka : What Model(s) of Assurance Cases Will Increase the Feasibility of Accomplishing Both Vision and Strategy? , *Review of Integrative Business and Economics Research*, Vol. 7, No.2, (2018), 1-17.
- [4] N. Kobayashi, M. Kawase, S. Shirasaka : 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,
- [5] N. Kobayashi, A. Nakamoto, M. Kawase, S. Shirasaka: Comparison of Two Quantitative Evaluation Methods for Assurance Cases, *International Journal of Japan Association for Management Systems*, Vol. 8 No.1, (2016), 27-34
- [6] T. Kaneko: CC-Case: An Integrated Method of Security Analysis and Assurance. , Institute of Information Security, Ph.D. Thesis., (2014)
- [7] N. Kobayashi, M. Kawase, S. Shirasaka: A Proposal of Assurance Case Description Method for Sharing a Company's Vision, *Journal of Japan Association for Management Systems*, Vol.34, No.1, (2017), 85-94
- [8] N. Kobayashi, M. Kawase, S. Shirasaka: A Proposal for an Assurance Case Description Method for Business Assignment Using Information Systems, *Journal of Japan Association for Management Systems*, Vol.34, No.3, (2018), 321-328
- [9] Tim Kelly: Arguing Safety – A Systematic Approach to Managing Safety Case, Ph.D. Thesis, University of York, (1998)
- [10] 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.
- [11] GSN Community.: *GSN COMMUNITY STANDARD VERSION 1*, Origin Consulting (York), (2011)
- [12] Y. Matsuno, T. Takai, S. Yamamoto: *D-Case NYUUMONN Dependability Case WO KAITEMIYOU!(D-Case Introduction. -Let's write a dependability case!-)*, Daitec Holding Co., Ltd. (2012), 67-82