A Proposal of Assurance Case Description Method Using Process of ISO 15288

Nobuyuki KOBAYASHI\textsuperscript{a*}, Eriko HIKISHIMA\textsuperscript{a}, Aki NAKAMOTO\textsuperscript{b}, Tsuguto INAYAMA\textsuperscript{b}, Makoto IOKI\textsuperscript{b}, Seiko SHIRASAKA\textsuperscript{b}

\textsuperscript{a}The 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

\textsuperscript{b}Graduate School of System Design and Management, Keio University, 4-1-1 Hiyoshi, Kohoku-ku, Yokohama-shi, Kanagawa 223-8526 Japan

Abstract

Previous studies showed that using assurance cases to increase the feasibility of accomplishing management vision and management strategy. The assurance case description method proposed by previous studies, however, does not take into account the work whose purpose changes in the progress. This study proposes an assurance case description method according to the PROCESS definition defined in this study, for being able to visualize that assuring a task whose purpose changes according to the work progress. The reason we refer to ISO 15288:2015 is that PROCESS defined in ISO 15288:2015 considers Purpose, and thus assumes changes in a certain work’s purpose in the progress of the work. This study evaluates the effectiveness of both a) being able to understand the purpose of PROCESS and b) being able to visualize that assuring a work whose purpose changes according to the work progress by using both open coding and paired t-test. Based on the paired t-test result, the proposed description method was judged effective compared with current practice, about a) being able to understand the purpose of PROCESS and b) being able to visualize that assuring a work whose purpose changes according to the work progress. Furthermore, from the open coding results, the results suggested why the proposed description method is effective. This study concludes with future research topics.

Keywords: Process, Assurance case, Goal Structuring Notation, D-Case,

1. Introduction

Kobayashi et al. proposed assurance case [1] description method for solving communication challenges in business [2] [3] [4]. Kobayashi et al. also showed that using assurance cases increases the feasibility of accomplishing management vision and management strategy [5] [6]. The assurance case description method proposed by Kobayashi et al., however, does not take into account the work whose purpose changes in the progress. The example includes design work whose purpose changes agilely. It is required to consider the purpose of work each time depending on the progress of work.

This study extends the definitions provided inside ISO 15288:2015 [7] and applies the extended definition to our assurance case description method. The reason we refer to ISO 15288:2015 is that PROCESS defined in ISO 15288:2015 considers Purpose, and thus assumes changes in a certain work’s purpose in the progress of the work. As shown in Figure 1, in ISO 15288:2015, each PROCESS needs Purpose, Outcome and one or more ACTIVITY. Figure 1 shows that the PROCESS needs to have no PROCESS, or one or more PROCESS. The PROCESS of Figure 1 needs one or more arbitrary ACTIVITYs. In Addition, the ACTIVITY of Figure 1 needs one or more arbitrary TASKs. ISO15288:2015 [7] indicates PROCESS, ACTIVITY, and TASK as follows: “Processes require a purpose and outcome. All processes have at least one activity. Activities are constructs for grouping together related tasks. The activities provide a means to look at related tasks within the process to improve understanding and communication of the process. If an activity is cohesive enough, it can be converted to a (lower level) process by drafting a purpose and a set of outcomes. A task is a detailed provision for implementation of a process. It may be a requirement (“shall”), a recommendation (“should”), or a permission (“may”).”

“Purpose
The purpose of the Infrastructure Management process is to provide the infrastructure and services to projects to support organization and project objectives throughout the life cycle.
This process defines, provides and maintains the facilities, tools, and communications and information technology assets needed for the organization’s business with respect to the scope of this International Standard.

Outcomes
As a result of the successful implementation of the Infrastructure Management process:
a) The requirements for infrastructure are defined.
b) The infrastructure elements are identified and specified.
c) Infrastructure elements are developed or acquired.
d) The infrastructure is available.

Activities and Tasks
The organization shall implement the following activities and tasks in accordance with applicable organization policies and procedures with respect to the Infrastructure Management process.
a) Establish the infrastructure. This activity consists of the following tasks:
1) Define project infrastructure requirements.
2) Identify, obtain and provide infrastructure resources and services that are needed to implement and support projects.
b) Maintain the infrastructure. This activity consists of the following tasks:
1) Evaluate the degree to which delivered infrastructure resources satisfy project needs.
2) Identify and provide improvements or changes to the infrastructure resources as the project requirements change.”

PROCESS of ISO 15288:2015, however, lacking steps, which companies need for implementing the PROCESS. The process because doesn’t have to define steps. This study therefore additionally uses a concept called PROCEDURE, and defines in PROCEDURE the steps supposed by the companies. For example, as shown in Figure 2, we set PROCEDURE with multiple PROCESS connected one another. PROCESS and its steps are determined inside a PROCEDURE.

Figure 2 The description example of PROCEDURE

When setting the optimized steps of PROCESS to PROCEDURE, it is desirable that each PROCESS is set as the minimum unit. As shown in Figure 3, we thus set one ACTIVITY in PROCESS as the minimum unit of PROCESS. The reason is that the person in charge of updating the PROCESS may misunderstand that they can combine PROCESS by combining multiple ACTIVITYs, which would make PROCESS huge, namely a black box. As a result, the PROCEDURE becomes obsolete over time, and unnecessary ACTIVITYs remain in PROCESS, which leads to increase in cost. Therefore, each PROCESS is required to be managed in the minimum unit.

Figure 3 The definition of this study made by the authors
(Revised definition of ISO15288:2015)

In addition, the setting method of the sequence of the PROCESS in PROCEDURE varies depending on the company; therefore the setting method itself is not defined in this study.
This study therefore aims to define the PROCESS because the PROCESS is not defined in detail in ISO 15288:2015. The evaluation carries out with three people who understand and satisfy the following conditions; a person who recognizes the difference between PROCESS and the word Process that is commonly used in Japanese contexts, knowing the PROCEDURE construction, and administrator of PROCESS. The evaluation was conducted with those three people, whether the definition of PROCESS can be understood. This study secures validity by the above evaluation. This study proposes an assurance case description method according to the PROCESS definition defined in this study, for being able to visualize that assuring a task whose purpose changes according to the work progress. In addition, the reason for this proposal is that Kobayashi et al. [8] described the need to develop description rules and guidelines for creating assurance cases.
This study evaluates the effectiveness of both "being able to understand the purpose of PROCESS" and "being able to visualize that assuring a work whose purpose changes according to the work progress" by using both open
coding and paired t-test. This study concludes with future research topics.

2. PROCESS definitions

Combination of plurality PROCESS is not limited to PROCESS presented in ISO 15288:2015. Since PROCESS itself exists in multiple fields, the selection range of PROCESS is not limited to ISO 15288:2015. However, there is a prerequisite that the steps exist in PROCEDURE, but there are no steps in PROCESS. The format for expressing PROCESS in ISO 15288:2015 is defined in INCOSE (2016) [9] and is shown in Figure 4.

![Figure 4 PROCESS indicated by INCOSE (modified by authors)](image)

There is no mention of the classification method regarding the conditions of Controls in Figure 4. Therefore, the classification method is defined as follows in this study. As shown in Table 1, the classification method for utilizing in the enterprise is divided into four conditions of A, B, C and D according to the two axes, whether there is a scientific basis and whether it is determined arbitrarily.

<table>
<thead>
<tr>
<th>Based on a scientific basis</th>
<th>NOT arbitrarily</th>
<th>arbitrarily</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition A</td>
<td></td>
<td>Condition B</td>
</tr>
<tr>
<td>Condition C</td>
<td></td>
<td>Condition D</td>
</tr>
</tbody>
</table>

For example, when a condition is based on a scientific basis, the condition will be described using evidence such as a calculation formula explaining the scientific basis or a paper. Since the judgment of arbitrarily includes the organizational culture, a condition will be described based on an agreement for the judgment of arbitrarily among stakeholders. Having expressed the conditions in Table 1, this study is able to visualize how the conditions are determined. This study shows an example for Manufacturing of lighter.

The condition A in Table 1 indicates that the Condition A is based on a scientific basis but not an arbitrary. For example, the organization that has a custom of lighting incense stickers with lighter.

The Condition D in Table 1 indicates that the condition D is not based on a scientific basis but an arbitrary. For example, including in the condition that whether the lighter can easily set the fire, even though we do not use the lighter in space. In other words, despite knowing that it will not be used, there is work to check.

Classifying into four conditions like above will enable to make a judgment possible that which is significant and which is not.

An example of judgment is shown below. The condition A and C can be thought as prerequisite to some extent because those are conditions of not arbitrary. On the other hand, since the Condition B and D are arbitrary, it is necessary to reconsider whether to make it conditional. As a result, the four conditions can be used for both visualizing the Controls in enterprise and as judgement criteria for continually improving the conditions defined in Controls, assuming the reuse of PROCESS.

Next, the ISO 15288:2015 PROCESS covers the purpose, Figure 4 indicated by the INCOSE is not an expression considering the purpose and result. The definition of PROCESS in this study therefore is re-expressed in Figure 5 based on PROCESS indicated by INCOSE.

![Figure 5 PROCESS definition defined in this study](image)

The definitions given in Figure 5 are defined as follows.
- Define purpose of this process: Define the purpose of PROCESS.
- Measure: Judgment criteria for “Outputs” (for example, to define units).
- Convert & divide: Convert interpretation to “Inputs” from input-information of PROCESS.
- Input: input information for ACTIVITY from “Convert & divide”.
- Controls: The conditions specified in A, B, C and D are determined.
- Enablers: The “Enablers” that are bound by Controls.
- ACTIVITY: ACTIVITY premised on “Enablers”.
- Outputs: Output-information from ACTIVITY.
- Review: “Outputs” are determined by Measure. NG will start over again.
- Convert: Convert interpretation of “Outputs” after approved in “Review”.
- Satisfied Purpose: the purpose that satisfied the purpose of PROCESS.

This study confirmed with three persons who understand and satisfy the following conditions; a person who recognizes the difference between PROCESS and the
word Process are commonly used in Japanese contexts, PROCEDURE construction and PROCESS administrator. As a result, this study had evaluated that the three administrators can understand, the reliability of the PROCESS definitions therefore was secured.

3. Previous Studies

GSN [10], which was proposed by Kelly [11] in 1998, is one of the notation methods used for safety cases 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 [12] extends the 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 [10] [13]. These six nodes are shown in Table 2.

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

4. Proposed description method using PROCESS definitions

As for the description method, PROCEDURE decomposition, PROCESS decomposition, ACTIVITY decomposition and TASK decomposition are proposed in this study. In order to try disassembling at each viewpoint, the example is picked up from department 1 in Figure 2. The Figure 6 expresses ACTIVITY in PROCESS. Representing the definition of Section 2, the Enablers are presupposing Controls.

![Figure 6 Expressed by PROCEDURE viewpoint.](image)

ACTIVITY is established on the premise of Enablers. The Figure 7 represents the TASK in ACTIVITY from (1) in Figure 6. The reason Controls is defined in Figure 7 is that, it is a prerequisite to performing an ACTIVITY defined in INCOSE (2016) [9] in Figure 4. Therefore, it is necessary to set common Controls for a plurality of TASKs for realizing ACTIVITY.

![Figure 7 Expressed (1) in Figure 6 with ACTIVITY viewpoint.](image)

As Figure 6 explains, the Controls and Enablers are different in each PROCESS. The decomposition results are shown in Figure 8-9. The Figure 8 explains the PROCEDURE decomposition and PROCESS decomposition. The Figure 9 explains the ACTIVITY decomposition and TASK decomposition.

-PROCEDURE decomposition is a way of dividing into PROCESS set in PROCEDURE.
-PROCESS decomposition can be broken up individually in items with the PROCESS definition shown in Figure 5. The explanation of each item is as shown in Section 2.
-ACTIVITY decomposition is a way of dividing into TASK set in ACTIVITY.
-TASK decomposition is decomposed into “TASK input”, “TASK processing” and “TASK output” using a way closer to process decomposition indicated by Matsuno et al. (2012) [13]. But, “TASK input” and “TASK output” exist as necessary, these therefore are not necessarily present.

5. Evaluation and Discussion

5.1 Evaluation Methods

Applicability of this study is to apply the decomposition method indicated in Chapter 3 to PROCEDURE for formulating cross-company security policy. The reason for this is because such work has never been done in the company and the purpose of work changes dynamically similar to design work.
The evaluation methods are enforced in correspondence relation of Table 3.

Table 4 shows the criteria of assessments and questionnaire statements for assessing "being able to understand the purpose of PROCESS" and "being able to visualize that assuring a work whose purpose changes according to the work progress" of the proposed description method. Responses were given on a five-point ordinal scale, ranging from -2-"disagree," to +2-"agree," with 0 representing "neither agree nor disagree." Scores from +1 to +2 were assumed to be valid for business improvement. With regard to the qualitative data analysis, free descriptive answers were used as the data, and analyzed by the following procedure, using qualitative coding methods [14].

Step 1: Picking up the interviewer’s answer related to the assurance case from the descriptive answer in survey and decide the viewpoint, which is going to be used to
categorize the Affinity Diagram in the next step. The viewpoint was set as "reason being able to understand the purpose of PROCESS," in order to evaluate if the purpose of PROCESS is being understood by using assurance case.

Step 2: Based on the viewpoint aforementioned in Step 1, sort the descriptive comments with similar meaning into groups according to the Affinity Diagram.

Step 3: Write titles for each group that summarizes the essence of the group, at a slightly higher level of abstraction (called "Open coding results" in this study).

Step 4: Count the number of descriptive answers related to open coding results.

Table 3 Correspondence between Evaluation methods and Evaluation items.

<table>
<thead>
<tr>
<th>Evaluation methods</th>
<th>Evaluation items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paired-t test</td>
<td>Being able to understand the purpose of PROCESS.</td>
</tr>
<tr>
<td>Open coding</td>
<td>Being able to visualize that assuring a work whose purpose changes according to the work progress.</td>
</tr>
</tbody>
</table>

Table 4 Correspondence between Questionnaire statement and Criteria of assessment.

<table>
<thead>
<tr>
<th>Criteria of assessment</th>
<th>Questionnaire statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Being able to understand the purpose of PROCESS before seeing the assurance case.</td>
<td>Do you think to be able to understand the purpose of PROCESS in the business of the company you work now?</td>
</tr>
<tr>
<td>Being able to visualize that assuring a work whose purpose changes according to the work progress before seeing the assurance case.</td>
<td>Do you think to be able to visualize that assuring a work whose purpose changes according to the work progress in the business of the company you work now?</td>
</tr>
<tr>
<td>Being able to understand the purpose of PROCESS after seeing the assurance case.</td>
<td>Did you think to be able to understand the purpose of PROCESS for the work you described by using Assurance case?</td>
</tr>
<tr>
<td>Being able to visualize that assuring a work whose purpose changes according to the work progress after seeing the assurance case.</td>
<td>Did you think to be able to visualize that assuring a work whose purpose changes according to the work progress by using Assurance case?</td>
</tr>
</tbody>
</table>

5.2 Evaluation Results

This section describes the evaluation results. Respondents of twenty-three answered after showing the assurance case actually created. Respondents are persons engaged in a work whose purpose changes according to the work progress and indicate the attribute information of the work experience years in Table 5. The reason for showing the work experience years is that, the respondents who have work experience for many years can understand that the purpose changes according to the work progress, thus we considered that they can judge the proposed method is effective or not.

Table 5 The work experience years.

<table>
<thead>
<tr>
<th>The work experience years</th>
<th>Number of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-5</td>
<td>3</td>
</tr>
<tr>
<td>6-10</td>
<td>4</td>
</tr>
<tr>
<td>11-20</td>
<td>8</td>
</tr>
<tr>
<td>21-</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
</tr>
</tbody>
</table>

Table 6 The results of the questionnaire

<table>
<thead>
<tr>
<th>Criteria of assessment</th>
<th>Average</th>
<th>Standard deviation</th>
<th>p value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Being able to understand the purpose of PROCESS before seeing the assurance case.</td>
<td>1.91</td>
<td>1.083</td>
<td>0.001</td>
</tr>
<tr>
<td>Being able to understand the purpose of PROCESS after seeing the assurance case.</td>
<td>3.30</td>
<td>1.146</td>
<td></td>
</tr>
<tr>
<td>Being able to visualize that assuring a work whose purpose changes according to the work progress before seeing the assurance case.</td>
<td>2.65</td>
<td>1.229</td>
<td>0.024</td>
</tr>
<tr>
<td>Being able to visualize that assuring a work whose purpose changes according to the work progress after seeing the assurance case.</td>
<td>3.52</td>
<td>1.163</td>
<td></td>
</tr>
</tbody>
</table>

This study evaluated with two situations. One situation is the situation of each respondent's current work, and another situation is after showing the described assurance case.

In order to confirm that an assurance case can be described, the confirmation being done by actually describing an assurance case.

Next, the results of the questionnaires as well as paired t-test are shown in Table 6.
purpose changes according to the work progress.” The difference was confirmed to be statistically significant as to the average value, with Table 6 showing p = 0.024. The open coding results are shown in Table 7.

Table 7 The open coding results.

<table>
<thead>
<tr>
<th>Open coding results</th>
<th>Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using assurance case can grasp Hierarchical relationship on the premise of purpose.</td>
<td>29</td>
</tr>
<tr>
<td>Using assurance case can match the purpose and the action.</td>
<td>26</td>
</tr>
<tr>
<td>Using assurance case can describe considering the PROCESS.</td>
<td>16</td>
</tr>
<tr>
<td>Using assurance case can understand the components of PROCESS.</td>
<td>15</td>
</tr>
<tr>
<td>Using assurance case can explain to a third party</td>
<td>6</td>
</tr>
<tr>
<td>The judgment criteria for the changed purpose become clear</td>
<td>4</td>
</tr>
<tr>
<td>Using assurance case will consider to improve ACTIVITY</td>
<td>3</td>
</tr>
</tbody>
</table>

5.3 Discussion

Based on the paired t-test result, the proposed description method was judged effective about "being able to understand the purpose of PROCESS" and "being able to visualize that assuring a work whose purpose changes according to the work progress". This study failed to collect a statistically significant number of questionnaires, and thus made the assessment based on descriptive study [15]. Next, the open coding results will be described.

“Using assurance case can grasp Hierarchical relationship on the premise of purpose”: This comment describes what we realized by writing Assurance Case. The proposed description method therefore contributes to understanding the purpose of PROCESS.

“Using assurance case can match the purpose and the action”: This comment describes that thinking to improve actions will work by understanding the purpose, as a result, it will be possible to conduct activities which match the action and the purpose. Therefore, the proposed description method contributes to both being able to understand the purpose of PROCESS and being able to visualize that assuring a work whose purpose changes according to the work progress.

“Using assurance case can describe considering the PROCESS”: This comment describes what we realized from describing it in the rule of the assurance case, the proposed description method contributes to understanding the purpose of PROCESS.

“Using assurance case can understand the components of PROCESS”: The proposed description method is contributing to understand the purpose of PROCESS, as it is realized with the detailed definition defined in this study.

“Using assurance case can explain to a third party”: This comment describes it is realized by way of using the Assurance case, the proposed description method therefore contributes to understanding the purpose of PROCESS. Because it is impossible to explain to the third party if you cannot understand the purpose of PROCESS.

“The judgment criteria for the changed purpose become clear”: This comment describes what is being realized in thinking, the proposed description method contributes to understanding the purpose of PROCESS. In addition, this comment describes that being able to visualize that assuring a work whose purpose changes according to the work progress. Because we use evidence nodes indicating that we assure to show the criteria for judgment in the proposed description method.

“Using assurance case will consider to improve ACTIVITY”: This comment describes what is being realized in the thought of writer/reader for an assurance case, the proposed description method therefore contributes to being able to visualize that assuring a work whose purpose changes according to the work progress. Because it is necessary to grasp the criteria of judgment by using evidence nodes indicating that the top goal is assured in order to think about improving ACTIVITY.

Based on the above, we can understand the components of PROCESS, we can consider the PROCESS when describes the assurance case, and we can think about improving ACTIVITY, therefore the proposed description method leads to understanding the purpose of PROCESS. Furthermore, the judgment criteria for the purpose become clearer, we will think to improve ACTIVITY, and we can match the purpose and the action, therefore the proposed description method can visualize that assuring a work whose purpose changes according to the work progress.

6. Conclusions

This study proposed an assurance case description method according to the PROCESS definition, for being able to visualize that assuring a task whose purpose changes according to the work progress. Based on the paired t-test result, the proposed description method was judged effective compared with current practice, about “being able to understand the purpose of PROCESS” and “being able to visualize that assuring a work whose purpose changes according to the work progress”. Furthermore, from the open coding results, the results suggested why the proposed description method is effective. This study can be seen from the difference of each average value shown in Table 6, there is a possibility that the effectiveness may be further improved. Improving the expression method therefore is possible in the future. Future challenge includes increasing the number of applications.

References


