Assurance case review using System Theory

Shuichiro YAMAMOTO*, Shuji MORISAKI*

*Graduate School of Informatics, Nagoya University, Furo-Cho, Chikusa-ku, Nagoya, 464-8601 Japan

Abstract

Assurance case is widely recognized as the fundamental document to certify safety critical systems. Several assurance case review methods are proposed to validate correctness of syntax rules, and traceability among artifacts and assurance cases. However, it is not established to review assurance cases from the point of target configuration information to be assured. In this paper, an assurance case review approach is proposed based on system theory. The proposed approach uses a system diagram to represent configuration information such as artifact models, quality attributes, and risk definitions. The primary contribution of this paper is a framework for reviewing assurance cases based on system theoretic information extracted from target assurance cases to satisfy description rules.

Keywords: dependability, assurance case, review, system theory, experimental evaluation

1. Introduction

The safety case, the assurance case, and the dependability case are currently the focus of considerable attention for the purpose of providing assurance and confidence that systems are safe. Methods have thus been proposed for representing these using Goal Structuring Notation (GSN) [1, 2, 3, 4, 5]. Review rules [6, 7] for assurance cases are proposed based on GSN. For example, the direct principle is defined to evaluate how extent the argument and evidences directly support the conclusion. The review principle shows that the claim is stronger supported if it has multiple independent arguments and evidences, because the defect for the one argument option does not affect another option. The validity of assurance cases depends not only the argument structure but on the content information of assurance cases. The content information includes artefact constituents, risk factors, and quality attributes. If the content information is not analysed, it is difficult to confirm the validity of the assurance cases in total.

This paper proposes a review method for assurance cases based on the content information that is represented by the systemigram [8].

Section 2 describes related work on the review methods of assurance cases. Section 3 proposes an approach to review assurance cases based on the systemigram. Section 4 describes an example of applying the proposed approach to review an assurance case. In section 5, we discuss the effectiveness of the proposed approach. Section 6 concludes the paper and shows the future work.

2. Related work

The safety case, the assurance case, and the dependability case are currently the focus of considerable attention for the purpose of providing assurance and confidence that systems are safe. Methods have thus been proposed for representing these using Goal Structuring Notation (GSN). Kelly proposed the review approach consists of four steps for the assurance case [6]. In the first step of the review method, reviewers try to understand the argument structure. Then, the validity of the argument structure is confirmed. The sufficiency and completeness of argument situation are also confirmed. Finally, the critique and refutation of the argument are confirmed. The stepwise review process only repeats the third process. Kelly also discussed six quality attributes of review, such as completeness, independency, boundedness, directness, relationship and robustness.

Context evidence matrix (CEM) is proposed to review GSN [9]. CEM represents the relationship between context and evidences. The method can be used to evaluate the equivalence and inclusion relationships between GSNs by generating CEMs from GSNs.

Matsumura and others [10] proposed a method to generate the Word Relationship Diagram (WRD) from D-Case. D-Case is an extended assurance case to argue about dependability. The WRD development rules extract the word relationship from claims, strategies, context, and evidences by analysing node names in Natural language.

Matsumura and others also proposed a method to develop D-case based on Context Dependency Diagram [11].

The OMG (Object Management Group) defined the Structured Assurance Case Metamodel (SACM) to clarify overall concepts on assurance cases [12]. Although SACM provides rich notions to define assurance cases, it was not concentrated assurance case review.

Stefan [13] proposed the Quamoco quality meta-model that contains product factor and quality aspects. The Quamoco quality meta-model did not concern the assurance case argument.

Boadman proposed the systemigram [8, 14] as the simple diagram that has the clear relationship with natural language sentences based on the system model diagram.
The system model diagram was originally used in the SSM (Soft System Methodology) by Checkland [15]. SSM was developed to analyze complex human behavior. Fig.1 shows an example of systemigram. There are three nodes, containment, internal and external nodes in the systemigram. The containment node contains the internal node. The Link-a and Link-b are the relationships between nodes.

Nodes of systemigrams represent artefacts, agents, and critical attributes. Node names are defined by noun phrases. Node links define the relationship between nodes. Links are named by verb phrases.

Systemigrams were widely used to represent complex systems [16, 17]. For example, the 7 samurai model of systems engineering [18] can be easily described in systemigram. The editor of systemigram, named as systemitool [19], can be used.

3. Assurance Case Review Approach

3.1 Relationship between context information and assurance case

In this paper, claims are categorized in the following two types, attribute and measure claims.

[Type 1] Attribute claim
<System> satisfies <Attribute>

[Type 2] Countermeasure claim
<System> takes countermeasures against <Risk>

The attribute claim is decomposed into sub claims by the constituents of the system. For the attribute claim of the system and the corresponding countermeasure claim, there is the relationship that the attribute claim is achieved by the claim. In this case, the context of the decomposition argument shall be the risk of countermeasure claim. The countermeasure claims are supported by evidences. The claims are the lowest claims.

3.2 Relationship between assurance cases and systemigrams

For an attribute claim, the following systemigram in Fig.2 is developed. The outer node is the object of the claim. The inner node of the object is the attribute of the claim. The diagram shows that the object has the attribute as its state.

If the system includes multiple elements, elements are described as the inner nodes of the system node. For example, two elements A and B are consisted in the system, the following systemigram in Fig.3 is developed.

The countermeasure claim is necessary to achieve that system satisfies the attribute. The following systemigram is developed to describe the situation. The countermeasure contributes to achieve the attribute of the system by providing resolution means for the risk that will harm the corresponding attribute.

Fig. 4 shows the inter relationship among attribute, risk and countermeasure. The risk harms the attribute of the system. The countermeasure resolves the risk and contributes the attribute.

Fig. 5 shows that the countermeasure is supported by the evidence fact.
Table 1 Review Rules

<table>
<thead>
<tr>
<th>View points</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Completeness</td>
<td>1) no omissions 2) attribute risks are defined 3) counter measures are existed for risks 4) configuration information is corresponded to context 5) evidences are existed for countermeasure</td>
</tr>
<tr>
<td>Clarity</td>
<td>1) clear 2) no same name for different nodes 3) no undefined concept</td>
</tr>
<tr>
<td>Appropriateness</td>
<td>1) no errors 2) necessary items are included 3) unnecessary items are not included</td>
</tr>
<tr>
<td>Traceability</td>
<td>1) clearness of evidences 2) no omission on transitive closure of relationships</td>
</tr>
</tbody>
</table>

Step 3) Cause analysis.
The cause of the problem is clarified by analyzing omissions and errors in systemigram.

Step 4) Revision.
The assurance case is revised by resolving problems detected in the above steps.

3.4 Example
This section shows the application of the proposed review method for the assurance case to explain that train operation is safe shown in Fig.6.

![Figure 6 Assurance case for safety train operation](image)

The following systemigram in Fig. 7 can be developed from Fig.6. The systemigram satisfies review rule 1) 2) 3) 4) of completeness. As the rule 5) is defined for evidences, the rule is not applied for the systemigram.

The node “train operation” in Fig. 7 includes nodes, “safe”, “risk”, “train driver”, “operation place” and “natural environment”. The “train operation” and “safe” nodes are extracted from the top claim “train operation is safe” of Fig.6, as the “safe” is the attribute of the “train operation”. The “risk” node of the “train operation” node is extracted from the context description of Fig.6. In the same way, “train driver” node of the systemigram includes “safe” and “risk” nodes.

For the clarity rule 2), there are nodes of the same name, such as safe and risk. As these names are used to represent states of different object nodes, there is no problem to use these same names.

The Fig. 8 shows the portion of the assurance case for the claim that train operator is safe. The Fig. 9 is the systemigram derived from Fig. 8.

![Figure 7 Systemigram for the assurance case in Fig.6](image)

![Figure 8 Assurance case for the claim of drivers safety](image)

![Figure 9 Systemigram for the assurance case in Fig.8](image)

Fig. 10 shows the portion of the assurance case for that train operation places are safe. Fig.11 is the systemigram developed from Fig. 10.

![Figure 10 Assurance case to show that train operation places are safe](image)
The systemigram in Fig.11 clarifies the risk mitigation measure that ATS has been installed. The corresponding evidence is also clarified. This shows the triangle relationship among attribute, risk, and countermeasure in Fig. 5.

![Figure 11 Systemigram for the assurance case in Fig.10](image1)

Finally, Fig.12 shows the portion of the assurance case for that natural environment is safe. Fig.13 is the systemigram developed from Fig. 12.

![Figure 12 Assurance case to show that natural environment is safe](image2)

The countermeasure for the safety is defined for the natural phenomena not for the natural environment as the systemigram shows in Fig.13. Therefore, it is necessary to unify natural environment and natural phenomena, or clarify their inter-relationship.

![Figure 13 Systemigram for the assurance case in Fig.12](image3)

In this way, the proposed approach can find mistakes caused by detecting lacks of the dependence relationships among words that are in the claim statements of assurance cases. If there is isolated concept word in the derived systemigram from the assurance case, the concept represents that the corresponding assurance case claim statement causes ambiguity. As the approach provides a systematic procedure and review rules to derive systemigram from assurance cases, the approach is expected to help reviewers find these kinds of errors in assurance cases.

4. Case Study

The example study was conducted to evaluate the effectiveness of the proposed assurance case review approach.

4.2 Over view of the review

The target system of the case study is a simple embedded system to boil water by an electric heater. The subjects were ordered to assure the target system by describing assurance cases. The number of subjects was 14. The described assurance cases were reviewed by two reviewers. The reviewers evaluate assurance cases independently. They first reviewed assurance cases without systemigram. Then they reviewed same assurance cases with systemigram again.

4.3 Result

Table II shows the number of improper items according to improper types defined in Table I. In the Table II, traditional review did not use systemigram. The proposed review uses systemigram. For the completeness and appropriateness, traditional review did not detect improper points. Whereas the proposed review detected 25 and 57 improper points for the category of completeness and appropriateness respectively.

<table>
<thead>
<tr>
<th>Category</th>
<th>Traditional review</th>
<th>Proposed review</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>common</td>
<td>different</td>
</tr>
<tr>
<td>Completeness</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Clarity</td>
<td>0</td>
<td>63</td>
</tr>
<tr>
<td>Appropriateness</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Traceability</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>total</td>
<td>10</td>
<td>68</td>
</tr>
</tbody>
</table>

4.4 Comparison of review Capability

The mean number of improper items pointed out by reviewers with systemigram was 9.4. The mean number of improper points commonly pointed is 5.4. Therefore, the number of improper points was approximately 57.4%.

<table>
<thead>
<tr>
<th>Review type</th>
<th>common</th>
<th>different</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed review</td>
<td>5.4</td>
<td>4</td>
<td>9.4</td>
</tr>
<tr>
<td>Traditional review</td>
<td>0.9</td>
<td>2.2</td>
<td>3.1</td>
</tr>
</tbody>
</table>

The mean number of improper points by traditional review method was 3.1. The mean number of improper points commonly detected was 0.9. Therefore, the approximately 71% of improper points was differently detected by reviewers for the traditional review.

To evaluate the mean value of common detected points, MCDP, and the ration of the number of common detection points, CDR, the following symbols are defined.
MCDP: mean value of common detection points
NoCDP: the number of common detection points
NoR: the number of reviewers =2
NoDDP: the number of different detection points
NoS: the number of subjects =14
CDR: the ratio of the number of common detection points
TDP: total number of detection points

Based on the above definition, we can derive the following equations.
MCDP = (NoCDP + NoDDP / NoR) / NoS
CDR = NoCDP / TDP

By using these equations, MCDP and CDR for traditional and proposed reviews can be calculated as follows.
MCDP for traditional review is (10+68/2)/14=3.14
CDR for traditional review is 10/78= 12.8%
MCDP for proposed review is (76+122/2)/14= 9.79
CDR for proposed review is 76/198= 38.3%

MCDP for traditional and proposed review are 3.14 and 9.79 respectively. The ratio of the number of common detected points for traditional and proposed review method are 12.8% and 38.3% respectively.

Fig. 14 shows the comparison of the number of common detected points and common detection ratio for the traditional and proposed review.

5. Discussion

In this section, we discuss on the effectiveness and limitations of the proposed method.

5.1 Effectiveness

As the example study showed, the systemigram based approach was useful to analyze the problems of the given assurance case. The conflict among words of claims and context detected by the systemigram may not be clear only by checking the given assurance case. This showed that the effectiveness of the proposed method. Although the evaluation was only executed for a simple example, same results can be expected for other assurance cases.

The case study showed that the number of improper items for system theoretic review was 3 times higher than those of traditional review. Therefore, the proposed approach can improve the effectiveness of assurance case review.

5.2 Review Meta Model

The Meta model of the systemigram in Fig.3 can be described as in Fig.15. The Meta model is simple but sufficient to execute assurance case review. The system can be decomposed into sub systems. The attribute is also decomposed into sub attributes. The system and sub systems shall satisfy the corresponding attributes. The risk may harm system and attributes. The countermeasures resolve risks and contribute attributes that system shall satisfy. The evidence proves the validity of the corresponding countermeasure.

5.3 Novelty

Although there are some studies on the assurance case review such as [20,21], there was no approach that applies systemigram to review assurance cases so far. Northern Territory Government Australia [20] showed the regulation-based check items of safety cases to be reviewed. However, it lacks review method of descriptive statements of safety case nodes. UK Ministry of Defense [21] developed the Acquisition Safety & Environmental Management System (ASEMS). The AEMS provides safety case review objectives and examples of poor safety cases.

The proposed method to review assurance cases for safety management systems combines the assurance case and systemigram for the first time. This paper, in addition, proposed the assurance case review meta model as well as the mapping rule between assurance cases and systemigrams. Assurance cases discuss the validity of the claim by decomposing it with a tree structure. By describing business goals as claims, the validity of business activities can be argued by using assurance cases. For example, BGSN [22] has been proposed to discuss the applicability of assurance case towards business IT governance. However, the review approach of BGSN has not been realized. The BGSN review approach can easily be realized by analyzing claims of BGSN with the proposed method using systemigram. Furthermore, the content of goal sentences created by the goal-oriented business strategy method such as B-SCP [23] can be analyzed using the proposed method so that the relationship between terms constituting the business strategy can be reviewed.
5.4 Limitation

This paper only examines the effectiveness of the proposed method for a simple example assurance case. It is necessary to show the effectiveness of the method by evaluating number of assurance cases. This paper also examined the effectiveness of the review approach for an example quantitatively. More quantitative evaluations of the proposed method are also necessary.

The detection commonality of the proposed method also can be improved. More strict review rules are necessary to reduce the number of different kinds of inappropriateness among reviewers. The quantitative evaluation of the proposed method showed that the number of improper items commonly pointed out was still not high. It is necessary to improve the commonality of pointed improper items among reviewers by using systemigram.

6. Conclusion

This paper introduced the method for reviewing assurance cases by visualizing context information with systemigram. The 13 review rules were specified by the points of completeness, clarity, appropriateness, and traceability. An evaluation example of the approach was also shown for detecting problems of sentences among claims and context of the assurance case. The example evaluations showed the effectiveness of the approach.

The contribution of the paper are as follows.

The systematic assurance case review method has been proposed by using the system theory. Moreover, the effectiveness of the proposed method has been evaluated by an experiment. The Meta model of assurance case review concept has also been defined based on the systemigram model for assuring that system satisfies attributes.

Future work includes more experimental evaluations of the proposed approach, and the comparative analysis with traditional review methods. The transformation rules to systemigram from assurance cases shall also be precisely defined to improve the detection commonality of reviewers.

Acknowledgments

This work has been conducted as a part of "Research Initiative on Advanced Software Engineering in 2015" supported by Software Reliability Enhancement Center (SEC), Information Technology Promotion Agency Japan (IPA).

References(Sample)