Creation of Assurance Case Using Collaboration Diagram

Takuya Saruwatari, Shuichiro Yamamoto

Creation of Assurance case using Collaboration diagram

Takuya Saruwatari[1] and Shuichiro Yamamoto[2]

[1] Graduate School of Information Science Nagoya University, Nagoya, Japan
saruwatari.takuya@e.mbox.nagoya-u.ac.jp,
[2] Strategy Office, Information and Communications Headquarters, Nagoya University, Japan
yamamotosui@icts.nagoya-u.ac.jp

Abstract. Recently, serious failures of complex IT systems are becoming social problems. Assurance case attracts an attention as a technique to assure the dependability of critical systems. We have proposed d* framework which is an extended assurance case notation based on the network of dependable actors. In this paper, The assurance case creation procedure that creates the assurance case from the collaboration diagram is proposed and the case study is performed using this procedure. In this case study, a result is described by d* framework.

Keywords: assurance case, dependability, d* framework, collaboration diagram

1 Introduction

Recently, serious failures on complex IT systems are becoming social problems. A failure of critical system raises a significant loss. Therefore, assurance of dependability of such critical systems is an important issue. But, it is not an easy task. In such a situation, an assurance case attracts an attention as a technique to assure the dependability of critical systems. In the assurance case, the argument of dependability is described. GSN (Goal Structuring Notation) [1] is proposed as a graphical notation of assurance cases. d* framework (d*) which introduced the concept of actor to extend assurance case [2] is also proposed. In this paper, the assurance case creation procedure that creates the assurance case from a collaboration diagram is proposed and the case study is performed using it.

In section 2, some related works are described. In section 3, d* framework is described. It is used in the proposed procedure. In section 4, the assurance case creation procedure is descirbed. In section 5, the case study is described. Discussions and conclusions are described in section 6 and section 7.

2 Related work

The assurance case is a document that describes argument of system dependability. Such a document is needed for critical systems that require high assurance.

Dependability is defined as an integrated concept including availability, reliability, safety, integrity, and maintainability [3]. The assurance case is proposed as the document that describes argument of system safety. This may be called safety case. GSN [1] and CAE (Claim, Argument Evidence) [4] are proposed as graphical notation to describe a safety case. In GSN, safety cases are described mainly by four types of nodes (goal, strategy, evidence, and context) and two types of relationships ("supported by" and "in context of"). Recently, target of assurance case is extended to dependability[5]. An assurance case for dependability may be called as dependability case. There are several definitions for the assurance case. One definition is shown as follows [6].

A documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment.

There are many researches for the assurance case. In [7], a module concept of assurance case is researched. By using the module of the assurance case, there is an advantage that can manage and represent a large assurance case. Creation process of assurance case is also researched. In [1], six process steps are proposed to create safety cases based on GSN. Another assurance creation methods are also proposed [8]. Meanwhile, method for the decomposition of arguments as required when creating assurance cases is proposed [9], [10].

3 d* framework (d*)

The d* framework (d*) is an extended assurance case notation [2]. In d*, an actor concept is introduced into assurance case. 5 types of node (actor, goal, strategy, context, and evidence) and 4 types of relationship ("supported by", "in context of", "depend on", and "belong to") of nodes are defined. An actor is a new element. Previous notations do not have it. A person, an organization, a system, a subsystem, and a component etc. can be defined as actor.

4 Assurance case creation procedure

In this paper, an assurance case creation procedure is proposed. The assurance case is created from collaboration diagram in this procedure. It is consisted of 3 steps. They are shown below.

- Step 1 : Actor definition
  Actors of assurance case are defined. Objects in a collaboration diagram are defined as actors in an assurance case.
- Step 2 : Inter dependency definition
  Arguments (goal) between actors in an assurance case are defined using message relationships between objects in collaboration diagram.
- Step 3 : Actor merging
  Actors that should be merged into one actor are merged.

5 Case study

5.1 Collaboration diagram of target system

The target system for case study is an "AP Download system". Using this system, user can select the application (AP) and download it from the system to his/her IC Card. The collaboration diagram of target system is shown in Fig. 1. In this diagram, 6 objects and 13 message relationships between them are represented.

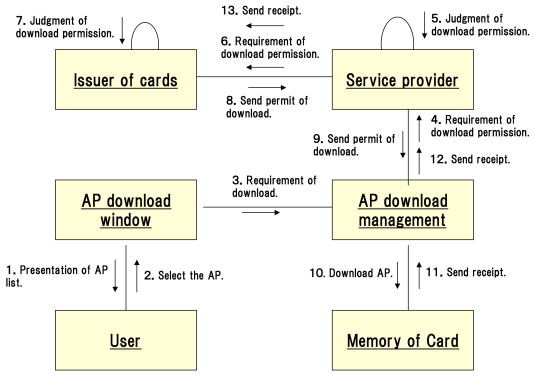

Fig. 1. Collaboration diagram of AP download system.

5.2 Creation Experiment

In the case study, the assurance case creation experiment is performed. The created assurance case is described by d*. The result of experiment for each step in procedure is shown as below.

1. Step 1
   In this step, 6 objects are defined as assurance case's actor from collaboration diagram. The 6 actors are "Issuer of cards", "Service provider", "AP download window", "AP download management", "User", and "Memory of Card".
2. Step 2
   In this step, 8 dependability arguments (goals) are defined between actors. For example, "Sevice provider" requires the download permission to "Issuer of cards" and "Issuer of cards" permits the download to "Service provider" in the collaboration diagram. Therefore, it is considered that "Issuer of the card" depend on "Service provider". The dependum is that "only permitted AP can be downloaded". Created assurance case is shown in Fig. 2.

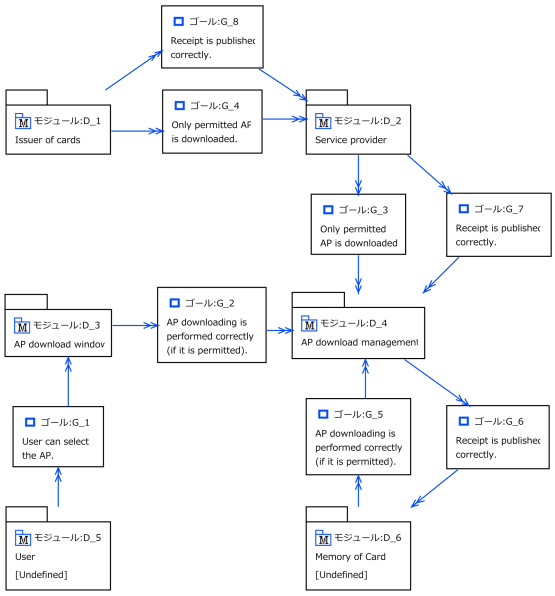

Fig. 2. Assurance case after Step 2.

3. Step 3
   In this step, “AP download window” and “AP download management” are merged. The two actors are included in the same system. Therefore,they are merged. The new actor is “AP download system”. Modified assurance case is shown in Fig. 3.

6 Discussions

6.1 Merits of using collaboration diagrams

When creating assurance case, it is convenient if there is information that can be used. In this research, it is confirmed that collaboration diagram is useful for creating assurance case. 2 merits are shown as follows. 1) The actor of assurance case can be defined using collaboration diagram’s object. 2) The dependability requirement between actors of assurance case can be considered using message relationships of collaboration diagram. In the case study, 6 actors are defined in the assurance case from 6 objects in the collaboration diagram directly (Step 1). Moreover, 8 dependability requirements between actors are defined from message relationships in the collaboration diagram (Step 2). In this definition, 13 message relationships in collaboration diagram are used. Thus, it can be say that collaboration diagram is useful, when assurance case is created by d*.

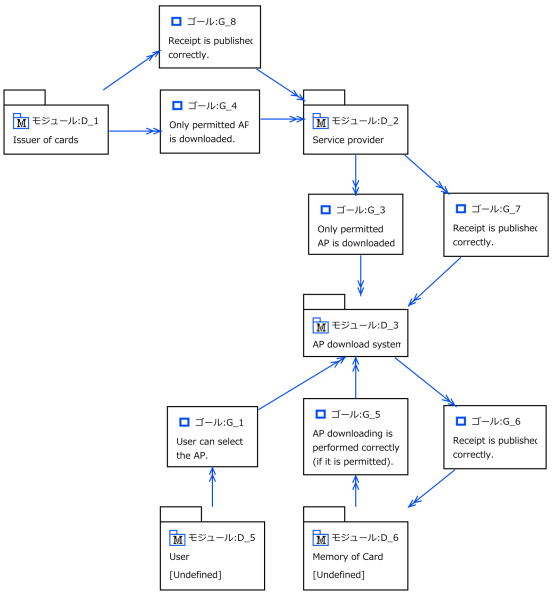

Fig. 3. Assurance case after Step 3.

6.2 dependability propagation

By the case study, it is understood that assurance case of d* can represent the dependability propagation that passes between actors. Commonly, some dependability information is propagating between actors. In the case study, dependability requirement ("Only permitted AP is downloaded") is propagating between "Issuer of cards", "Service provider", and "AP download system." Two dependability requirements have same sentence. But, evidences of requirement may be different between them. This difference should become clear by continuous arguments. Thus, dependability propagation can be considered by using an assurance case of d*. Previous assurance case notation like the GSN does not have this characteristic. This is a one of the strong point of d*.

6.3 Granularity of the actor

Deciding granularity of actor is one of the problems when creating assurance case by d*. Creating the assurance case from collaboration diagram is one of the solutions against this problem. Objects in collaboration diagram can be used directly to define actors in assurance case of d*. At this point, granularity of actor is decided. But, granularity may be not appropriate for actors in assurance case. Since, a purposes of creation is different between them. In the proposed creation procedure, granularity of actors is adjusted in Step 3.

6.4 Limitation of experiments

- Scale of case study was small. Therefore, the case study situation is different from concrete situation.
- In the case study, one researcher created the assurance case. Real developers did not create it. Therefore, the case study situation is different from concrete situation.
- Validity of assurance case is not clear.

7 Conclusion

In this paper, the assurance case creation procedure is proposed. The collaboration diagram is used in the procedure. Moreover, the case study is perfomed using this proposed procedure. As a result, effectiveness of proposed procedure was confirmed. That is, the collaboration diagram is useful, when the assurance case is created. In future works, an effectiveness of proposed procedure has to be confirmed in concrete situation.

Acknowledgments. This research is partially supported by JSPS Research Project Number:24220001.

References

1. Kelly, T.: Arguing Safety - A Systematic Approach to Managing Safety Cases. PhD thesis, University of York (1998)
2. Yamamoto, S. and Matsuno, Y.: d* framework: Inter-Dependency Model for Dependability. DSN 2012 (2012)
3. Avizienis, A., Laprie, J., Randell, B. and Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. Dependable and Secure Computing, vol.1, pp.11-33 (2004)
4. Adelard, http://www.adelard.com/web/hnav/ASCE/.
5. Despotou, G. and Kelly, T.: Extending the Safety Case Concept to Address Dependability. in Proceedings of the 22nd International System Safety Conference (2004)
6. Ankrum, T.S. and Krombolz, A. H.: Structured Assurance Cases: Three Common Standards. Slides presentation at the Association for Software Quality (ASQ) Section 509 meeting (2006)
7. Fenn, J., Hawkins, R., Williams, P. and Kelly, T.: Safety case composition using contracts - refinements based on feedback from an industrial case study. In Proceedings of 15th Safety Critical Systems Symposium (SSS'07), Springer (2007)
8. Despotou, G. and Kelly, T.: Dessign and Development of Dependability Case Architecture during System Development. in proceedings of the 25th International System Safety Conference (ISSC), Baltimore, USA (2007)
9. Bloomfield, R. and Bishop, P.: Safety and assurance cases: Past, present and possible future - an Adelard perspective. in proceedings of 18th Safety-Critical Systems Symposium (2010)
10. Yamamoto, S. and Matsuno, Y.: An Evaluation of Argument Patterns to Reduce Pitfalls of Applying Assurance Case. In proceedings of ASSURE2013, co-located ICSE2013, San Francisco, CA, USA (2013)