Chapter 77
A New Method for Writing Assurance Cases

Yutaka Matsuno
Nagoya University, Japan

Shuichiro Yamamoto
Nagoya University, Japan

ABSTRACT

In this paper, the authors present a new method for writing assurance cases. Assurance cases are documented bodies of evidence that provide a convincing and valid argument that a system is adequately dependable for a given application in a given environment. Assurance cases have been used mostly in the safety field, but are now beginning to be widely applied in other areas. Cyber security is one such area, and recently, assuring security of cyber systems has become crucial. Several methods and various guidelines for writing assurance cases have been used. Unfortunately, only experts are currently able to write assurance cases, and it is still difficult for ordinary engineers to write them. This paper presents a new method for writing assurance cases. The main ideas are that (1) documents generated and used during the system lifecycle must be either used by the assurance cases or must be referred to in the assurance cases, and (2) typical patterns exist for assurance cases, and these patterns have not yet been well discussed. This paper presents the preliminary steps in developing a method for writing assurance cases. The authors also report on a preliminary experiment carried out on a web server demo system.

1. INTRODUCTION

There have been growing concerns for cyber security as our daily lives now heavily depend on cyber systems, and numerous threats to those systems and our assets have been reported. For example, the Japan National Police Agency (National Police Agency, 2012) reported that the number of cyber criminals arrested in Japan during January through June in 2012 is 3268, an increase of 755 from the same period in 2011. The number of cyber security criminals arrested for offenses such as unauthorized access and falsification totals 338, an increase of 186 from the same period in 2011. Cyber systems interact with each other and involve a wider range of stakeholders. Also, threats to systems come from diverse threat agents, often in unexpected ways. Therefore, it is

DOI: 10.4018/978-1-4666-8473-7.ch077

important to *assure* stakeholders of the security of cyber systems to the greatest extent possible. In the *Build Security In* project (Build Security In, 2012) hosted by the U.S. Department of Homeland Security, software assurance is stated as one of the most important topics.

System assurance has become of great importance in many industry sectors too. Safety cases (assurance cases concerning the safety of systems) must be submitted to certification bodies when developing and operating safety-critical systems, e.g., those involving the automotive, railway, defense, nuclear plants, and off-shore petroleum industries (Howell, 2004). Several relevant standards, such as EUROCONTROL (Eurocontrol, 2006), the Rail Yellow Book, and MoD Defense Standard 00-56 (MoD, 2007), mandate the use of safety cases. Currently, assurance cases have been used mostly in the safety area; now, however, they are beginning to be used in various other areas, including the cyber security area.

There are several definitions of *assurance cases*. One such definition as follows:

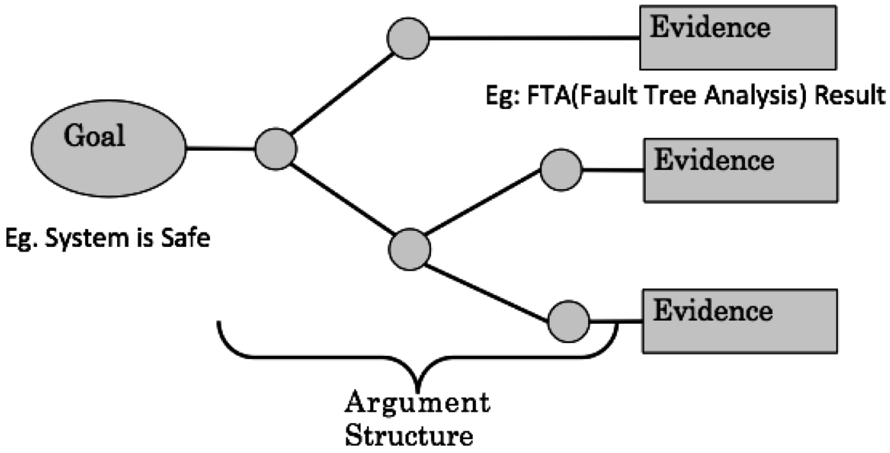
A documented body of evidence that provides a convincing and valid argument that a system is adequately dependable for a given application in a given environment. (Adelard).

An assurance case is called a safety case when arguing the safety of a system. Similarly, it is called a dependability case, security case, reliability case, or availability case when arguing the dependability, security, reliability, or availability of a system, respectively. The basic structure of assurance cases is shown in Figure 1 (slightly modified from the Figure in Bishop & Bloomfield, 1998).

As shown in Figure 1, an assurance case is often structured as a goal-based document. The top goal is a claim about one of the system's properties, such as dependability, safety, or security. The top goal is decomposed into sub-goals. Each piece of evidence is called a *leaf*, all of which ultimately support the top goal. The structure of decomposed goals is called an *argument structure*.

A recent report by The National Academies of the U.S.A. (Jackson, Thomas, & Millett, 2007) suggests the need for dependability cases based on broad surveys of recent serious incidents. Dependability has been considered an umbrella term that includes multiple attributes such as safety, reliability, availability, integrity, and maintainability. As quoted in (Lipson & Weinstock, 2008), the report said "The committee thus subscribes to the view that software is 'guilty until proven innocent,' and that the burden of proof falls on the developer to convince the certifier or regulator that the software

Figure 1. Basic structure of an assurance case


Evidence
Eg: FTA(Fault Tree Analysis) Result
Goal
Evidence
Eg. System is Safe
Evidence
Argument
Structure