Invited Talk: How the Fundamental Assurance Question Pervades Certification

Martin Feather
Jet Propulsion Laboratory, California Institute of Technology

Abstract

Assurance Cases are promoted as a means by which to present an argument for why a system is sufficiently dependable (alternate terms for the same concept include “Dependability Cases”, “Safety Cases” when the concern is safety, “Security Cases”, etc.). The purpose of such an argument is typically to inform a decision maker, often in the context of a key certification decision, so he/she will be better able to make that decision. Examples of such decisions include whether to deploy a system, whether to make an upgrade to an existing system, whether to advance a system to the next phase in its development. Assurance Cases are widely practiced in Europe, and are receiving growing attention in North America.

For software systems in particular, an assurance-case-based approach is often contrasted to a standards-based approach, the latter being characterized as more “prescriptive” in specifying the process and techniques to be applied to sufficiently assure software. The proponents of an assurance-case-based approach point out that the need to construct a sufficiently convincing Assurance Case puts the onus on the provider of the software to present the argument for its dependability, as compared to putting the onus on the regulator to have described in advance a sufficient process to be followed by the provider in their development of software. The distinction is not as clear-cut as it might at first seem. Both approaches have the need to assess by how much the outcomes of assurance activities (e.g., testing; code review; fault tree analysis; model-checking) raise confidence in decisions made about the system. For a standards-based approach, how is it possible to determine whether the required standard practice can be relaxed or waived entirely, when an alternate approach can be substituted, when additional activities are warranted? These determinations hinge on an understanding of the role of assurance activities, and the information conveyed by their outcome. These questions will arise more often and become more urgent to answer in the evolving world mentioned in the Call for Papers. For an assurance-case-based approach the outcome of an assurance activity will be evidence located within the assurance case, which makes it easier to see the role it plays in the overall assurance argument, but the same question arises – what is its information contribution to confidence?

Distilling these gives the “Fundamental Assurance Question,” namely how much do assurance activities contribute to raising decision confidence about system qualities, such as safety? These questions – and an intriguing start at answering them – will be the focus of this talk.

Speaker's Biography

Martin Feather is a principal in the Quality Assurance Office of the Jet Propulsion Laboratory, California Institute of Technology, where he has worked within the Software Assurance and Assurance Research group for the past 17 years. His work at JPL has focused on developing and infusing promising research ideas into practice. In recent years he has explored the use of Safety Cases for software systems, applied information visualization techniques to a variety of software assurance data, developed risk-based mission concept simulations to guide decisions, and participated in a study of "Roadmapping the California Smart Grid through Risk Retirement". He holds a Ph.D. in Artificial Intelligence from the University of Edinburgh, Scotland, UK.