Analysing Dependability Case Arguments Using Quality Models

Michaela Huhn and Axel Zechner
Institute for Software Systems Engineering
Technische Universität Braunschweig
Braunschweig, Germany
{m.huhn,a.zechner}@tu-braunschweig.de

Abstract. The Goal Structuring Notation (GSN) [1] facilitates a clear presentation of the argument structure in dependability cases for dependable systems. However, assessment of an argument structure with respect to validity, sufficiency and consistency of argumentation and the provided evidence still strongly depends on individual, tacit expert knowledge. We propose a 2-phase analysis method for argument structures:

Firstly, syntactic completeness, consistency, and proper instantiation of argument patterns are examined using a UML profile for GSN and OCL constraints. For the second phase, we propose 2-dimensional quality models to assist the expert in explicitly judging on the conclusiveness of argumentation. A quality model explicitly represents the impact of facts on design activities and software-system’s properties relevant for dependability. The impact value aggregates state-of-the-art knowledge and standard’s recommendations. Missing, negative or conflicting impact indicates impairment of the argument either by revealing a gap in the line of arguments or incompatibilities or opposing principles between decisions or techniques in the process. We show first steps towards the integration of the analysis into model-based tool supported development.

Keywords: Safety Case, Dependability Case, Argument structures, Argument Assessment, Quality models, Model-based development.

1 Introduction

Dependability, safety, trust, and other high assurance properties of a system are usually demonstrated in so-called dependability, assurance or safety cases. Citing Bishop and Bloomfield - a (safety) case is “a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment[2]. Assessing the line of arguments and the evidence provided in the dependability case is a task assigned to certification authorities by law (see e.g. EN50126 for the railway domain).

Dependability cases are provided by manufacturers and operating companies. They usually comprise large, complex argument structures on the development process, on system properties and environmental assumptions, and on operating procedures with multiple interdependencies and references to external documents.
containing facts backing the evidence. As a major step towards a clear presentation of arguments, Kelly proposed the Goal Structuring Notation (GSN) [1]. However, judging conclusiveness of the argument structure and strength of evidence needs structured methods (1) to make the expert’s assessment explicit and defensible and (2) to support communication on the findings to all stakeholders. As a preparatory step to argument assessment, we propose structural well-formedness checks: Modelling an argument structure within a UML profile for GSN enables automated exploration by using static analysis techniques. Thus, syntactic rules and proper instantiation of argument patterns can be analysed.

The focus of this paper is set on a method to assess the conclusiveness of argumentation. The underlying rationale is transferred from activity-based quality models for software characteristics [3,4] like maintainability or architecture evaluation: Relevant facts, characterising the system or its environment, development or operation, are appraised with regard to their effects on product-oriented activities undertaken to achieve and assure the requested system quality. An argument is confirmed, in case it is drawn upon activities positively supported by facts. Otherwise, the argument is marked as weak or even rebutted. We structure facts and activities in taxonomies adjusted to dependable systems. Fact and impact values reflect dependability-related aspects of the considered system. Thus, the method fosters systematic assessment of the following issues in the concrete system context: (1) Are the selected activities and techniques appropriate for their purposes and criticality level? (2) Is the portfolio of techniques sufficient and consistent? Does it conform to the relevant standards? (3) Have the selected activities the potential to constitute conclusive evidence for the dependability claims? If not, the causal entry in the quality model indicates a substantial reason for rejecting the argument and for improving the system or the case.

An indispensable further step is to appraise the evidence or external references of an argument structure. However, this part is not considered here.

2 Background

According to [5], dependability is an integrative concept composed of the attributes: “availability: readiness for correct service; reliability: continuity of correct service; safety: absence of catastrophic consequences on the user(s) and the environment; confidentiality: absence of unauthorized disclosure of information; integrity: absence of improper system state alterations; maintainability; ability to undergo repairs and modification. Such emergent system properties are usually demonstrated by argumentation in so-called dependability cases.

2.1 Goal Structuring Notation

The Goal Structuring Notation (GSN) by Kelly [1] is a widely accepted concept for concise, graphical presentation of safety cases (see Fig. 1). In principal, a

1 “Product-oriented” focusses on artifacts, deliverables and operational actions that directly concern the system, and is meant in opposite to a process-centric view.