An Artificial Science for System Value Engineering and Assurance

Michael Shell
School of Electrical and
Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30332–0250
Email: http://www.michaelshell.org/contact.html

Homer Simpson
Twentieth Century Fox
Springfield, USA
Email: homer@thesimpsons.com

James Kirk
and Montgomery Scott
Starfleet Academy
San Francisco, California 96678-2391
Telephone: (800) 555–1212
Fax: (888) 555–1212

***Abstract*—Research community of system quality attributes has been trying to define system qualities for a decade, but there is still no shared understanding for quality attributes, and yet we don't know how to assure them effectively. There are some theories and graphical tools like ACE and GSN, to help engineers to assure qualities in real projects. However, most graphical tools are not easy to scale. Besides, it's very hard to obtain feedback from engineers. Without the engineers' validation of such theories, it is very hard to evolve them if there are deficiencies exist. In this paper, we present a scientific theory and a framework for quality definition and assurance. We formalize a top-down taxonomy for quality attributes, and then integrates it with our previous work, a bottom-up formal language for quality requirements analysis, for quality attributes definition and assurance. Our theory uses the semantic formal language to parse the quality requirements to ilities, and provides evidence as the leafs of the top-down taxonomy. It then assures the the highest level quality by deductively reasoning the lower levels of qualities originally start from the leafs. We also present an illustration example by using this framework to conduct quality assurance analysis of a smart home project.**

I. Introduction

The value of system arises from a combination of many system qualities: from functionality and dependability to usability, flexibility, and others. Today our understanding of and ability to engineer system qualities is weak. There are no consensus definitions for many qualities. We have a poor understanding of means-ends relationships among qualities. We lack frameworks for reasoning about tradeoffs. Our ability to manage them across lifecycle is weak. These engineering problems are in turn rooted in weak science. Research in this area has often been informal and imprecise, with theories expressed in natural language, tables, graphics, and without the benefit of the kinds of mathematical, computational, and logical notations that are critical to producing clear, unambiguous, testable, generalized theories. Consequently we also lack foundations for automated tools for assisting with such issues, which are in turn a key to the dissemination, testing, validation, and eventual adoption and use of fundamental concepts of comprehensive quality requirements and engineering. We offer an approach that combines Bosch?s concept of innovation experiment systems with the use of rigorous formal specification and software synthesis using constructive logic proof assistant technology. We refine and express quality theories using the highly expressive language of the Coq proof assistant, which is capable of unified treatment of mathematical, computational, and logical concerns. We use synthesis from such specifications to support continuous deployment of web-based software implementations of the concepts embodied in such theories, and user-driven testing based on such tools to drive theory testing, evolution, and validation. Elements of the specific framework that we are constructing include a hierarchy of qualities and relationships parameterized by stakeholders, contexts, and system operational stages, based on recent work by Boehm; quality-specific specification languages for expressing detailed requirements (based on recent work by Ross and Rhodes); and a novel integration of the distinct, previously conflicting theories underlying these two efforts. We present our overall approach and illustrate its application with an example system for home automation. The overall contribution of this work is a novel, rigorous, and promising new approach to developing, promulgating, testing, evolving, and validating the scientific theory that is needed to underpin rigorous new approaches to comprehensive system quality engineering.

II. Related Work

Significant progress in these areas has been made for certain properties, particularly for system dependability properties, but not for others, such as flexibility, security, resilience, and many others. Yet the challenge in systems engineering is to produce value by achieving quality across broad ranges of system properties.

- Our overall approach is to create a scientific innovation experiment system to develop an integrated framework for quality definition, specification, realization, assurance
    - formal theory expressed using highly expressive language capable of unified treatment of mathematical, computational, and logical concerns that arise in relation to definition, specification, and assurances of diverse system qualities
    - continuous deployment supported by software synthesis from such expressions to create tools for concept dissemination, user-driven validation, and evolution

- Elements of the specific framework that we are constructing
    - hierarchies of qualities and relationships (Boehm)
    - languages for expressing specific requirements (e.g., Ross)
    - formalization of these preceding constructs
    - integrate diverse approaches to system qualities, e.g., Boehm?s top-down system quality taxonomy and Ross?s bottom-up semantic approach
    - reusable theories that can be instantiated for many projects (parameterization)

A. Shortcoming of Related Work

- Weak engineering foundations
    - No consensus definitions for many system properties
    - Weak understanding of means-ends relationships among system properties
    - Lack a framework for reasoning about tradeoffs among system qualities
    - Poor ability to manage full range of system qualities across system lifecycle
    - Fundamental weaknesses in our ability to handle system requirements
- Weak scientific foundations
    - Lack of rigor in research, notations, and methods employed in this area
        - Research in this area has been informal, qualitative, even sloppy
        - Theories are expressed informally: natural language, tables, graphics
        - No use of mathematical, computational, and logical notations critical to producing clear, unambiguous, testable theories
        - Weak basis for automation, a key to dissemination, testing, validation, and to adoption and evolution of basic concepts, method, and tools
        - Lack of rigorous and usable notations / languages for specifying the full range of system qualities that systems have to have
    - Weak understanding the nature of assurance, in particular in understanding the role and interpretation of evidence and the relationship between inductive and deductive reasoning in system quality assurance

III. Approach

- Our overall approach is to create a scientific innovation experiment system to develop an integrated framework for quality definition, specification, realization, assurance
    - formal theory expressed using highly expressive language capable of unified treatment of mathematical, computational, and logical concerns that arise in relation to definition, specification, and assurances of diverse system qualities
    - continuous deployment supported by software synthesis from such expressions to create tools for concept dissemination, user-driven validation, and evolution
- Elements of the specific framework that we are constructing
    - hierarchies of qualities and relationships (Boehm)
    - languages for expressing specific requirements (e.g., Ross)
    - formalization of these preceding constructs
    - integrate diverse approaches to system qualities, e.g., Boehm?s top-down system quality taxonomy and Ross?s bottom-up semantic approach
    - reusable theories that can be instantiated for many projects (parameterization)

IV. Evaluation

We also present an illustration example by using this framework to conduct quality assurance analysis of a smart home project.

V. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...