

How much

Formality for RE?

Outline

- Introduction
- Strengths of formal methods
- Weaknesses of formal methods
- Technical Expertise
- Conclusion

Introduction

Introduction 1 / 2

- Example
 - REQ1: The application calculates the number of days between two dates.
- Specification
 - Complete
 - Unambiguous
 - Consistent

Introduction 2 / 2

- Definition: Formal Methods
 - Techniques for modelling and verification of computer systems
- Techniques
 - Algebraic Specification
 - Z
 - OCL

Formal Methods and their

Strengths

Strengths

- Correctness and Reliability
- Provability
 - Consistency
 - Features
- Simulations possible

Formal Methods and their

Weaknesses

Weaknesses I

- Creation is difficult and time consuming
- Not readable without education
- Comprehensive specifications overstrain even professionals
- Supported model aspects limited (e.g. no UI)

Weaknesses II

- Proof of completeness is not simplified
- Proof of adequacy difficult (end-users cannot read the formal specification)
- Difficulties caused by lack of understanding are not eliminated
- Requirements change → formal specs. must be adopted

Technical Expertise

Historical Context of Formal Methods

- In former times, basic concepts applicable and sufficient for many domains →
- Universal methods arose out of immature fields of science
- Time changes: Domains become highly specialized
- Universal methods are only applicable to a certain degree

Historical Context continued

- Universal methods are replaced by formal micro-methods
- Micro-methods address problems of detail
- Focus changes from unrealistic simple complete systems to small parts or abstractions of real applications
- Security or a proof of certain functionality is now in scope

[Jackson 1998]

Formal Methods in RE I

- Formal methods can lead to cost savings
 - Creation of formal spec. is time consuming but
 - Improves the correctness of the specification
 - → Errors are detected earlier and can be avoided
 - Second time phenomenon
- For most software it is not worth the cost to apply formal methods
 - Verification is expensive (raise costs with factor 2-5)
 - Doing it twice is often cheaper

[Berry 2002]

Improve the Quality of the RS

- Main problems in RE arise from misunderstandings of the application domain
 - Not solved by formal methods
- Fundamental knowledge required
 - Ignoramus
- Introduce Competition
 - Developer vs. inspectors

Conclusion

- Applicable for critical components
 - Correctness of a specification is increased
 - Cost may be saved
-
- Formal methods do not find gaps in understanding
 - Further techniques required for a high quality requirements specification

...thanks for your Attention!