Softwaretechnik / Software-Engineering

Lecture 6: Requirements Engineering

2017-05-22

Prof. Dr. Andreas Podelski, Dr. Bernd Westphal

Albert-Ludwigs-Universität Freiburg, Germany

You Are Here.

<table>
<thead>
<tr>
<th>Course</th>
<th>L 1: 24.4, Mon</th>
<th>L 2: 27.4, Thu</th>
<th>T 1: 4.5, Thu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scales, Metrics</td>
<td></td>
<td>1.5, Mon</td>
<td></td>
</tr>
<tr>
<td>Costs, Development</td>
<td></td>
<td>8.5, Mon</td>
<td>11.5, Thu</td>
</tr>
<tr>
<td>Process</td>
<td></td>
<td>15.5, Mon</td>
<td></td>
</tr>
<tr>
<td>Requirements Engineering</td>
<td></td>
<td>18.5, Thu</td>
<td>22.5, Mon</td>
</tr>
<tr>
<td>-</td>
<td></td>
<td>25.5, Thu</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>29.5, Mon</td>
<td>16.5, Thu</td>
<td>5.6, Mon</td>
</tr>
<tr>
<td>T 2: 8.6, Thu</td>
<td></td>
<td>12.6, Mon</td>
<td></td>
</tr>
<tr>
<td>L 9: 19.6, Mon</td>
<td></td>
<td>22.6, Thu</td>
<td></td>
</tr>
<tr>
<td>Arch. &amp; Design</td>
<td>26.6, Mon</td>
<td>29.6, Thu</td>
<td></td>
</tr>
<tr>
<td>Software Modelling</td>
<td>L 12: 3.7, Mon</td>
<td>L 13: 6.7, Thu</td>
<td>L 14: 10.7, Mon</td>
</tr>
<tr>
<td>-</td>
<td>L 10: 3.7, Mon</td>
<td>L 15: 17.7, Mon</td>
<td></td>
</tr>
<tr>
<td>Patterns</td>
<td>L 18: 27.7, Thu</td>
<td></td>
<td></td>
</tr>
<tr>
<td>QA (Testing, Formal Verif.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wrap-Up</td>
<td>L 12: 22.7, Thu</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Recall: Structure of Topic Areas

Example: Requirements Engineering

<table>
<thead>
<tr>
<th>Vocabulary</th>
<th>e.g. consistent, complete, tacit, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Techniques</td>
<td></td>
</tr>
<tr>
<td>informal</td>
<td></td>
</tr>
<tr>
<td>semi-formal</td>
<td></td>
</tr>
<tr>
<td>formal</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

Vocabulary: Requirements (Analysis)
Usages of Requirements Specifications

Requirements Specification
Requirements Analysis
Desired Properties
Kinds of Requirements
Analysis Techniques

Documents
Dictionary
Specification

Requirements Specification Languages
Natural Language
**requirement**

1. A condition or capability needed by a user to solve a problem or achieve an objective.
2. A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents.
3. A documented representation of a condition or capability as in (1) or (2).

IEEE 610.12 (1990)

**requirements analysis**

1. The process of studying user needs to arrive at a definition of system, hardware, or software requirements.
2. The process of studying and refining system, hardware, or software requirements.

IEEE 610.12 (1990)

---

**Usages of the Requirements Specification**

- **negotiation**
  - (with customer, marketing department, or ...)

- **design and implementation.**
  - without specification, programmers may just “ask around” when in doubt, possibly yielding different interpretations → difficult integration

- **documentation.** e.g. the user’s manual,
  - without specification, the user's manual author can only describe what the system does, not what it should do (“every observation is a feature”)

- **preparation of tests.**
  - without a description of allowed outcomes, tests are randomly searching for generic errors (like crashes) → **systematic testing hardly possible**

- **acceptance** by customer,
  - resolving later objections or regress claims.
  - without specification, it is unclear at delivery time whether behaviour is an error (developer needs to fix or correct (customer needs to accept and pay) → nasty disputes, additional effort

- **re-use.**
  - without specification, re-use needs to be based on re-reading the code → risk of unexpected changes

- **later re-implementations.**
  - the new software may need to adhere to requirements of the old software; if not properly specified, the new software needs to be a 1:1 re-implementation of the old → additional effort
The hardest single part of building a software system is deciding precisely what to build.
No other part of the conceptual work is as difficult as establishing the detailed technical requirements ...
No other part of the work so cripples the resulting system if done wrong.
No other part is as difficult to rectify later.  

F.P. Brooks (Brooks, 1995)
Requirements Specifications

Requirements Analysis. . .

... in the sense of “finding out what the exact requirements are”.
"Analysing an existing requirements/feature specification” → later.

In the following we shall discuss:

(i) desired properties of

• requirements specifications,
• requirements specification documents.

(ii) kinds of requirements

• hard and soft,
• open and tacit,
• functional and non-functional.

(iii) (a selection of) analysis techniques

(iv) documents of the requirements analysis:

• dictionary,
• requirements specification (‘Lastenheft’),
• feature specification (‘Pflichtenheft’).

• Note: In the following (unless otherwise noted), we discuss the feature specification, i.e. the document on which the software development is based.
To maximise confusion, we may occasionally (inconsistently) call it requirements specification or just specification – should be clear from context...

• Recall: one and the same content can serve both purposes; only the title defines the purpose then.
A requirements specification should be

- **correct**
  - it correctly represents the wishes/needs of the customer.

- **complete**
  - all requirements (existing in somebody’s head, or a document, or …) should be present.

- **relevant**
  - things which are not relevant to the project should not be constrained.

- **consistent, free of contradictions**
  - each requirement is compatible with all other requirements; otherwise the requirements are not realisable.

- **neutral, abstract**
  - a requirements specification does not constrain the realisation more than necessary.

- **correct, complete**
  - things which are not relevant to the project should not be constrained.

- **traceable, comprehensible**
  - the sources of requirements are documented, requirements are uniquely identifiable.

- **testable, objective**
  - the final product can objectively be checked for satisfying a requirement.

**Correctness and completeness** are defined relative to something which is usually only in the customer’s head.

→ is is difficult to be sure of correctness and completeness.

"Dear customer, please tell me what is in your head!" is in almost all cases not a solution!

It’s not unusual that even the customer does not precisely know...!

For example, the customer may not be aware of contradictions due to technical limitations.

**Excursion: Informal vs. Formal Techniques**

<table>
<thead>
<tr>
<th>Example: Requirements Engineering, Airbag Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirement: Whenever a crash is detected, the airbag has to be fired within 300 ms (at).</td>
</tr>
<tr>
<td>- VS. Fix observables: crashed_detected ; Time → (0, 1) and fire_airbag ; Time → (0, 1)</td>
</tr>
<tr>
<td>- Formalise requirement: ∀ t, t' ∈ Time • crashed_detected(t) ∧ fire_airbag(t') → t' - t ≤ 300 - ε, t + 300 + δ</td>
</tr>
<tr>
<td>- no more misunderstandings, sometimes tools can objectively decide: requirement satisfied yes/no.</td>
</tr>
</tbody>
</table>

Requirements on Requirements Specifications
The representation and form of a requirements specification should be:

- **easily understandable,** not unnecessarily complicated — all affected people should be able to understand the requirements specification.
- **precise** — the requirements specification should not introduce new unclarities or rooms for interpretation (→ testable, objective).
- **easily maintainable** — creating and maintaining the requirements specification should be easy and should not need unnecessary effort.
- **easily usable** — storage of and access to the requirements specification should not need significant effort.

**Note:** Once again, it’s about compromises.

- A very precise objective requirements specification may not be easily understandable by every affected person. → provide redundant explanations.
- It is not trivial to have both, low maintenance effort and low access effort. → value low access effort higher, a requirements specification document is much more often read than changed or written (and most changes require reading beforehand).

**Pitfall: Vagueness vs. Abstraction**

Consider the following examples:

- **Vague** (not precise):
  “the list of participants should be sorted conveniently”

- **Precise, abstract**:
  “the list of participants should be sorted by immatriculation number, lowest number first”

- **Precise, non-abstract**:
  “the list of participants should be sorted by

  public static <T> void Collections::sort( List<T> list, Comparator c );

  where T is the type of participant records, c compares immatriculation number numerically.”

- A requirements specification should always be as precise as possible (→ testable, objective).
  It need not denote exactly one solution; precisely characterising acceptable solutions is often more appropriate.
- Being too specific, may limit the design decisions of the developers, which may cause unnecessary costs.

- Idealised views advocate a strict separation between requirements (“what is to be done?”) and design (“how are things to be done?”).
Kinds of Requirements
Kinds of Requirements: Functional and Non-Functional

- **Proposal**: View software $S$ as a function

$$S : i_1, i_2, i_3, \cdots \mapsto o_0, o_1, o_2, \ldots$$

which maps sequences of inputs to sequences of outputs.

**Examples:**
- Software "compute shipping costs":
  - $o_0$: initial state,
  - $i_1$: shipping parameters (weight, size, destination, ...),
  - $o_1$: shipping costs
  And no more inputs, $S : i_1 \mapsto o_1$.

- Software "traffic lights controller":
  - $o_0$: initial state,
  - $i_1$: pedestrian presses button,
  - $o_1, o_2, \ldots$: stop traffic, give green to pedestrians,
  - $i_n$: button pushed again
  - ...

- Every constraint on things which are observable in the sequences is a functional requirement (because it requires something for the function $S$).
  Thus timing, energy consumption, etc. may be subject to functional requirements.

- Clearly non-functional requirements:
  programming language, coding conventions, process model requirements, portability...

Kinds of Requirements: Hard and Soft Requirements

- **Example of a hard requirement**:
  - Cashing a cheque over $N \in$ must result in a new balance decreased by $N$; there is not a micro-cent of tolerance.

- **Examples of soft requirements**:
  - If a vending machine dispenses the selected item within 1s, it’s clearly fine; if it takes 5 min., it’s clearly wrong – where’s the boundary?
  - A car entertainment system which produces "noise" (due to limited bus bandwidth or CPU power) in average once per hour is acceptable, once per minute is not acceptable.

The border between hard/soft is difficult to draw, and

- **as developer**, we want requirements specifications to be "as hard as possible", i.e. we want a clear right/wrong.
- **as customer**, we often cannot provide this clarity; we know what is "clearly wrong" and we know what is "clearly right", but we don’t have a sharp boundary.

$\mapsto$ intervals, rates, etc. can serve as precise specifications of soft requirements.
Kinds of Requirements: Open and Tacit

- **open**: customer is aware of and able to explicitly communicate the requirement.

- **(semi-)tacit**: customer not aware of something being a requirement (obvious to the customer but not considered relevant by the customer, not known to be relevant).

Examples:

- buttons and screen of a mobile phone should be on the same side.
- important web-shop items should be on the right hand side because the main users are socialised with right-to-left reading direction.
- the ECU (embedded control unit) may only be allowed use a certain amount of bus capacity.

- distinguish **don’t care**: intentionally left open to be decided by developer.

---

![Table showing the distinction between customer/client and analyst](image)

**Content**

- **Introduction**
  - Vocabulary: Requirements (Analysis)
  - Usages of Requirements Specifications

- **Requirements Specification**
  - Requirements Analysis
  - Desired Properties
  - Kinds of Requirements
  - Analysis Techniques

- **Documents**
  - Dictionary
  - Specification

- **Requirements Specification Languages**
  - Natural Language
### (A Selection of) Analysis Techniques

<table>
<thead>
<tr>
<th>Analysis Technique</th>
<th>current situation</th>
<th>Focus desired situation</th>
<th>innovation consequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analysis of existing data and documents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Observation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Questioning with (closed structured open) questions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interview</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modelling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prototyping</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Participative development</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Ludewig and Lichter, 2013]
Observation:
Customers can not be assumed to be trained in stating/communicating requirements.

It is the task of the analyst to:
- ask what is wanted, ask what is not wanted,
- establish precision, look out for contradictions,
- anticipate exceptions, difficulties, corner-cases,
- have technical background to know technical difficulties,
- communicate (formal) specification to customer,
- “test” own understanding by asking more questions.

Goal: automate opening/closing of a main door with a new software.
A made up dialogue...

Analyst: So in the morning, you open the door at the main entrance?
Customer: Yes, as I told you.
A: Every morning?
C: Of course.
A: Also on the weekends?
C: No, on weekends, the entrance stays closed.
A: And during company holidays?
C: Then it also remains closed of course.
A: And if you are ill or on vacation?
C: Then Mr. M opens the door.
A: And if Mr. M is not available, too?
C: Then the first client will knock on the window.
A: Okay. Now what exactly does “morning” mean?

How Can Requirements Engineering Look In Practice?

- Set up a core team for analysis (3 to 4 people), include experts from the domain and developers. Analysis benefits from highest skills and strong experience.
- During analysis, talk to decision makers (managers), domain experts, and users. Users can be interviewed by a team of 2 analysts, ca. 90 min.
- The resulting “raw material” is sorted and assessed in half- or full-day workshops in a team of 6-10 people. Search for, e.g., contradictions between customer wishes, and for prioritisation.

Note: The customer decides. Analysts may make proposals (different options to choose from), but the customer chooses. (And the choice is documented.)

- The “raw material” is basis of a preliminary requirements specification (audience: the developers) with open questions.
Analysts need to communicate the requirements specification appropriately (explain, give examples, point out particular corner-cases).
Customers without strong maths/computer science background are often overstrained when “left alone” with a formal requirements specification.

Result: dictionary, specified requirements.

- Many customers do not want (radical) change, but improvement.
- Good questions: How are things done today? What should be improved?
Content

- Introduction
  - Vocabulary: Requirements (Analysis)
  - Usages of Requirements Specifications

- Requirements Specification
  - Requirements Analysis
  - Desired Properties
  - Kinds of Requirements
  - Analysis Techniques

- Documents
  - Dictionary
  - Specification

- Requirements Specification Languages
  - Natural Language

Requirements Documents
Requirements analysis should be based on a dictionary.

A dictionary comprises definitions and clarifications of terms that are relevant to the project and of which different people (in particular customer and developer) may have different understandings before agreeing on the dictionary.

Each entry in the dictionary should provide the following information:

- term and synonyms (in the sense of the requirements specification),
- meaning (definition, explanation),
- delimitations (where not to use this terms),
- validness (in time, in space, ...),
- denotation, unique identifiers, ....
- open questions not yet resolved,
- related terms, cross references.

Note: entries for terms that seemed "crystal clear" at first sight are not uncommon.

All work on requirements should, as far as possible, be done using terms from the dictionary consistently and consequently.

The dictionary should in particular be negotiated with the customer and used in communication (if not possible, at least developers should stick to dictionary terms).

Note: do not mix up real-world/domain terms with ones only “living” in the software.

Dictionary Example

Example: Wireless Fire Alarm System

During a project on designing a highly reliable, EN-54-25 conforming wireless communication protocol, we had to learn that the relevant components of a fire alarm system are

- terminal participants (heat/smoke sensors and manual indicators),
- repeaters (a non-terminal participant),
- and a central unit (not a participant).

Repeaters and central unit are technically very similar, but need to be distinguished to understand requirements. The dictionary explains these terms.

Excerpt from the dictionary (ca. 50 entries in total):

- **Part**: A part of a fire alarm system is either a **participant** or a **central unit**.
- **Repeater**: A repeater is a **participant** which accepts messages for the **central unit** from other **participants**, or messages from the **central unit** to other **participants**.
- **Central Unit**: A central unit is a **part** which receives messages from different assigned **participants**, assesses the messages, and reacts, e.g. by forwarding to persons or optical/acoustic signalling devices.
- **Terminal Participant**: A terminal participant is a **participant** which is not a **repeater**. Each terminal participant consists of exactly one wireless communication module and devices which provide sensor and/or signalling functionality.
**specification** – A document that specifies, in a complete, precise, verifiable manner, the requirements, design, behavior, or other characteristics of a system or component, and, often, the procedures for determining whether these provisions have been satisfied.

IEEE 610.12 (1990)

**software requirements specification (SRS)** – Documentation of the essential requirements (functions, performance, design constraints, and attributes) of the software and its external interfaces.

IEEE 610.12 (1990)
**Requirements Specification Languages**

**Specification language** – A language, often a machine-processible combination of natural and formal language, used to express the requirements, design, behavior, or other characteristics of a system or component.

For example, a design language or requirements specification language. Contrast with: programming language; query language. IEEE 610.12 (1990)

**Requirements specification language** – A specification language with special constructs and, sometimes, verification protocols, used to develop, analyze, and document hardware or software requirements. IEEE 610.12 (1990)
## Natural Language Specification

(Ludewig and Lichter, 2013) based on (Rupp and die SOPHISTen, 2009)

### Natural Language Patterns

Natural language requirements can be (tried to be) written as an instance of the pattern \[ \langle A \rangle \langle B \rangle \langle C \rangle \langle D \rangle \langle E \rangle \langle F \rangle \]. (German grammar) where

<table>
<thead>
<tr>
<th>rule</th>
<th>explanation, example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>R1</strong></td>
<td>State each requirement in active voice. Name the actors, indicate whether the user or the system does something. Not “the item is deleted”.</td>
</tr>
<tr>
<td><strong>R2</strong></td>
<td>Express processes by full verbs. Not “is”, “has”, but “reads”, “creates”; full verbs require information which describe the process more precisely. Not “when data is consistent” but “after program P has checked consistency of the data”.</td>
</tr>
<tr>
<td><strong>R3</strong></td>
<td>Discover incompletely defined verbs. In “the component raises an error”, ask whom the message is addressed to.</td>
</tr>
<tr>
<td><strong>R4</strong></td>
<td>Discover incomplete conditions. Conditions of the form “if-else” need descriptions of the if- and the then-case.</td>
</tr>
<tr>
<td><strong>R5</strong></td>
<td>Discover universal quantifiers. Are sentences with “never”, “always”, “each”, “any”, “all” really universally valid? Are “all” really all or are there exceptions.</td>
</tr>
<tr>
<td><strong>R6</strong></td>
<td>Check nominalisations. Nouns like “registration” often hide complex processes that need more detailed descriptions; the verb “register” raises appropriate questions: who, where, for what?</td>
</tr>
<tr>
<td><strong>R7</strong></td>
<td>Recognise and refine unclear substantives. Is the substantive used as a generic term or does it denote something specific? Is “user” generic or is a member of a specific classes meant?</td>
</tr>
<tr>
<td><strong>R8</strong></td>
<td>Clarify responsibilities. If the specification says that something is “possible”, “impossible”, or “may”, “should”, “must” happen, clarify who is enforcing or prohibiting the behaviour.</td>
</tr>
<tr>
<td><strong>R9</strong></td>
<td>Identify implicit assumptions. Terms (“the firewall”) that are not explained further often hint to implicit assumptions (here: there seems to be a firewall).</td>
</tr>
</tbody>
</table>

Example:

After office hours \((= A)\), the system \((= C)\) should \((= B)\) offer to the operator \((= D)\) a backup \((= F)\) of all new registrations to an external medium \((= E)\).
Tell Them What You’ve Told Them...

- Requirements Documents are important – e.g., for negotiation, design & implementation, documentation, testing, delivery, re-use, re-implementation.
- A Requirements Specification should be correct, complete, relevant, consistent, neutral, traceable, objective.
  Note: vague vs. abstract.
- Requirements Representations should be easily understandable, precise, easily maintainable, easily usable
- It is the task of the analyst to elicit requirements.
- Natural language is inherently imprecise, counter-measures:
  - natural language patterns.
  - Do not underestimate the value of a good dictionary.
References


