Universität Zürich
Institut für Informatik

Requirements Engineering II

Martin Glinz, Professor, Dr. rer. nat.

Assignment 4: Formal Requirements Specification

1. Tasks

- Read the mandatory items in the reading list
- Be prepared to answer the questions given below in class
- Prepare a 15 minutes presentation (5-10 slides) on the theme assigned to your course group. Browse/read additional papers and/or web pages where necessary.
- Specify the authentication subsystem of an ATM (automated teller machine) (a) in Z, (b) with a statechart, and (c) with a Petri net (predicate-transition net). Assume that you have two predicates, CardIsValid and CodeIsValid for determining whether the user's card and code are valid.

2. Reading list

Prerequisites

It is assumed that you are familiar with the basics of statecharts and Petri nets. You may want to refresh your knowledge by studying the slides on this topic in the course Informatik II (Part a: Modeling, Chapter 7 on 'Verhaltensmodelle' [Glinz 2005]). If you can't read German, read the sections on statecharts and Petri nets in a software engineering textbook.

Some basic knowledge of Z is also assumed. If you don't know Z yet, the mandatory reading of [Jacky 1997] (see below) will provide you an introduction from scratch. However, in this case reading will take more time.

Mandatory reading

Chapters 7 to 12.1 of [Jacky 1997] provide an introduction to the basic concepts of Z. [Glinz 2002] discusses the use of statecharts for requirements specification.

[Jackson 1998] and [Berry 2002] discuss general issues of using formal methods in software development; in particular in requirements engineering.

Mandatory browsing

Browse [Polak 1998], where a practical example of using formal methods in practice is reported. Answer the question given below.

Optional reading

[Parnas 1998] provides another viewpoint on the issue of using formal methods in software engineering. Chapter 15 of [Jacky 1997] describes formal reasoning in Z. [Spivey 1992] is a reference manual for Z. If you want to dig deeper into state-based formal requirements specification, read [Leveson et al. 1994] on RSML and [Heimdahl and Leveson 1996] on formal analysis of RSML.

3. Questions

- Why are formal requirements specification techniques not broadly used in practice? Is this just a technology transfer problem?
- What are the basic concepts of a set-based specification language such as Z?

- What can we learn from Berrry (2002) for requirements elicitation?
- In a given project, how do we decide how much formality we need for requirements specification?
- Why was automatic code generation from a formal requirements specification successful in the situation described in [Polak 1998]?
- What was your experience when specifying the same problem in Z, with a statechart, and with a Petri net?

4. Themes for presentation

(Will be assigned by the research assistant who tutors this course; your group can apply for the theme you would like to work on)

A. How much formality for requirements specification?

B. A comparison of set-based and state-based formal specification techniques

C. Z explained*

*The goal of this presentation is to illustrate the use of Z with examples. Use the case studies given in chapters 16 and 17 of [Jacky 1997] as a basis for this talk.

References

Berry, D.M. (2002). Formal Methods: The Very Idea. Some Thoughts About Why They Work When They Work. *Science of Computer Programming* **42** (1). 11-27

Glinz, M. (2002). Statecharts For Requirements Specification – As Simple As Possible, As Rich As Needed. *ICSE International Workshop on Scenarios and State Machines: Models, Algorithms and Tools*, Orlando, May 2002.

Glinz, M. (2005). Informatik II, Teil a: Modellierung (in German). Course notes, University of Zurich. Available at http://www.ifi.unizh.ch/req/courses/inf_II

Heimdahl, M.P.E. and Leveson, N.G. (1996). Completeness and Consistency in Hierarchical State-Based Requirements. *IEEE Transactions on Software Engineering* **22** (6). 363-377.

Jackson, M. (1998). Formal Methods and Traditional Engineering. *Journal of Systems and Software* **40** (3). 191-194.

Jacky, J. (1997). *The Way of Z: Practical Programming With Formal Methods*. New York: Cambridge University Press.

Leveson, N.G., Heimdahl, M.P.E., Hildreth, H., Reese, J.D. (1994). Requirements Specification for Process-Control Systems. *IEEE Transactions on Software Engineering* **20** (9). 684-707.

Parnas, D. L. (1998). “Formal Methods” Technology Transfer Will Fail. *Journal of Systems and Software* **40** (3). 195-198.

Polak, W. (2002). Formal Methods in Practice. *Science of Computer Programming* **42** (1). 75-85.

Spivey, J.M. (1992). *The Z Notation: A Reference Manual*. Second Edition. Hemel Hempstead: Prentice Hall International.

Web resources

- Zeta is a Z tool set: http://uebb.cs.tu-berlin.de/zeta/
- The Z user group maintains a web site at http://www.zuser.org/
- The Z virtual library contains numerous links to Z-related sites: http://vl.zuser.org/