

Formal Methods for Developing Reliable Software in Industry

Shigeru Otsuki,

Systems Development Laboratory, Hitachi, Ltd.

Developing reliable and high quality software is difficult, even if a lot of specification languages, models, and methods are proposed in academic field. Experience shows that some engineering techniques are useful and effective in applying theories for practical development projects.

Software engineering is the technical and managerial discipline concerned with developing and modifying computer software systems. The primary goal is to develop software products that : satisfy the requirements, user needs, and customer expectations; are developed on time and within budget; are easy to modify and maintain; instill pride in the developers. Software engineering should be based on science from the point of formal approach. However, general speaking, formal methods are difficult to use, have no methodology, and are not applicable to huge and complex systems either.

Each formal method is one of the candidates for silver bullets. We should elaborate the usage of formal methods. Introducing new technologies always causes some kind of paradigm shift of development process. It is important that each development project has well designed management plan which defines product, budget, schedule, documentation, tools, methods, and other managerial or technical issues. Phased approach is useful for introducing new technologies.

This course describes an overview of industrial strength formal methods, project management techniques, and educational issues. The course also includes experiences and case studies of using formal methods in developing products, Cleanroom development method, Z notation, Statecharts and so on. The tutorial will present empirical studies of the effectiveness of formal methods, and also propose the framework for the usage guidelines of these various techniques.

Shigeru Otsuki is a researcher of Systems Development Laboratory, Hitachi Ltd., in Japan, where he has developed methods and environments for real-time software system. Now, he is very interested in the field of technology transfer of software engineering. He is also a promoter of in-house education courses and consultant of project management. He started Cleanroom Method Working Group in IPJS-SIGSE from October, 1996. He is a member of the IEEE Computer Society, IPSJ, and JEIDA advanced software technology working group.