A Survey of Formal Methods in Software Development

The use of formal methods and formal techniques in industry is steadily growing. In this survey we shall characterise what we mean by software development and by a formal method; briefly overview a history of formal specification languages - some of which are: VDM (Vienna Development Method, 1974-..., [1]), Z (Z for Zermelo Fraenkel, 1980-..., [2]), RAISE (Rigorous Approach to Industrial Software Engineering, 1987-..., [3]) Event B (B for Bourbaki, 1990/2000-..., [4]) and Alloy [5]; and outline the basics of a formal development using, for example, RAISE: first developing a domain description D, then a requirements prescription R, and finally a software design S - showing (arguing or formally proving) that S, in the context of D satisfies (is correct with respect to) R. We shall then mention industries in Japan, Europe and USA which, in a number of projects, use formal methods; discuss what it takes for an industry to do so; discuss what education that candidates for these industries need, that is, which courses must be part of a BSc/MSc Software Engineering curriculum. Finally we shall comment on distinctions between formal methods and formal techniques; limitations of mono-language formalisations, hence need for multi-language formalisation (Petri Nets, MSC, StateChart, Temporal Logics); the sociology of university and industry acceptance of formal methods; the inevitability of the use of formal software development methods; while referring to seminal monographs and textbooks on formal methods.