Handling Safety Critical Requirements in System Engineering Using the B Formal Method

Didier Essamé

Siemens Transportation Systems.
50, rue Barbés. BP 531, 92542 Montrouge Cedex, France
Tel: 01 49 65 72 90
Didier.Essame@siemens.com

Overview

The IEEE standard "std 1220-1998" defines system engineering as a collaborative and an interdisciplinary approach to transform customer needs into a system solution. The fundamental system engineering objective is to provide high-quality products and services, with the correct people and performances features, at an affordable price, and on time. Building critical system involves stringent management of safety critical requirements. In particular, the engineering process must guarantee that resulting technical requirements do not jeopardize customer safety needs.

Introduced by Jean Raymond Abrial in 1998, "Event B" is an extension of the B formal method. Several studies and publications showed the significance of Event B for system level modelling and analysis. However, the approach still needed to be put to the test in an industrial context. Research at Siemens Transportation Systems (formerly MATRA Transport International) defined a methodology of use of Event B in system engineering based on the IEEE 1220 and EIA 632 standard that govern system engineering processes. These standards define a set of processes and activities and give recommendations about how to achieve systems studies. Since Event B has to improve system engineering work, it must:

- Be integrated in the existing system life cycle
- Respect the documentary chain that accompanies the system life cycle.

It must also be accessible to non-specialists and allow systematic practices.

Siemens Transportation Systems defined a set of activities concerning the main disciplines of system engineering where formalization and in particular the B-Method can be applied. This research resulted in two major processes of engineering namely:

- Transparent integration of the formal B-method in systems studies to meet safety critical customer requirements.
- Systematic formal system modelling to prove that resulting technical requirements do not jeopardize customer safety needs.

This talk presents the methodological elements for the application of these two processes in an industrial context with technical and economic constraints. I present a case study of a railway train protection system. I show how to analyse the conditions of the contract and formally derive system's specifications that respect customer safety needs.

M. Heisel et al. (Eds.): SAFECOMP 2004, LNCS 3219, p. 115, 2004.