Formal Modelling and Simulation of Train Control Systems Using Petri Nets

Michael Meyer zu Hörste[1] and Eckehard Schnieder[1]

Institut für Regelungs- und Automatisierungstechnik, Technische Universität
Braunschweig, Langer Kamp 8, D-38106 Braunschweig, Germany
{meyer|schnieder}@ifra.ing.tu-bs.de

Abstract. A formal model was prepared on behalf of the German railways (Deutsche Bahn AG) starting from an informal (natural language) specifications of the European Train Control System (ETCS) system. Proceeding from the existing models of the system design - the waterfall and the spiral model - a model for the system design was developed so as to use Petri nets as a universal means of description for all the phases of the ETCS. Following a thorough and detailed comparison, it was decided to use Petri nets as a means of description for this procedure, as they permit universal application, the use of different methods and formal analysis. The method developed is an integrated event- and data-oriented approach, which shows the different aspects of the system on their own net levels. The model comprises three sub-models with a model of the environment developed next to the onboard and trackside systems. This environment model covers all the additional systems connected through the system interfaces, examples of which are interlocking or regulation. Starting from a net representing the system context, the process of the onboard and trackside sub-systems was modelled. Here, the different operations and processes are visualized in the form of scenarios, which in turn have access to additional refinements representing specific functions. System modelling was supported by the tool Design/CPN. It was chosen after a careful evaluation of several Petri net tools. ETCS system modelling was taken to a point permitting partial model simulation. On the basis of these models, additional options of the spiral model of the system design now appear: the train and trackside models may expand into specific visualizations, the algorithms can be further refined and compared, the models can be used for different kinds of tests and also for purposes of system quality assurance, which may go as far as furnishing proof of safety standards. Additional phases of system development may now be elaborated on the basis of the spiral model. Our experience has shown that it is possible to take real-life and operational systems specifications written in a natural language and express their content as a formal specification. Our experience has also demonstrated that it is possible to incorporate real life practices of software development cycles (spiral model, waterfall model) into formal models. The paper makes an overview of our experiences and highlights the various problems which were encountered and solved.

References can be found at: `www.ifra.ing.tu−bs.de/∼m31/etcsrefs.html`

J. Wing, J. Woodcock, J. Davies (Eds.): FM'99, Vol. II, LNCS 1709, pp. 1867–1867, 1999.