Foundations of the Formal Sciences
Speaker : Heiko Mantel
May 9th, 9:30

Refinement in Formal Systems Engineering

The reliability of complex software systems is becoming increasingly important for technical systems. Malfunctioning of software may lead to loss or garbling of data, security risks, danger of life and limb, and, in almost all cases to severe economic losses.

The integration of formal methods into the engineering process allows one to guarantee properties of the resulting systems with mathematical rigour. The standard software engineering process is divided into different phases. Starting from abstract requirements, a system is developed in a stepwise manner. The system under development becomes more and more concrete during these phases until one ends up with a working system. In formal methods, this corresponds to the development of levels of specifications with an increasingly constructive contents.

Refinement is the theoretical basis for the migration from one level to a more concrete one.

We present different notions of refinement, discuss their properties, and their applications.