Refinement-Based Verification of Device-to-Device Information Flow

Ning Dong
KTH Royal Institute of Technology

Abstract: I/O devices are the critical components that allow a computing system to communicate with the external environment. From the perspective of a device, interactions can be divided into two parts, with the processor (mainly memory operations by the driver) and through the communication medium with external devices. In this paper, we present an abstract model of I/O devices and their drivers to describe the expected results of their execution, where the communication between devices is made explicit and the device-to-device information flow is analyzed. In order to handle general I/O functionalities, both half-duplex (transmission and reception) and full-duplex (sending and receiving simultaneously) data transmissions are considered. We propose a refinement-based approach that concretizes a correct-by-construction abstract model into an actual hardware device and its driver. As an example, we formalize the Serial Peripheral Interface (SPI) with a driver. In the HOL4 interactive theorem prover, we verified the observational equivalence of the concrete SPI model and the abstract model by establishing a weak bisimulation. We show how this result can be used to establish both functional correctness and information flow security for both single devices and when devices are connected in an end-to-end fashion.