

2.3 Exercises

1. Enumerate the essential requirements of a communication channel between two processes. Identify safety and security properties.
2. Assume that software for Automated Teller Machine (ATM) is to be constructed following the process model in Fig. 2.1. Answer the following questions:
 - What is the domain of application? Enumerate a few domain entities, the attributes for each entity, and the relationship among the entities. What properties of entities govern security? Develop a property to be verified in the software implementing the ATM.
 - Describe the environment for ATM to function. What constraints are to be imposed by the software on the environment? What constraints the environment may impose on the software?
 - What software components should be formalized? For each formal unit state the property to be verified in it.