Specification and Verification II

A simple device CP is informally specified as follows:

> CP stores values of type σ. It has two inputs: `inp` carries values of type σ and `func` carries 2-bit words; it has an output line `outp` carrying the value stored. CP is a state machine whose next state depends on the value input at `func`:
>
> - if `func`=0 the value stored is unchanged
> - if `func`=1 the value on `inp` replaces the value stored
> - if `func`=2 the value stored is transformed by a function $f_2 : \sigma \to \sigma$
> - if `func`=3 the value stored is transformed by a function $f_3 : \sigma \to \sigma$

Define a predicate CP that formalises this specification in higher order logic. [4 marks]

Write down logical models of the following components:

- a combinational multiplexer that routes one of four σ-valued inputs to a single output, depending on the value of a 2-bit control input; [3 marks]
- a unit-delay register that holds values of type σ. [3 marks]

Draw a schematic diagram of an implementation of CP built from these components. [3 marks]

Write down a formula that expresses the correctness of your implementation. [4 marks]

Discuss briefly how you would go about proving your correctness formula. You need not give a detailed proof, but you should aim to convince the reader that given time you could produce one. [3 marks]