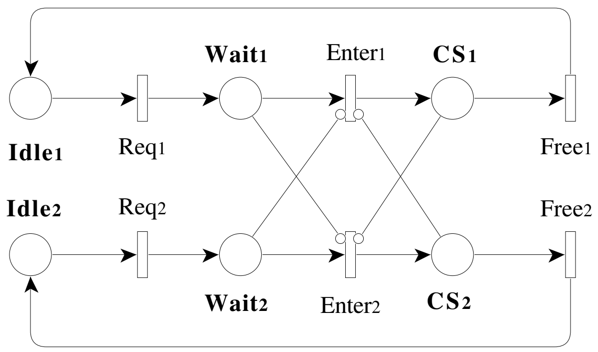

Figure 1.1: Mutual exclusion algorithm

P1 : The algorithm is deadlock free.

P2 : At each state, there is at most one process in critical section.

P3 : The algorithm is starvation free. Each process that asks for critical section will obtain it.

P4 : The entries in critical section are in the same order as requests.

These four properties can be expressed with a CTL or an LTL formula. They must be satisfied by each state of each execution. In the subsection 1.2.4 we present some differences between CTL and LTL.

When we consider Petri nets, the atomic propositions are conditions on the number of tokens in places. For example, the truth value of atomic proposition "$p \leq 2$" is true at each marking with at most two tokens in place p. As the number of tokens is positive, the atomic proposition "$p \geq 0$" is equivalent to the constant *true*. The structure to verify the formulas is the reachability graph of the model, the states are the markings and the possible paths, or executions, are the paths of the reachability graph. Each path begins with the initial marking of the Petri net.

Property P1 To express property P1 with a temporal logic formula, we first have to express that a marking is deadlock free. This is true if it enables at least one transition. This property involves no temporal operator.

Let $\mathcal{N} = \langle P, T, \mathbf{Pre}, \mathbf{Post}, \mathbf{Inh} \rangle$ be a Place/Transition Petri net with inhibitor arcs, a reachable marking $\mathbf{m}$ is deadlock free if and only if it satisfies the formula:

$$f_{deadlockfree}(\mathcal{N}) = \bigvee_{t \in T} \bigwedge_{p \in P} (p \geq \mathbf{Pre}[p,t] \wedge p < \mathbf{Inh}[p,t])$$

When we consider the Petri net of Figure 1.1 the formula $f_{deadlockfree}(\mathcal{N})$ is:

$$(Idle_1 \geq 1) \vee (Idle_2 \geq 1) \vee (CS_1 \geq 1) \vee (CS_2 \geq 1) \vee$$