

Proof of Condition 1

$Init \Rightarrow Inv$

1. $Init \Rightarrow TypeOK$

PROOF: By Init1.

2. $Init \Rightarrow MutualExclusion$

PROOF: By the definition of *MutualExclusion* and Init2, which implies $InCS(i)$ is false for both processes i .

3. $Init \Rightarrow \forall i \in \{0, 1\} : InCS(i) \vee (pc[i] = \text{“e2”}) \Rightarrow x[i]$

PROOF: By Init2, which implies $InCS(i)$ is false and $pc[i] \neq \text{“e2”}$, for each i . (Of course, we are using the fact that $FALSE \Rightarrow P$ is true for any formula P .)

4. Q.E.D.

PROOF: By steps 1–3 and the definition of *Inv*

CLOSE