MODULE *sys*1

EXTENDS *Integers*
CONSTANTS *UN*
VARIABLES x, y, pc

Define initial actions

$$al0l1 \triangleq \\ \land pc = \text{“l0”} \\ \land pc' = \text{“l1”} \\ \land x' = 0 \\ \land y' = 0$$

Define transition actions

$$al1l1 \triangleq \\ \land pc = \text{“l1”} \\ \land x \leq 5 \\ \land x' = x + 1 \\ \land y' = y \land pc' = pc$$

$$al1l2 \triangleq \\ \land pc = \text{“l1”} \\ \land pc' = \text{“l2”} \\ \land x' = x \ \land y' = y$$

$$al2l1 \triangleq \\ \land pc = \text{“l2”} \\ \land y < 50 \\ \land pc' = \text{“l1”} \\ \land x' = 0 \ \land y' = y + x$$

$$al2l3 \triangleq \\ \land pc = \text{“l2”} \\ \land y \geq 50 \\ \land pc' = \text{“l3”} \\ \land x' = x \ \land y' = y$$

$$al3l1 \triangleq \\ \land pc = \text{“l3”} \\ \land pc' = \text{“l1”} \\ \land x' = 0 \ \land y' = 0$$

Define the computation relation

$$next \triangleq al0l1 \lor al1l2 \lor al1l1 \lor al2l1 \lor al2l3 \lor al3l1 \lor \text{UNCHANGED } \langle x, y, pc \rangle$$

Define the initial conditions

$init \triangleq pc = \text{“l0”} \land x = UN \land y = UN$

Define the safety

$safety \triangleq$

$\land\ pc \neq \text{“l0”} \Rightarrow 0 \leq x \land x \leq 6$

$\land\ pc \neq \text{“l0”} \Rightarrow 0 \leq y \land y \leq 55$

---

* Modification History

* Last modified *Wed Jan* 24 08:57:45 *CET* 2018 by *mery*

* Created *Wed Sep* 09 17:02:47 *CEST* 2015 by *mery*