

```

|----- MODULE appex1_4 -----|
| modules de base importables |
| EXTENDS Naturals, Integers, TLC |
|-----|
| CONSTANTS x1, x2, U, MAX |
|  $MIN \triangleq -MAX$  |
|-----|
| VARIABLES y1, y2, y3, z1, z2, pc |
|-----|
|  $locs \triangleq \{\text{"START"}, \text{"HALT"}, \text{"LOOP"}\}$  |
|-----|
|  $BF(X) \triangleq X \neq U \Rightarrow X \in MIN .. MAX$  |
| ASSUME  $BF(x1) \wedge BF(x2)$  |
|-----|

|  $Init \triangleq pc = \text{"START"} \wedge y1 = U \wedge y2 = U \wedge y3 = U \wedge z1 = U \wedge z2 = U$  |
|-----|

|  $actionSTART\_LOOP \triangleq$  |
|    $\wedge pc = \text{"START"}$  |
|    $\wedge pc' = \text{"LOOP"}$  |
|    $\wedge y1' = 0$  |
|    $\wedge y2' = 0$  |
|    $\wedge y3' = x1$  |
|    $\wedge \text{UNCHANGED } \langle z1, z2 \rangle$  |

|  $actionLOOP\_HALT \triangleq$  |
|    $\wedge pc = \text{"LOOP"}$  |
|    $\wedge y3 = 0$  |
|    $\wedge pc' = \text{"HALT"}$  |
|    $\wedge y1' = y1$  |
|    $\wedge y2' = y2$  |
|    $\wedge y3' = y3$  |
|    $\wedge z1' = y1$  |
|    $\wedge z2' = y2$  |

|  $actionLOOP\_LOOP \triangleq$  |
|    $\wedge pc = \text{"LOOP"}$  |
|    $\wedge y3 \neq 0$  |
|    $\wedge pc' = pc$  |
|    $\wedge y1' = \text{IF } y2 + 1 = x2 \text{ THEN } y1 + 1 \text{ ELSE } y1$  |
|    $\wedge y2' = \text{IF } y2 + 1 = x2 \text{ THEN } 0 \text{ ELSE } y2 + 1$  |
|    $\wedge y3' = y3 - 1$ 

```

$$\begin{array}{l} \wedge \quad z1' = z1 \\ \wedge \quad z2' = z2 \end{array}$$

$$skip \triangleq \text{UNCHANGED } \langle y1, y2, y3, z1, z2, pc \rangle$$

$$\begin{array}{l} Next \triangleq \\ \quad \vee \text{ action } START_LOOP \\ \quad \vee \text{ action } LOOP_HALT \\ \quad \vee \text{ action } LOOP_LOOP \\ \quad \vee skip \end{array}$$

$$\begin{array}{l} \text{vérification du contrôle} \\ safety1 \triangleq pc \in locs \\ \text{correction partielle} \\ safety2 \triangleq pc = \text{"HALT"} \Rightarrow z1 = x1 \div x2 \wedge z2 = x1 \% x2 \wedge PrintT(z1) \wedge PrintT(z2) \\ safety3 \triangleq pc = \text{"HALT"} \Rightarrow \quad x1 = z1 * x2 + z2 \quad \wedge 0 \leq z2 \wedge z2 < x2 \\ safety4 \triangleq BF(z1) \wedge BF(z2) \wedge BF(y1) \wedge BF(y2) \wedge BF(y3) \\ tes \triangleq safety1 \wedge safety2 \wedge safety3 \wedge safety4 \\ Safety \triangleq safety1 \wedge safety2 \quad \wedge safety3 \quad \wedge safety4 \end{array}$$