453 The user's variable is binary b . The implementer's variables are natural x and y . The operations are:

$done \ = \ b:= x=y=0$

$step \ = \ \textbf{if } y>0 \textbf{ then } y:= y-1 \textbf{ else } x:= x-1.\ \textbf{new } n: nat\cdot y:= n \textbf{ fi}$

Replace the two implementer's variables x and y with a single new implementer's variable: natural z .

After trying the question, scroll down to the solution.

§ Use transformer $x{=}z \land y{=}0$. Then *done* becomes

$$\forall x, y\cdot\ x{=}z \land y{=}0 \ \Rightarrow\ \exists x', y'\cdot\ x'{=}z' \land y'{=}0 \ \land\ b' = (x{=}y{=}0) \land x'{=}x \land y'{=}y \qquad \text{one-pt } x, y$$
$$= \quad \exists x', y'\cdot\ x'{=}z' \land y'{=}0 \ \land\ b' = (z{=}0) \land x'{=}z \land y'{=}0 \qquad \text{one-pt } x', y'$$
$$= \quad b' = (z{=}0) \land z'{=}z$$
$$= \quad b{:=}\ z{=}0$$

and *step* becomes

$$\forall x, y\cdot\ x{=}z \land y{=}0 \ \Rightarrow\ \exists x', y'\cdot\ x'{=}z' \land y'{=}0 \ \land\ \mathbf{if}\ y{>}0\ \mathbf{then}\ y{:=}\ y{-}1\ \mathbf{else}\ x{:=}\ x{-}1.\ \ \mathbf{new}\ n{:}\ nat\cdot\ y{:=}\ n\ \mathbf{fi}$$
$$= \quad \forall x, y\cdot\ x{=}z \land y{=}0 \ \Rightarrow\ \exists x', y'\cdot\ x'{=}z' \land y'{=}0 \land (y{>}0 \Rightarrow x'{=}x \land y'{=}y{-}1) \land (y{=}0 \Rightarrow x'{=}x{-}1) \qquad \text{one-pt } x, y$$
$$= \quad \exists x', y'\cdot\ x'{=}z' \land y'{=}0 \land x'{=}z{-}1 \qquad \text{one-pt } x', y'$$
$$= \quad z'{=}z{-}1$$
$$\Leftarrow \quad z{:=}\ z{-}1$$

Or, use transformer $z = x{+}y$. Then *done* becomes

$$\forall x, y\cdot\ z = x{+}y \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \ \land\ b' = (x{=}y{=}0) \land x'{=}x \land y'{=}y \qquad \text{one-pt } x', y'$$
$$= \quad \forall x, y\cdot\ z = x{+}y \ \Rightarrow\ z' = x{+}y \ \land\ b' = (x{=}y{=}0) \qquad \text{since } x, y{:}\ nat\text{ , } (x{=}y{=}0) \text{ is the same as } (x{+}y{=}0)$$
$$= \quad \forall x, y\cdot\ z = x{+}y \ \Rightarrow\ z' = x{+}y \ \land\ b' = (x{+}y{=}0) \qquad \text{use context } z = x{+}y$$
$$= \quad \forall x, y\cdot\ z = x{+}y \ \Rightarrow\ z'{=}z \land b'{=}(z{=}0) \qquad \text{distributive law}$$
$$= \quad (\exists x, y\cdot\ z = x{+}y) \ \Rightarrow\ z'{=}z \land b'{=}(z{=}0) \qquad \text{lemma (below)}$$
$$= \quad z'{=}z \land b'{=}(z{=}0)$$
$$= \quad b{:=}\ z{=}0$$

The needed lemma, that every natural z is the sum of two naturals, is proved as follows:

$$\exists x, y\cdot\ z = x{+}y \qquad \text{generalization: for } x \text{ use } z \text{ and for } y \text{ use } 0$$
$$\Leftarrow \quad z = z{+}0 \qquad \text{identity}$$
$$= \quad \top$$

and *step* becomes

$$\forall x, y\cdot\ z = x{+}y \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \ \land\ \mathbf{if}\ y{>}0\ \mathbf{then}\ y{:=}\ y{-}1\ \mathbf{else}\ x{:=}\ x{-}1.\ \ \mathbf{new}\ n{:}\ nat\cdot\ y{:=}\ n\ \mathbf{fi}$$
$$= \quad \forall x, y\cdot\ z = x{+}y \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \land (y{>}0 \Rightarrow x'{=}x \land y'{=}y{-}1) \land (y{=}0 \Rightarrow x'{=}x{-}1) \qquad \text{splitting law}$$
$$\Leftarrow \quad (\forall x, y\cdot\ z = x{+}y \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \land (y{>}0 \Rightarrow x'{=}x \land y'{=}y{-}1)) \qquad \text{dist and port}$$
$$\land\ (\forall x, y\cdot\ z = x{+}y \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \land (y{=}0 \Rightarrow x'{=}x{-}1)) \qquad \text{distributive and portation}$$
$$= \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \land x'{=}x \land y'{=}y{-}1) \qquad \text{one-point}$$
$$\land\ (\forall x, y\cdot\ z = x{+}y \land y{=}0 \ \Rightarrow\ \exists x', y'\cdot\ z' = x'{+}y' \land x'{=}x{-}1) \qquad \text{one-point}$$
$$= \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ z' = x{+}y{-}1) \ \land\ (\forall x, y\cdot\ z = x{+}y \land y{=}0 \ \Rightarrow\ \exists y'\cdot\ z' = x{-}1{+}y')$$
$$= \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ z' = x{+}y{-}1) \ \land\ (\forall x, y\cdot\ z = x{+}y \land y{=}0 \ \Rightarrow\ z' \ge x{-}1)$$

For the right conjunct, use context $y{=}0$ to simplify $z = x{+}y$, and then one-point on x and y

$$= \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ z' = x{+}y{-}1) \ \land\ z' \ge z{-}1$$
$$\Leftarrow \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ z' = x{+}y{-}1) \ \land\ z' = z{-}1 \qquad \text{context}$$
$$= \quad (\forall x, y\cdot\ z = x{+}y \land y{>}0 \ \Rightarrow\ z{-}1 = x{+}y{-}1) \ \land\ z' = z{-}1 \qquad \text{arithmetic and specialize}$$
$$= \quad z' = z{-}1$$
$$\Leftarrow \quad z{:=}\ z{-}1$$

Or, taking a hint from Exercise 320, which is solved in Chapter 5, we could let $f{:}\ nat{\rightarrow}nat$ be an unknown function, let $s = \Sigma f\,[0;..x]$, and use transformer $z = x{+}y{+}s$.