Interaction

Interaction

shared variables

Interaction

shared variables

can be read and written by any process (most interaction)

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

difficult to reason about

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

difficult to reason about

interactive variables

can be read by any process, written by only one process (some interaction)

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

difficult to reason about

interactive variables

can be read by any process, written by only one process (some interaction)

easier to implement

easier to reason about

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

difficult to reason about

interactive variables

can be read by any process, written by only one process (some interaction)

easier to implement

easier to reason about

boundary variables

can be read and written by only one process (least interaction)

but initial value can be seen by all processes

Interaction

shared variables

can be read and written by any process (most interaction)

difficult to implement

difficult to reason about

interactive variables

can be read by any process, written by only one process (some interaction)

easier to implement

easier to reason about

boundary variables

can be read and written by only one process (least interaction)

but initial value can be seen by all processes

easiest to implement

easiest to reason about

Interactive Variables

boundary variable **new** a: $T\cdot S$

Interactive Variables

boundary variable $\quad$ **new** $a\colon T\cdot\ S \;=\; \exists a, a'\colon T\cdot\ S$

Interactive Variables

boundary variable	**new** a: T· S $=$ $\exists a, a'$: T· S
interactive variable	**new** x: $time \rightarrow T$· S

Interactive Variables

boundary variable $\quad \textbf{new}\ a{:}\ T\cdot\ S \ \ = \ \ \exists a, a'{:}\ T\cdot\ S$

interactive variable $\quad \textbf{new}\ x{:}\ \mathit{time}{\to}T\cdot\ S \ \ = \ \ \exists x{:}\ \mathit{time}{\to}T\cdot\ S$

Interactive Variables

boundary variable $\quad$ **new** $a: T\cdot\ S \ = \ \exists a, a': T\cdot\ S$

interactive variable $\quad$ **new** $x: time \to T\cdot\ S \ = \ \exists x: time \to T\cdot\ S$

The value of variable x at time t is $x\ t$

Interactive Variables

boundary variable $\quad \textbf{new}\ a{:}\ T\cdot\ S \ = \ \exists a, a'{:}\ T\cdot\ S$

interactive variable $\quad \textbf{new}\ x{:}\ time{\rightarrow}T\cdot\ S \ = \ \exists x{:}\ time{\rightarrow}T\cdot\ S$

The value of variable x at time t is $x\ t$

But sometimes we write x for $x\ t$, x' for $x\ t'$, x'' for $x\ t''$, ...

Interactive Variables

boundary variable $\textbf{new}\ a: T\cdot S \ = \ \exists a, a': T\cdot S$

interactive variable $\textbf{new}\ x: time\to T\cdot S \ = \ \exists x: time\to T\cdot S$

The value of variable x at time t is $x\ t$

But sometimes we write x for $x\ t$, x' for $x\ t'$, x'' for $x\ t''$, ...

$a:= a+x$

is really

$a:= a + x\ t$

Interactive Variables

boundary variable $\quad$ **new** $a{:}\ T\cdot\ S\ \ =\ \ \exists a, a'{:}\ T\cdot\ S$

interactive variable $\quad$ **new** $x{:}\ \mathit{time}\to T\cdot\ S\ \ =\ \ \exists x{:}\ \mathit{time}\to T\cdot\ S$

The value of variable x at time t is $x\ t$

But sometimes we write x for $x\ t$, x' for $x\ t'$, x'' for $x\ t''$, ...

$$a{:=}\ a{+}x$$

is really

$$a{:=}\ a + x\ t$$

Most laws still work but not the Substitution Law

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'=a \;\wedge\; b'=b \;\wedge\; t'=t$

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'=a \;\wedge\; b'=b \;\wedge\; t'=t$

$x'=x \;\wedge\; y'=y$ means $x\,t' = x\,t \;\wedge\; y\,t' = y\,t$

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$$ok \quad = \quad a'=a \ \land \ b'=b \ \land \ t'=t$$

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$$ok \quad = \quad a'=a \;\wedge\; b'=b \;\wedge\; t'=t$$

$$a{:=}\,e \quad = \quad a'=e \;\wedge\; b'=b \;\wedge\; t'=t$$

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$$ok \;=\; a'=a \;\land\; b'=b \;\land\; t'=t$$

$$a{:=}\,e \;=\; a'=e \;\land\; b'=b \;\land\; t'=t$$

$$x{:=}\,e \;=\; a'=a \;\land\; b'=b \;\land\; x'=e \;\land\; (\forall t''\cdot\, t\le t''\le t' \Rightarrow y''=y)$$
$$\land\;\; t' = t+(\text{the time required to evaluate and store } e\,)$$

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'{=}a \;\wedge\; b'{=}b \;\wedge\; t'{=}t$

$a{:=}\, e \quad = \quad a'{=}e \;\wedge\; b'{=}b \;\wedge\; t'{=}t$

$x{:=}\, e \quad = \quad a'{=}a \;\wedge\; b'{=}b \;\wedge\; x'{=}e \;\wedge\; (\forall t''\cdot\, t{\le}t''{\le}t' \Rightarrow y''{=}y)$

$\wedge\;\; t' = t+(\text{the time required to evaluate and store } e\ )$ ←

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'=a \ \land \ b'=b \ \land \ t'=t$

$a{:=}\ e \quad = \quad a'=e \ \land \ b'=b \ \land \ t'=t$

$x{:=}\ e \quad = \quad a'=a \ \land \ b'=b \ \land \ x'=e \ \land \ (\forall t''\cdot\ t\le t''\le t' \Rightarrow y''=y)$ ←

$\land \ \ t' = t+$(the time required to evaluate and store e)

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'{=}a \;\land\; b'{=}b \;\land\; t'{=}t$

$a{:=}\, e \quad = \quad a'{=}e \;\land\; b'{=}b \;\land\; t'{=}t$

$x{:=}\, e \quad = \quad a'{=}a \;\land\; b'{=}b \;\land\; x'{=}e \;\land\; (\forall t''\cdot\, t{\le}t''{\le}t' \Rightarrow y''{=}y)$

$\land\;\; t' = t+$(the time required to evaluate and store e)

$P.\,Q \quad = \quad \exists a'', b'', t''\cdot$ (substitute a'', b'', t'' for a', b', t' in P)

$\land$ (substitute a'', b'', t'' for a, b, t in Q)

Interactive Variables

suppose boundary a , b ; interactive x , y ; time t

$ok \quad = \quad a'=a \;\land\; b'=b \;\land\; t'=t$

$a{:=}\,e \quad = \quad a'=e \;\land\; b'=b \;\land\; t'=t$

$x{:=}\,e \quad = \quad a'=a \;\land\; b'=b \;\land\; x'=e \;\land\; (\forall t''\cdot\ t\le t''\le t' \Rightarrow y''=y)$

$\qquad\qquad \land\;\; t' = t+$(the time required to evaluate and store e)

$P.\,Q \quad = \quad \exists a'', b'', t''\cdot$ (substitute a'', b'', t'' for a', b', t' in P)

$\qquad\qquad\qquad \land$ (substitute a'', b'', t'' for a, b, t in Q)

$P\|Q \quad = \quad \exists t_P, t_Q\cdot$ (substitute t_P for t' in P)

$\qquad\qquad \land$ (substitute t_Q for t' in Q)

$\qquad\qquad \land\;\; t' = t_P\uparrow t_Q$

$\qquad\qquad \land\;\; (\forall t''\cdot\ t_P\le t''\le t' \Rightarrow x\ t''=x(t_P))$ interactive variables of P

$\qquad\qquad \land\;\; (\forall t''\cdot\ t_Q\le t''\le t' \Rightarrow y\ t''=y(t_Q))$ interactive variables of Q

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y)\ \|\ (y{:=}\ 3.\ \ y{:=}\ x{+}y)$$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \,\|\, (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(\underline{x{:=}\ 2}.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$=\quad (a'{=}a \wedge x\,t'{=}2 \wedge t'{=}t{+}1\,.$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ \underline{x{:=}\ x{+}y}.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \land x\ t'{=}2 \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1.$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ \underline{x{:=}\ x{+}y})\ \|\ (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad x$ left, y right, a left, b right

$= \quad (a'{=}a \wedge x\ t'{=}2 \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (\underline{y{:=}\ 3}.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \land x\ t'{=}2 \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1)$

$\parallel\ (b'{=}b \land y\ t'{=}3 \land t'{=}t{+}1.$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \,\|\, (y{:=}\ 3.\ \ \underline{y{:=}\ x{+}y})$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \wedge x\ t'{=}2 \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

$\|\ (b'{=}b \wedge y\ t'{=}3 \wedge t'{=}t{+}1.\ \ b'{=}b \wedge y\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y) \qquad x \text{ left},\ y \text{ right},\ a \text{ left},\ b \text{ right}$$

$$= \quad (a'{=}a \land x\ t'{=}2 \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1)$$

$$\parallel\ (b'{=}b \land y\ t'{=}3 \land t'{=}t{+}1.\ \ b'{=}b \land y\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1)$$

$$= \quad (a'{=}a \land x(t{+}1){=}2 \land x(t{+}2){=}x(t{+}1){+}y(t{+}1) \land x(t{+}3){=}x(t{+}2){+}y(t{+}2) \land t'{=}t{+}3)$$

$$\parallel\ (b'{=}b \land y(t{+}1){=}3 \land y(t{+}2){=}x(t{+}1){+}y(t{+}1) \land t'{=}t{+}2)$$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \land x\ t'{=}2 \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1.\ \ a'{=}a \land x\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1)$

$\parallel (b'{=}b \land y\ t'{=}3 \land t'{=}t{+}1.\ \ b'{=}b \land y\ t'{=}x\ t{+}y\ t \land t'{=}t{+}1)$

$= \quad (a'{=}a \land x(t{+}1){=}2 \land x(t{+}2){=}x(t{+}1){+}y(t{+}1) \land x(t{+}3){=}x(t{+}2){+}y(t{+}2) \land t'{=}t{+}3)$

$\parallel (b'{=}b \land y(t{+}1){=}3 \land y(t{+}2){=}x(t{+}1){+}y(t{+}1) \land t'{=}t{+}2)$

$= \quad x(t{+}1){=}2 \land x(t{+}2){=}x(t{+}1){+}y(t{+}1) \land x(t{+}3){=}x(t{+}2){+}y(t{+}2)$

$\land\ y(t{+}1){=}3 \land y(t{+}2){=}x(t{+}1){+}y(t{+}1) \land y(t{+}3){=}y(t{+}2)$

$\land\ a'{=}a \land b'{=}b \land t'{=}t{+}3$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \wedge x\ t'{=}2 \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

$\parallel (b'{=}b \wedge y\ t'{=}3 \wedge t'{=}t{+}1.\ \ b'{=}b \wedge y\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

$= \quad (a'{=}a \wedge x(t{+}1){=}2 \wedge x(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge x(t{+}3){=}x(t{+}2){+}y(t{+}2) \wedge t'{=}t{+}3)$

$\parallel (b'{=}b \wedge y(t{+}1){=}3 \wedge y(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge t'{=}t{+}2)$

$= \quad x(t{+}1){=}2 \wedge x(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge x(t{+}3){=}x(t{+}2){+}y(t{+}2)$

$\wedge\ y(t{+}1){=}3 \wedge y(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge y(t{+}3){=}y(t{+}2)$ $\quad \longleftarrow$

$\wedge\ a'{=}a \wedge b'{=}b \wedge t'{=}t{+}3$

Interactive Variables

example boundary a , b ; interactive x , y ; extended natural time t

$(x{:=}\ 2.\ \ x{:=}\ x{+}y.\ \ x{:=}\ x{+}y) \parallel (y{:=}\ 3.\ \ y{:=}\ x{+}y)$ $\qquad$ x left, y right, a left, b right

$= \quad (a'{=}a \wedge x\ t'{=}2 \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1.\ \ a'{=}a \wedge x\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

$\parallel (b'{=}b \wedge y\ t'{=}3 \wedge t'{=}t{+}1.\ \ b'{=}b \wedge y\ t'{=}x\ t{+}y\ t \wedge t'{=}t{+}1)$

$= \quad (a'{=}a \wedge x(t{+}1){=}2 \wedge x(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge x(t{+}3){=}x(t{+}2){+}y(t{+}2) \wedge t'{=}t{+}3)$

$\parallel (b'{=}b \wedge y(t{+}1){=}3 \wedge y(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge t'{=}t{+}2)$

$= \quad x(t{+}1){=}2 \wedge x(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge x(t{+}3){=}x(t{+}2){+}y(t{+}2)$

$\wedge\ y(t{+}1){=}3 \wedge y(t{+}2){=}x(t{+}1){+}y(t{+}1) \wedge y(t{+}3){=}y(t{+}2)$

$\wedge\ a'{=}a \wedge b'{=}b \wedge t'{=}t{+}3$

$= \quad x(t{+}1){=}2 \wedge x(t{+}2){=}5 \wedge x(t{+}3){=}10 \wedge y(t{+}1){=}3 \wedge y(t{+}2){=}y(t{+}3){=}5 \wedge a'{=}a \wedge b'{=}b \wedge t'{=}t{+}3$

Thermostat

Thermostat

$thermometer \parallel control \parallel thermostat \parallel burner$

Thermostat

$$thermometer \parallel control \parallel thermostat \parallel burner$$

inputs to the thermostat:

- real *temperature* , which comes from the thermometer and indicates the actual temperature.
- real *desired* , which comes from the control and indicates the desired temperature.
- binary *flame* , which comes from a flame sensor in the burner and indicates whether there is a flame.

Thermostat

$thermometer \parallel control \parallel thermostat \parallel burner$

inputs to the thermostat:

- real $temperature$, which comes from the thermometer and indicates the actual temperature.
- real $desired$, which comes from the control and indicates the desired temperature.
- binary $flame$, which comes from a flame sensor in the burner and indicates whether there is a flame.

outputs of the thermostat:

- binary gas ; assigning it $\top$ turns the gas on and $\bot$ turns the gas off.
- binary $spark$; assigning it $\top$ causes sparks for the purpose of igniting the gas.

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$thermostat \;=\; (gas{:=}\bot \parallel spark{:=}\bot).\; GasOff$

$GasOff \;=\; \mathbf{if}\; temperature < desired - \varepsilon$

$\quad\mathbf{then}\; (gas{:=}\top \parallel spark{:=}\top \parallel t' \ge t{+}1) \;\land\; t' \le t{+}3.\; spark{:=}\bot.\; GasOn$

$\quad\mathbf{else}\; ((\mathbf{frame}\; gas, spark\cdot\, ok) \parallel t'{\ge}t) \;\land\; t' \le t{+}1.\; GasOff\; \mathbf{fi}$

$GasOn \;=\; \mathbf{if}\; temperature < desired + \varepsilon \;\land\; flame$

$\quad\mathbf{then}\; ((\mathbf{frame}\; gas, spark\cdot\, ok) \parallel t'{\ge}t) \;\land\; t' \le t{+}1.\; GasOn$

$\quad\mathbf{else}\; (gas{:=}\bot \parallel (\mathbf{frame}\; spark\cdot\, ok) \parallel t' \ge t{+}20) \;\land\; t' \le t{+}21.\; GasOff\; \mathbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

↓ ↓

$$\mathit{thermostat} \;=\; (\mathit{gas}{:=}\, \bot \,\|\, \mathit{spark}{:=}\, \bot).\;\; \mathit{GasOff}$$

$$\begin{aligned}
\mathit{GasOff} \;=\;\; & \textbf{if } \mathit{temperature} < \mathit{desired} - \varepsilon \\
& \textbf{then } (\mathit{gas}{:=}\, \top \,\|\, \mathit{spark}{:=}\, \top \,\|\, t' \ge t{+}1) \;\wedge\; t' \le t{+}3.\;\; \mathit{spark}{:=}\, \bot.\;\; \mathit{GasOn} \\
& \textbf{else } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; \mathit{GasOff} \textbf{ fi}
\end{aligned}$$

$$\begin{aligned}
\mathit{GasOn} \;=\;\; & \textbf{if } \mathit{temperature} < \mathit{desired} + \varepsilon \;\wedge\; \mathit{flame} \\
& \textbf{then } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; \mathit{GasOn} \\
& \textbf{else } (\mathit{gas}{:=}\, \bot \,\|\, (\textbf{frame } \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t' \ge t{+}20) \;\wedge\; t' \le t{+}21.\;\; \mathit{GasOff} \textbf{ fi}
\end{aligned}$$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$thermostat \;=\; (gas{:=}\bot \parallel spark{:=}\bot).\; GasOff$

$GasOff \;=\; \textbf{if}\ temperature < desired - \varepsilon$ ←

$\qquad \textbf{then}\ (gas{:=}\top \parallel spark{:=}\top \parallel t' \ge t+1) \;\land\; t' \le t+3.\; spark{:=}\bot.\; GasOn$

$\qquad \textbf{else}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \parallel t'{\ge}t) \;\land\; t' \le t+1.\; GasOff\ \textbf{fi}$

$GasOn \;=\; \textbf{if}\ temperature < desired + \varepsilon \;\land\; flame$

$\qquad \textbf{then}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \parallel t'{\ge}t) \;\land\; t' \le t+1.\; GasOn$

$\qquad \textbf{else}\ (gas{:=}\bot \parallel (\textbf{frame}\ spark\cdot\ ok) \parallel t' \ge t+20) \;\land\; t' \le t+21.\; GasOff\ \textbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that when the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$\mathit{thermostat} \;=\; (\mathit{gas}{:=}\,\bot \,\|\, \mathit{spark}{:=}\,\bot).\;\; \mathit{GasOff}$

$\mathit{GasOff} \;=\; \textbf{if } \mathit{temperature} < \mathit{desired} - \varepsilon$

$\longrightarrow$ $\textbf{then } (\mathit{gas}{:=}\,\top \,\|\, \mathit{spark}{:=}\,\top \,\|\, t' \ge t{+}1) \;\wedge\; t' \le t{+}3.\;\; \mathit{spark}{:=}\,\bot.\;\; \mathit{GasOn}$

$\textbf{else } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; \mathit{GasOff}\ \textbf{fi}$

$\mathit{GasOn} \;=\; \textbf{if } \mathit{temperature} < \mathit{desired} + \varepsilon \;\wedge\; \mathit{flame}$

$\textbf{then } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; \mathit{GasOn}$

$\textbf{else } (\mathit{gas}{:=}\,\bot \,\|\, (\textbf{frame } \mathit{spark}\cdot\, \mathit{ok}) \,\|\, t' \ge t{+}20) \;\wedge\; t' \le t{+}21.\;\; \mathit{GasOff}\ \textbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$thermostat \;=\; (gas{:=}\, \bot \,\|\, spark{:=}\, \bot).\; GasOff$

$GasOff \;=\; \textbf{if}\ temperature < desired - \varepsilon$

$\qquad \textbf{then}\ (gas{:=}\, \top \,\|\, spark{:=}\, \top \,\|\, t' \ge t{+}1) \;\wedge\; t' \le t{+}3.\; spark{:=}\, \bot.\; GasOn$

$\qquad \textbf{else}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\; GasOff\ \textbf{fi}$

$GasOn \;=\; \textbf{if}\ temperature < desired + \varepsilon \;\wedge\; flame$ ←

$\qquad \textbf{then}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\; GasOn$

$\qquad \textbf{else}\ (gas{:=}\, \bot \,\|\, (\textbf{frame}\ spark\cdot\ ok) \,\|\, t' \ge t{+}20) \;\wedge\; t' \le t{+}21.\; GasOff\ \textbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that when the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$thermostat \;=\; (gas{:=}\,\bot \,\|\, spark{:=}\,\bot).\;\; GasOff$

$GasOff \;=\;$ $\textbf{if}\ temperature < desired - \varepsilon$

$\quad\textbf{then}\ (gas{:=}\,\top \,\|\, spark{:=}\,\top \,\|\, t' \ge t{+}1) \;\wedge\; t' \le t{+}3.\;\; spark{:=}\,\bot.\;\; GasOn$

$\quad\textbf{else}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; GasOff\ \textbf{fi}$

$GasOn \;=\;$ $\textbf{if}\ temperature < desired + \varepsilon \;\wedge\; flame$

$\longrightarrow\ \textbf{then}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \,\|\, t'{\ge}t) \;\wedge\; t' \le t{+}1.\;\; GasOn$

$\quad\textbf{else}\ (gas{:=}\,\bot \,\|\, (\textbf{frame}\ spark\cdot\ ok) \,\|\, t' \ge t{+}20) \;\wedge\; t' \le t{+}21.\;\; GasOff\ \textbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$thermostat \;=\; (gas{:=}\ \bot \parallel spark{:=}\ \bot).\ \ GasOff$

$GasOff \;=\; \textbf{if}\ temperature < desired - \varepsilon \qquad \longleftarrow$

$\qquad \textbf{then}\ (gas{:=}\ \top \parallel spark{:=}\ \top \parallel t' \ge t+1)\ \land\ t' \le t+3.\ \ spark{:=}\ \bot.\ \ GasOn$

$\qquad \textbf{else}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \parallel t' \ge t)\ \land\ t' \le t+1.\ \ GasOff\ \textbf{fi}$

$GasOn \;=\; \textbf{if}\ temperature < desired + \varepsilon\ \land\ flame$

$\qquad \textbf{then}\ ((\textbf{frame}\ gas, spark\cdot\ ok) \parallel t' \ge t)\ \land\ t' \le t+1.\ \ GasOn$

$\qquad \textbf{else}\ (gas{:=}\ \bot \parallel (\textbf{frame}\ spark\cdot\ ok) \parallel t' \ge t+20)\ \land\ t' \le t+21.\ \ GasOff\ \textbf{fi}$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$$\mathit{thermostat} \;=\; (\mathit{gas}{:=}\,\bot \parallel \mathit{spark}{:=}\,\bot).\;\; \mathit{GasOff}$$

$$\begin{aligned}
\mathit{GasOff} \;=\;\; & \textbf{if } \mathit{temperature} < \mathit{desired} - \varepsilon \\
& \textbf{then } (\mathit{gas}{:=}\,\top \parallel \mathit{spark}{:=}\,\top \parallel t' \ge t{+}1) \;\land\; t' \le t{+}3.\;\; \mathit{spark}{:=}\,\bot.\;\; \mathit{GasOn} \\
\longrightarrow\; & \textbf{else } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \;\land\; t' \le t{+}1.\;\; \mathit{GasOff}\ \textbf{fi}
\end{aligned}$$

$$\begin{aligned}
\mathit{GasOn} \;=\;\; & \textbf{if } \mathit{temperature} < \mathit{desired} + \varepsilon \;\land\; \mathit{flame} \\
& \textbf{then } ((\textbf{frame } \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \;\land\; t' \le t{+}1.\;\; \mathit{GasOn} \\
& \textbf{else } (\mathit{gas}{:=}\,\bot \parallel (\textbf{frame } \mathit{spark}\cdot\ \mathit{ok}) \parallel t' \ge t{+}20) \;\land\; t' \le t{+}21.\;\; \mathit{GasOff}\ \textbf{fi}
\end{aligned}$$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$$\mathit{thermostat} \;=\; (\mathit{gas}{:=}\bot \parallel \mathit{spark}{:=}\bot).\ \mathit{GasOff}$$

$$\begin{aligned}\mathit{GasOff} \;=\;\; & \mathbf{if}\ \mathit{temperature} < \mathit{desired} - \varepsilon \\ & \mathbf{then}\ (\mathit{gas}{:=}\top \parallel \mathit{spark}{:=}\top \parallel t' \ge t{+}1) \;\wedge\; t' \le t{+}3.\ \mathit{spark}{:=}\bot.\ \mathit{GasOn} \\ & \mathbf{else}\ ((\mathbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \;\wedge\; t' \le t{+}1.\ \mathit{GasOff}\ \mathbf{fi}\end{aligned}$$

$$\begin{aligned}\mathit{GasOn} \;=\;\; & \mathbf{if}\ \mathit{temperature} < \mathit{desired} + \varepsilon \;\wedge\; \mathit{flame} \quad \longleftarrow \\ & \mathbf{then}\ ((\mathbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \;\wedge\; t' \le t{+}1.\ \mathit{GasOn} \\ & \mathbf{else}\ (\mathit{gas}{:=}\bot \parallel (\mathbf{frame}\ \mathit{spark}\cdot\ \mathit{ok}) \parallel t' \ge t{+}20) \;\wedge\; t' \le t{+}21.\ \mathit{GasOff}\ \mathbf{fi}\end{aligned}$$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$$\mathit{thermostat} \;=\; (\mathit{gas}{:=}\,\bot \parallel \mathit{spark}{:=}\,\bot).\ \mathit{GasOff}$$

$$\begin{aligned}
\mathit{GasOff} \;=\;\; & \mathbf{if}\ \mathit{temperature} < \mathit{desired} - \varepsilon \\
& \mathbf{then}\ (\mathit{gas}{:=}\,\top \parallel \mathit{spark}{:=}\,\top \parallel t' \ge t{+}1) \ \wedge\ t' \le t{+}3.\ \mathit{spark}{:=}\,\bot.\ \mathit{GasOn} \\
& \mathbf{else}\ ((\mathbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \ \wedge\ t' \le t{+}1.\ \mathit{GasOff}\ \mathbf{fi}
\end{aligned}$$

$$\begin{aligned}
\mathit{GasOn} \;=\;\; & \mathbf{if}\ \mathit{temperature} < \mathit{desired} + \varepsilon \ \wedge\ \mathit{flame} \\
& \mathbf{then}\ ((\mathbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \parallel t'{\ge}t) \ \wedge\ t' \le t{+}1.\ \mathit{GasOn} \\
\longrightarrow\ & \mathbf{else}\ (\mathit{gas}{:=}\,\bot \parallel (\mathbf{frame}\ \mathit{spark}\cdot\ \mathit{ok}) \parallel t' \ge t{+}20) \ \wedge\ t' \le t{+}21.\ \mathit{GasOff}\ \mathbf{fi}
\end{aligned}$$

Heat is wanted when the actual temperature falls ε below the desired temperature, and not wanted when the actual temperature rises ε above the desired temperature, where ε is small enough to be unnoticeable, but large enough to prevent rapid oscillation. To obtain heat, the spark should be applied to the gas for at least 1 second to give it a chance to ignite and to allow the flame to become stable. But a safety regulation states that the gas must not remain on and unlit for more than 3 seconds. Another regulation says that when the gas is shut off, it must not be turned on again for at least 20 seconds to allow any accumulated gas to clear. And finally, the gas burner must respond to its inputs within 1 second.

$$\mathit{thermostat} \;=\; (\mathit{gas}:=\bot \;\|\; \mathit{spark}:=\bot).\;\; \mathit{GasOff}$$

$$\mathit{GasOff} \;=\; \textbf{if}\ \mathit{temperature} < \mathit{desired} - \varepsilon$$

$$\textbf{then}\ (\mathit{gas}:=\top \;\|\; \mathit{spark}:=\top \;\|\; t' \ge t+1) \;\land\; t' \le t+3.\;\; \mathit{spark}:=\bot.\;\; \mathit{GasOn}$$

$$\textbf{else}\ ((\textbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \;\|\; t'\ge t) \;\land\; t' \le t+1.\;\; \mathit{GasOff}\ \textbf{fi}$$

$$\mathit{GasOn} \;=\; \textbf{if}\ \mathit{temperature} < \mathit{desired} + \varepsilon \;\land\; \mathit{flame}$$

$$\textbf{then}\ ((\textbf{frame}\ \mathit{gas}, \mathit{spark}\cdot\ \mathit{ok}) \;\|\; t'\ge t) \;\land\; t' \le t+1.\;\; \mathit{GasOn}$$

$$\textbf{else}\ (\mathit{gas}:=\bot \;\|\; (\textbf{frame}\ \mathit{spark}\cdot\ \mathit{ok}) \;\|\; t' \ge t+20) \;\land\; t' \le t+21.\;\; \mathit{GasOff}\ \textbf{fi}$$