$State ::= init \mid norm \mid broken \mid stop$

$OnOff ::= on \mid off$

$OpenClosed ::= open \mid closed$

Physical Constants

$$
\begin{array}{|l}
w_{min} : \mathbb{N} \\
w_{max} : \mathbb{N} \\
l : \mathbb{N} \\
d_{max} : \mathbb{N} \\
\delta_p : \mathbb{N} \\
\delta_d : \mathbb{N} \\
\hline
w_{min} < w_{max} \\
\end{array}
$$

Measured values

$$
\begin{array}{|l}
\hline
Input \\
\hline
w? : \mathbb{N} \\
d? : \mathbb{N} \\
\hline
\end{array}
$$

Control values

$$
\begin{array}{|l}
\hline
Pumps \\
\hline
p_1, p_2, p_3, p_4 : OnOff \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
SteamBoiler0 \\
\hline
Pumps \\
v : OpenClosed \\
a : OnOff \\
z : State \\
\hline
\end{array}
$$

Auxiliary Schemata

$$
\begin{array}{|l}
\hline
PumpsOff \\
\hline
Pumps' \\
\hline
p_1' = off \land p_2' = off \land p_3' = off \land p_4' = off \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
PumpsOn \\
\hline
Pumps' \\
\hline
p_1' = on \land p_2' = on \land p_3' = on \land p_4' = on \\
\hline
\end{array}
$$

Steam Boiler Initial State

*SteamBoilerInit*0

$$SteamBoiler0'$$

$$a' = off$$
$$z' = init$$

Operations for Initialisation

*SInitNormal*0

$$\Delta SteamBoiler0$$
$$Input$$

$$z = init$$
$$d? = 0$$
$$w? \geq w_{min} + d_{max}$$
$$w? \leq w_{max}$$
$$PumpsOff$$
$$z' = norm$$
$$v' = closed$$
$$a' = on$$

*SInitStop*0

$$\Delta SteamBoiler0$$
$$Input$$

$$z = init$$
$$d? > 0$$
$$z' = stop$$

*SInitFill*0

$$\Delta SteamBoiler0$$
$$Input$$

$$z = init$$
$$d? = 0$$
$$w? < w_{min} + d_{max}$$
$$PumpsOn$$
$$z' = z$$
$$v' = closed$$
$$a' = off$$

*SInitEmpty*0

$\Delta SteamBoiler0$
Input

$z = init$
$d? = 0$
$w? > w_{max}$
PumpsOff
$z' = z$
$v' = open$
$a' = off$

$ControlInit0 \mathrel{\widehat=} SInitNormal0$
$\lor\ SInitStop0$
$\lor\ SInitFill0$
$\lor\ SInitEmpty0$

Operations for Normal State

*SNormalFill*0

$\Delta SteamBoiler0$
Input

$z = norm$
$w?? \geq w_{min}$
$w? \leq w_{opt} - 3l$
PumpsOn
$v' = closed \land a' = on \land z' = z$

Note: Simplified version where all four pumps are swicthed on simultaneously.

*SNormalContinue*0

$\Xi SteamBoiler0$
Input

$z = norm$
$w? > w_{opt} - 3l$
$w? \leq w_{opt}$

*SNormalNotFill*0

$\Delta SteamBoiler0$
Input

$z = norm$
$w? > w_{opt}$
$w? \leq w_{max}$
PumpsOff
$v' = closed \land a' = on \land z' = z$

*SNormalStop*0

$\Delta SteamBoiler0$
Input

$z = norm$
$w? < w_{min} \lor w? > w_{max}$
$a' = off \land z' = stop$

$ControlNormal0 \mathrel{\widehat=} SNormalFill0$
$\lor\ SNormalContinue0$
$\lor\ SNormalNotFill0$
$\lor\ SNormalStop0$

$Control0 \mathrel{\widehat=} ControlInit0$
$\lor\ ControlNormal0$

Extended Solution
Additional Type

$WorksBroken ::= works \mid broken$

Additional measured values

ControlInput

$k_w? : WorksBroken$
$k_d? : WorksBroken$
$k_{p1}? : WorksBroken$
$k_{p2}? : WorksBroken$
$k_{p3}? : WorksBroken$
$k_{p4}? : WorksBroken$

Control values

*SteamBoiler*1

*SteamBoiler*0
$s : \mathbb{N}$
$\delta : \mathbb{N}$

Initial State

*SteamBoilerInit*1

$$SteamBoiler1'$$

$$a' = off$$
$$z' = init$$

Auxiliary Functions

$$pswitch : (OnOff \times WorksBroken) \rightarrow OnOff$$

$$pswitch(on, works) = on$$
$$pswitch(on, broken) = off$$
$$pswitch(off, works) = off$$
$$pswitch(off, broken) = off$$

$$pamount : (OnOff \times WorksBroken) \rightarrow \mathbb{N}$$

$$\forall x : OnOff, y : WorksBroken \mid x = off \lor y = broken \bullet$$
$$pamount(x, y) = 0$$
$$pamount(on, works) = 1$$

Auxilary Schemata

PumpsControlledOn

$$Pumps'$$
$$ControlInput$$

$$p_1' = pswitch(on, k_{p1}?) \land p_2' = pswitch(on, k_{p2}?)$$
$$p_2' = pswitch(on, k_{p3}?) \land p_4' = pswitch(on, k_{p4}?)$$

PumpsControlledOff

$$Pumps'$$
$$ControlInput$$

$$p_1' = pswitch(off, k_{p1}?) \land p_2' = pswitch(off, k_{p2}?)$$
$$p_2' = pswitch(off, k_{p3}?) \land p_4' = pswitch(off, k_{p4}?)$$

Operations for Initialisation

*SInitNormal*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = init$
$d? = 0$
$k_w = works \land k_d = works$
$w? \geq w_{min} + d_{max}$
$w? \leq w_{max}$
$z' = norm$
$v' = closed$
$a' = on$
$s' = w?$
PumpsOff

*SInitFill*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = init$
$d? = 0 k_w = works \land k_d = works$
$w? < w_{min} + d_{max}$
$z' = z$
$v' = closed$
$a' = off$
PumpsOn

*SInitEmpty*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = init$
$d? = 0$
$w? > w_{max}$
$z' = z$
$v' = open$
$a' = off$
PumpsOff

*SInitStop*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = init$
$d? > 0 \lor K_w = broken \lor k_d = broken$
$z' = stop$

$ControlInit1 \mathrel{\widehat=} SInitNormal1$
$\lor\ SInitFill1$
$\lor\ SInitEmpty1$
$\lor\ SInitStop1$

Operations for Normal State

*SNormalFill*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = norm$
$k_w = works$
$w? \geq w_{min}$
$w? \leq w_{opt} = 3l$
$s' = w?$
PumpsControlledOn
$v' = closed \land a' = on \land z' = z$

*SNormalContinue*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = norm$
$k_w = works$
$w? > w_{opt} - 3l$
$w? \leq w_{opt}$
$p_1' = pswitch(p_1, k_{p1}) \land p_2' = pswitch(p_2, k_{p2})$
$p_3' = pswitch(p_3, k_{p3}) \land p_4' = pswitch(p_4, k_{p4})$
$s' = w?$
$v' = v \land a' = a \land z' = z$

*SNormalNotFill*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = norm$
$k_w = works$
$w? > w_{opt}$
$w? \leq w_{max}$
$s' = w?$
PumpsControlledOff
$v' = closed \land a' = on \land z' = z$

*SNormalWaterStop*1

$\Delta SteamBoiler$
Input
ControlInput

$z = norm \lor z = broken$
$k_w = works$
$w? < w_{min} \lor w? > w_{max}$
$a' = off \land z' = stop$

*SNormalControlStop*1

$\Delta SteamBoiler1$
Input
ControlInput

$z = norm$
$k_w = broken \land k_d = broken$
$a' = off \land z' = stop$

AmountComputation

$SteamBoiler1$
ControlInput
$amount : \mathbb{N}$
$\delta_{pumps} : \mathbb{N}$

$amount = l * (pamount(p_1, k_{p1}?) + pamount(p_2, k_{p2}?) +$
$pamount(p_3, k_{p3}?) + pamount(p_4, k_{p4}?))$
$\delta_{pumps} = \delta_p * (pamount(p_1, works) + (pamount(p_2,$
$works) + (pamount(p_3, works) + (pamount(p_4, works))$

*SNormalBroken*1

$\Delta SteamBoiler1$
$Input$
$ControlInput$
$AmountComputation$

$= norm$
$k_w = broken$
$k_d = works$
$s' = s + amount - d?$
$\delta' = \delta_{pumps} + \delta_d$
$s' \geq w_{min} + \delta'$
$s' \leq w_{max} - \delta' aas' < (w_{min} + w_{max})/2 \rightarrow PumpsControlledOn$
$s' \geq (w_{min} + w_{max})/2 \rightarrow PumpsControlledOff$
$v' = closed \wedge a' = on$
$z' = broken$

Complete Operation

$ControlNormal1 \mathrel{\widehat{=}} SnormalFill1$
$\vee\ SNormalContinue1$
$\vee\ SNormalNotFill1$
$\vee\ SNormalWaterStop1$
$\vee\ SNormalControlStop1$
$\vee\ SNormalBroken1$

Operations for Broken State

*sBrokenContinue*1

$\Delta SteamBoiler1$
$Input$
$ControlInput$
$AmountComputation$

$z = broken$
$k_w = broken$
$k_d = works$
$s' = s + amount - d?$
$\delta' = \delta + \delta_{pumps} + \delta_d$
$s' \geq w_{min} + \delta'$
$s' \leq w_{max} - \delta'$
$s' < (w_{min} + w + max)/2 \rightarrow PumpsControlledOn$
$s' \geq (w_{min} + w_{max})/2 \rightarrow PumpsControlledOff$
$v' = closed \wedge a' = on$
$z' = broken$

*SBrokenNormal*1

$\Delta SteamBoiler1$
Input
ControlInput
AmountComputation

$z = broken$
$k_w = works$
$w? \geq w_{min}$
$w? \leq w_{max}$
$w? < (w_{min} + w_{max})/2 \rightarrow PumpsControlledOn$
$w? \geq (w_{min} + w_{max})/2 \rightarrow PumpsControlledOff$
$s' = w?$
$v' = closed \land a' = on$
$z' = norm$

*SBrokenControlStop*1

$\Delta SteamBoiler1$
Input
ControlInput

$= broken$
$k_w = broken$
$k_d = broken$
$a' = off \land z' = stop$

SBrokenWaterStop

$\Delta SteamBoiler1$
Input
ControlInput
AmountComputation

$z = broken \lor z = norm$
$k_w = broken$
$k_d works$
$s' = s + amount - d?$
$z = broken \rightarrow \delta' = \delta + \delta_{pumps} + \delta_d$
$z = norm \rightarrow \delta' = \delta + pumps + \delta_d$
$s' < w_{min} + \delta' \lor s' > w_{max} - d'$
$a' = off \land z' = stop$

$ControlBroken1 \mathrel{\widehat=} SBrokenContinue1$
$\lor SBrokenNormal1$
$\lor SBrokenControlStop1$
$\lor SBrokenWaterStop$