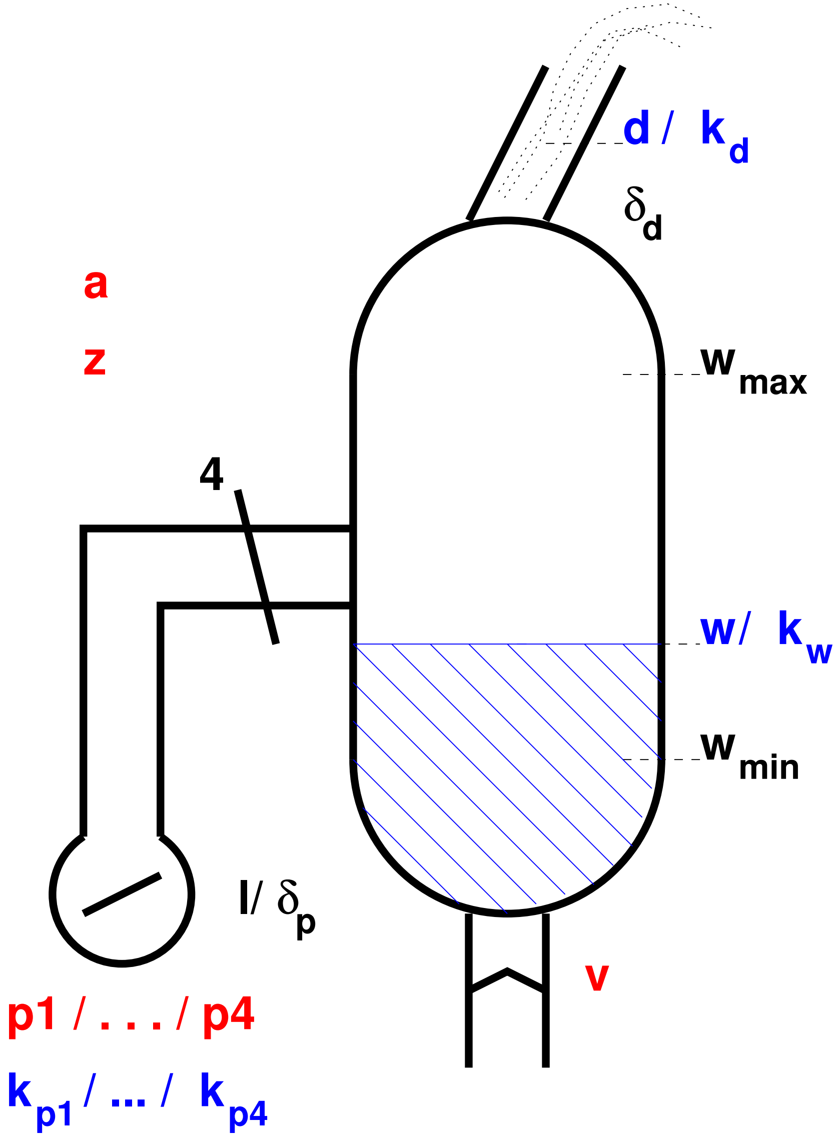
Formal Specification of Software

Steam Boiler Control
An Example in Z Formalisation

Bernhard Beckert

UNIVERSITÄT KOBLENZ-LANDAU

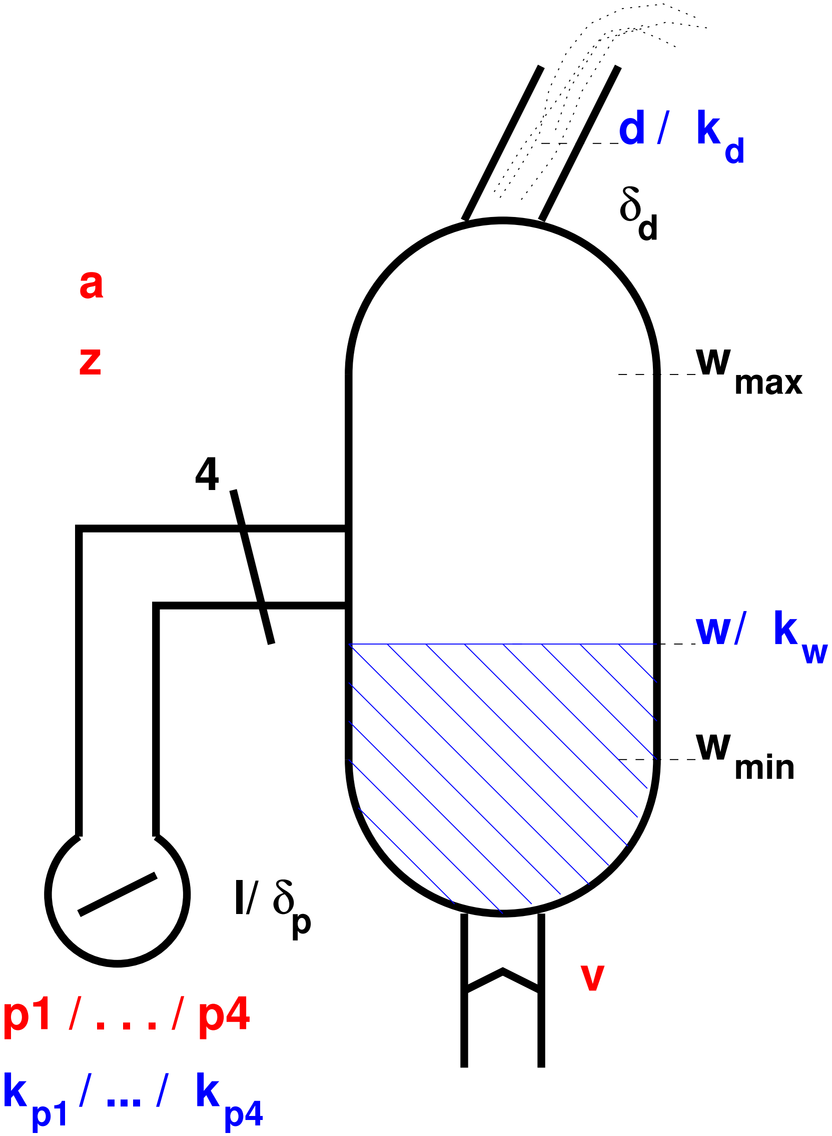
Steam Boiler Control: Scenario



System Components

- steam boiler
- water level measuring device
- four pumps
- four pump controlers
- steam quantity measuring device
- valve for emptying the boiler

Steam Boiler Control: Scenario

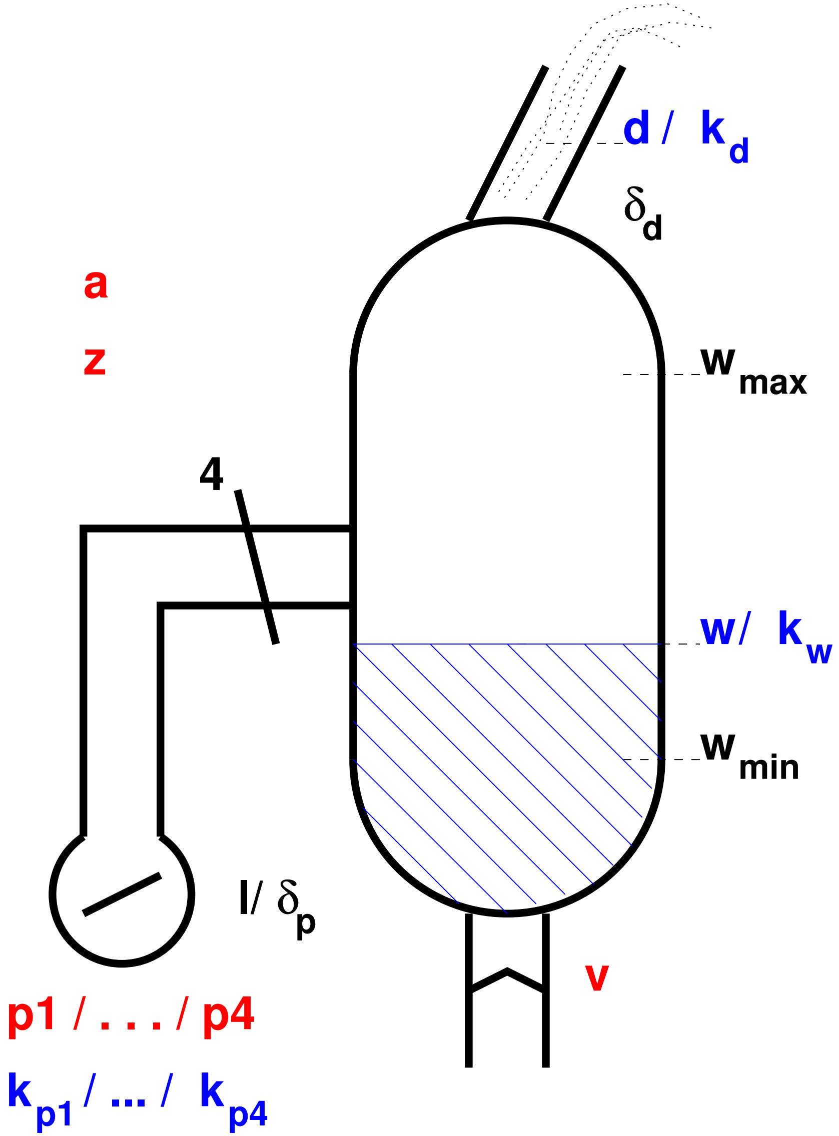


Physical constants

w_{min}	minimal water level
w_{max}	maximal water level
l	water amount per pu
d_{max}	maximal quantity of exiting the boiler
δ_p	error in the value of
δ_d	error in steam

measurement

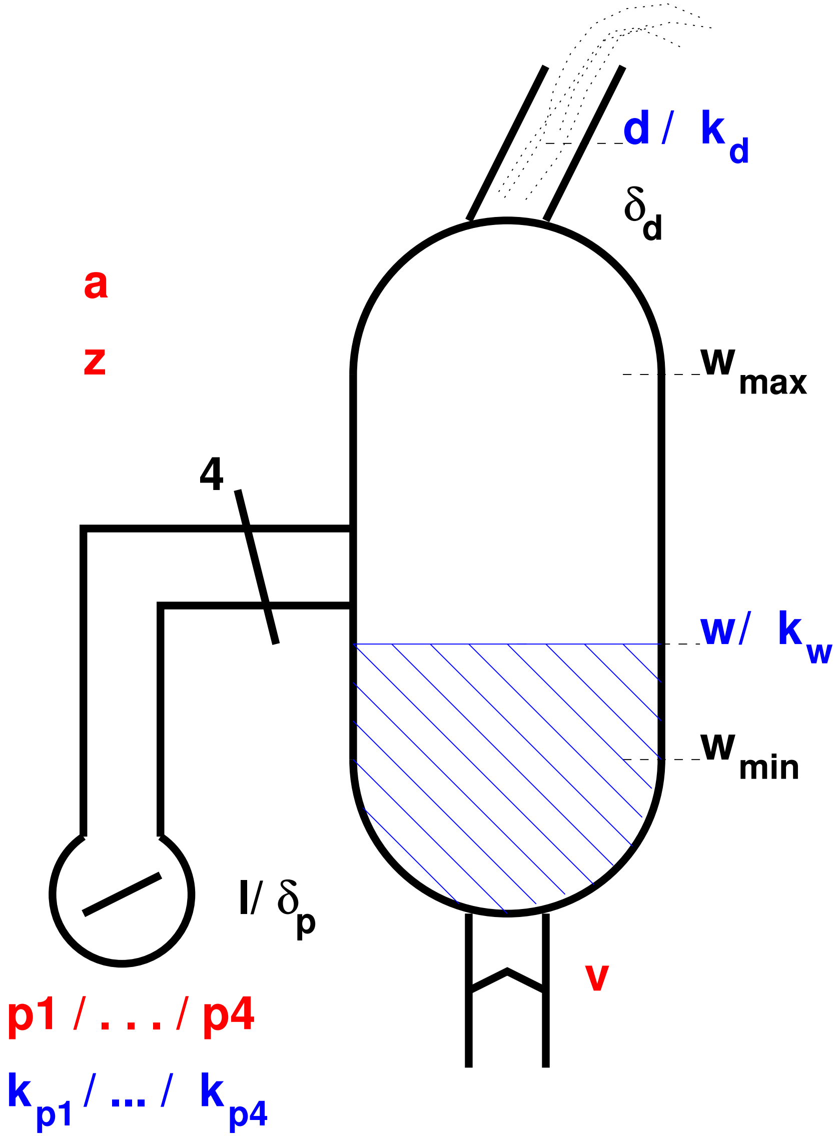
Steam Boiler Control: Scenario



Measured values

w	water level
d	amount of steam exiting the boiler
$k_{p,i}$	pump i works/broken
k_w	water level measuring device works/broken
k_d	steam amount measuring device works/broken

Steam Boiler Control: Scenario



Control values

p_i	**pump i on/off**
v	**valve open/closed**
a	**boiler on/off**
z	**state init/norm/broken/stop**

Steam Boiler Control

Types

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

$$OnOff ::= on \mid off$$

$$OpenClosed ::= open \mid closed$$

Steam Boiler Control

Physical constants

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

Steam Boiler Control

Physical constants

$$w_{min} : \mathbb{N}$$
$$w_{max} : \mathbb{N}$$
$$l : \mathbb{N}$$
$$d_{max} : \mathbb{N}$$
$$\delta_p : \mathbb{N}$$
$$\delta_d : \mathbb{N}$$

$$w_{min} < w_{max}$$

Measured values

Input

$$w? : \mathbb{N}$$
$$d? : \mathbb{N}$$

Steam Boiler Control

Control values

Pumps

$p_1, p_2, p_3, p_4 : \mathit{OnOff}$

*SteamBoiler*0

Pumps
$v : \mathit{OpenClosed}$
$a : \mathit{OnOff}$
$z : \mathit{State}$

Auxiliary Schemata

Auxiliary Schemata

PumpsOff

$Pumps'$

$$p'_1 = \mathit{off} \land p'_2 = \mathit{off} \land p'_3 = \mathit{off} \land p'_4 = \mathit{off}$$

PumpsOn

$Pumps'$

$$p'_1 = \mathit{on} \land p'_2 = \mathit{on} \land p'_3 = \mathit{on} \land p'_4 = \mathit{on}$$

Steam Boiler Initial State

SteamBoilerInit0

$SteamBoiler0'$

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

Operations for Initialisation

$SInitNormal0$

$\Delta SteamBoiler0$

$Input$

$z = init$

$d? = 0$

$w? \geq w_{min} + d_{max}$

$w? \leq w_{max}$

$PumpsOff$

$z' = norm$

$v' = closed$

$a' = on$

Operations for Initialisation

$SInitStop0$

$\Delta SteamBoiler0$
$Input$

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

Operations for Initialisation

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\mathit{SInitFill0}} \\
\Delta \mathit{SteamBoiler0} \\
\mathit{Input} \\
\hline
z = \mathit{init} \\
d? = 0 \\
w? < w_{min} + d_{max} \\
\mathit{PumpsOn} \\
z' = z \\
v' = \mathit{closed} \\
a' = \mathit{off} \\
\hline
\end{array}
$$

Operations for Initialisation

$SInitEmpty0$

$\Delta SteamBoiler0$

$Input$

$z = init$

$d? = 0$

$w? > w_{max}$

$PumpsOff$

$z' = z$

$v' = open$

$a' = off$

Operations for Initialisation

$$
\begin{array}{lcll}
\mathit{ControlInit0} & \mathrel{\widehat{=}} & & \mathit{SInitNormal0} \\
 & & \vee & \mathit{SInitStop0} \\
 & & \vee & \mathit{SInitFill0} \\
 & & \vee & \mathit{SInitEmpty0}
\end{array}
$$

Operations for Normal State

$SNormalFill0$

$\Delta SteamBoiler0$

$Input$

$z = norm$

$w? \geq w_{min}$

$w? \leq w_{opt} - 3l$

$PumpsOn$

$v' = closed \land a' = on \land z' = z$

Note:

Simplified version where all four pumps are switched simultaneously

Operations for Normal State

$$\begin{array}{|l}
\multicolumn{1}{l}{\textit{SNormalContinue}0} \\
\hline
\Xi \textit{SteamBoiler}0 \\
\textit{Input} \\
\hline
z = \textit{norm} \\
w? > w_{opt} - 3l \\
w? \leq w_{opt} \\
\hline
\end{array}$$

Operations for Normal State

$$
\begin{array}{|l}
\multicolumn{1}{l}{\underline{\quad \mathit{SNormalNotFill0} \qquad\qquad\qquad\qquad\qquad\qquad}} \\
\Delta \mathit{SteamBoiler0} \\
\mathit{Input} \\
\hline
z = \mathit{norm} \\
w? > w_{opt} \\
w? \leq w_{max} \\
\mathit{PumpsOff} \\
v' = \mathit{closed} \land a' = \mathit{on} \land z' = z \\
\hline
\end{array}
$$

Operations for Normal State

$SNormalStop0$

$\Delta SteamBoiler0$
$Input$

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

Complete Operation

$$
\begin{array}{rcl}
\mathit{ControlNormal}0 & \widehat{=} & \mathit{SNormalFill}0 \\
& \vee & \mathit{SNormalContinue}0 \\
& \vee & \mathit{SNormalNotFill}0 \\
& \vee & \mathit{SNormalStop}0
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Control}0 & \widehat{=} & \mathit{ControlInit}0 \\
& \vee & \mathit{ControlNormal}0
\end{array}
$$

Extended Solution

Additional Type

$$\mathit{WorksBroken} ::= \mathit{works} \mid \mathit{broken}$$

Extended Solution

Additional Type

$$\mathit{WorksBroken} ::= \mathit{works} \mid \mathit{broken}$$

Additional measured values

$$\begin{array}{|l}
\multicolumn{1}{l}{\mathit{ControlInput}} \\ \hline
k_w? : \mathit{WorksBroken} \\
k_d? : \mathit{WorksBroken} \\
k_{p1}? : \mathit{WorksBroken} \\
k_{p2}? : \mathit{WorksBroken} \\
k_{p3}? : \mathit{WorksBroken} \\
k_{p4}? : \mathit{WorksBroken} \\ \hline
\end{array}$$

Extended Solution

Control values

$SteamBoiler1$

$SteamBoiler0$
$s : \mathbb{N}$
$\delta : \mathbb{N}$

Extended Solution

Control values

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{SteamBoiler1}} \\
\hline
\mathit{SteamBoiler0} \\
s : \mathbb{N} \\
\delta : \mathbb{N} \\
\hline
\end{array}
$$

Initial State

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{SteamBoilerInit1}} \\
\hline
\mathit{SteamBoiler1}' \\
\hline
a' = \mathit{off} \\
z' = \mathit{init} \\
\hline
\end{array}
$$

Extended Auxiliary Schemata

Auxiliary Functions

$$
\begin{array}{|l}
\mathit{pswitch} : (\mathit{OnOff} \times \mathit{WorksBroken}) \rightarrow \mathit{OnOff} \\
\hline
\mathit{pswitch}(\mathit{on}, \mathit{works}) = \mathit{on} \\
\mathit{pswitch}(\mathit{on}, \mathit{broken}) = \mathit{off} \\
\mathit{pswitch}(\mathit{off}, \mathit{works}) = \mathit{off} \\
\mathit{pswitch}(\mathit{off}, \mathit{broken}) = \mathit{off}
\end{array}
$$

$$
\begin{array}{|l}
\mathit{pamount} : (\mathit{OnOff} \times \mathit{WorksBroken}) \rightarrow \mathbb{N} \\
\hline
\forall x : \mathit{OnOff}, y : \mathit{WorksBroken} \\
\qquad\qquad \mid x = \mathit{off} \lor y = \mathit{broken} \bullet \mathit{pamount}(x, y) = 0 \\
\mathit{pamount}(\mathit{on}, \mathit{works}) = 1
\end{array}
$$

Extended Auxiliary Schemata

Auxiliary Schemata

PumpsControlledOn

$Pumps'$
$ControlInput$

$$p'_1 = pswitch(on, k_{p1}?) \wedge p'_2 = pswitch(on, k_{p2}?)$$
$$p'_3 = pswitch(on, k_{p3}?) \wedge p'_4 = pswitch(on, k_{p4}?)$$

PumpsControlledOff

$Pumps'$
$ControlInput$

$$p'_1 = pswitch(off, k_{p1}?) \wedge p'_2 = pswitch(off, k_{p2}?)$$
$$p'_3 = pswitch(off, k_{p3}?) \wedge p'_4 = pswitch(off, k_{p4}?)$$

Operations for Initialisation

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{SInitNormal}1} \\
\hline
\Delta \mathit{SteamBoiler}1 \\
\mathit{Input} \\
\mathit{ControlInput} \\
\hline
z = \mathit{init} \\
d? = 0 \\
k_w = \mathit{works} \land k_d = \mathit{works} \\
w? \geq w_{min} + d_{max} \\
w? \leq w_{max} \\
z' = \mathit{norm} \\
v' = \mathit{closed} \\
a' = \mathit{on} \\
s' = w? \\
\mathit{PumpsOff} \\
\hline
\end{array}
$$

Operations for Initialisation

$SInitFill1$

$\Delta SteamBoiler1$
$Input$
$ControlInput$

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

Operations for Initialisation

$SInitEmpty1$

$\Delta SteamBoiler1$
$Input$
$ControlInput$

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

Operations for Initialisation

$$
\begin{array}{|l}
\hline
\textit{SInitStop}1 \\
\Delta \textit{SteamBoiler}1 \\
\textit{Input} \\
\textit{ControlInput} \\
\hline
z = \textit{init} \\
d? > 0 \lor k_w = \textit{broken} \lor k_d = \textit{broken} \\
z' = \textit{stop} \\
\hline
\end{array}
$$

Operations for Initialisation

$$\begin{aligned} \mathit{ControlInit}1 \quad \widehat{=} \quad & \ \mathit{SInitNormal}1 \\ & \vee\ \mathit{SInitFill}1 \\ & \vee\ \mathit{SInitEmpty}1 \\ & \vee\ \mathit{SInitStop}1 \end{aligned}$$

Operations for Normal State

$$
\begin{array}{|l}
\multicolumn{1}{l}{SNormalFill1} \\
\hline
\Delta SteamBoiler1 \\
Input \\
ControlInput \\
\hline
z = norm \\
k_w = works \\
w? \geq w_{min} \\
w? \leq w_{opt} - 3l \\
s' = w? \\
PumpsControlledOn \\
v' = closed \land a' = on \land z' = z \\
\hline
\end{array}
$$

Operations for Normal State

*SNormalContinue*1

$\Delta SteamBoiler1$
$Input$
$ControlInput$

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

Operations for Normal State

$SNormalNotFill1$

$\Delta SteamBoiler1$
$Input$
$ControlInput$

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

Operations for Normal State

$SNormalWaterStop1$

$\Delta SteamBoiler1$
$Input$
$ControlInput$

$$z = norm \lor z = broken$$
$$k_w = works$$

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

Operations for Normal State

$SNormalControlStop1$

$\Delta SteamBoiler1$

$Input$

$ControlInput$

$$z = norm$$

$$k_w = broken \land k_d = broken$$

$$a' = off \land z' = stop$$

Schema *AmountComputation*

$$
\begin{array}{|l}
\multicolumn{1}{l}{\textit{AmountComputation}} \\
\hline
\mathit{SteamBoiler}1 \\
\mathit{ControlInput} \\
\mathit{amount} : \mathbb{N} \\
\delta_{\mathit{pumps}} : \mathbb{N} \\
\hline
\mathit{amount} = l * (\mathit{pamount}(p_1, k_{p1}?) + \mathit{pamount}(p_2, k_{p2}?) + \\
\qquad\qquad\quad \mathit{pamount}(p_3, k_{p3}?) + \mathit{pamount}(p_4, k_{p4}?)) \\
\delta_{\mathit{pumps}} = \delta_p * (\mathit{pamount}(p_1, \mathit{works}) + \mathit{pamount}(p_2, \mathit{works}) + \\
\qquad\qquad\quad \mathit{pamount}(p_3, \mathit{works}) + \mathit{pamount}(p_4, \mathit{works})) \\
\hline
\end{array}
$$

Operations for Normal State

$$\mathit{SNormalBroken}1$$

$$\begin{array}{l}
\Delta \mathit{SteamBoiler}1 \\
\mathit{Input} \\
\mathit{ControlInput} \\
\mathit{AmountComputation}
\end{array}$$

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

Complete Operation

$$\begin{array}{lcl} \mathit{ControlNormal}1 & \widehat{=} & \ \mathit{SNormalFill}1 \\ & & \vee\ \mathit{SNormalContinue}1 \\ & & \vee\ \mathit{SNormalNotFill}1 \\ & & \vee\ \mathit{SNormalWaterStop}1 \\ & & \vee\ \mathit{SNormalControlStop}1 \\ & & \vee\ \mathit{SNormalBroken}1 \end{array}$$

Operations for Broken State

$$
\begin{array}{|l}
\multicolumn{1}{l}{\mathit{SBrokenContinue}1} \\
\hline
\Delta \mathit{SteamBoiler}1 \\
\mathit{Input} \\
\mathit{ControlInput} \\
\mathit{AmountComputation} \\
\hline
z = \mathit{broken} \\
k_w = \mathit{broken} \\
k_d = \mathit{works} \\
s' = s + \mathit{amount} - d? \\
\delta' = \delta + \delta_{pumps} + \delta_d \\
s' \geq w_{min} + \delta' \\
s' \leq w_{max} - \delta' \\
s' < (w_{min} + w_{max})/2 \;\rightarrow\; \mathit{PumpsControlledOn} \\
s' \geq (w_{min} + w_{max})/2 \;\rightarrow\; \mathit{PumpsControlledOff} \\
v' = \mathit{closed} \wedge a' = \mathit{on} \\
z' = \mathit{broken} \\
\hline
\end{array}
$$

Operations for Broken State

$$
\begin{array}{|l}
\multicolumn{1}{l}{\_\_\mathit{SBrokenNormal1}\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_} \\
\Delta \mathit{SteamBoiler1} \\
\mathit{Input} \\
\mathit{ControlInput} \\
\mathit{AmountComputation} \\
\hline
z = \mathit{broken} \\
k_w = \mathit{works} \\
w? \geq w_{min} \\
w? \leq w_{max} \\
w? < (w_{min} + w_{max})/2 \ \longrightarrow \ \mathit{PumpsControlledOn} \\
w? \geq (w_{min} + w_{max})/2 \ \longrightarrow \ \mathit{PumpsControlledOff} \\
s' = w? \\
v' = \mathit{closed} \wedge a' = \mathit{on} \\
z' = \mathit{norm} \\
\hline
\end{array}
$$

Operations for Broken State

$\mathit{SBrokenControlStop}1$

$\Delta \mathit{SteamBoiler}1$

Input

$\mathit{ControlInput}$

$z = \mathit{broken}$

$k_w = \mathit{broken}$

$k_d = \mathit{broken}$

$a' = \mathit{off} \land z' = \mathit{stop}$

Operations for Broken State

$$\begin{array}{l}
\textit{SBrokenWaterStop1} \\
\hline
\Delta \textit{SteamBoiler1} \\
\textit{Input} \\
\textit{ControlInput} \\
\textit{AmountComputation} \\
\hline
z = \textit{broken} \lor z = \textit{norm} \\
k_w = \textit{broken} \\
k_d = \textit{works} \\
s' = s + \textit{amount} - d? \\
z = \textit{broken} \;\longrightarrow\; \delta' = \delta + \delta_{\textit{pumps}} + \delta_d \\
z = \textit{norm} \;\longrightarrow\; \delta' = \delta_{\textit{pumps}} + \delta_d \\
s' < w_{\textit{min}} + \delta' \lor s' > w_{\textit{max}} - \delta' \\
a' = \textit{off} \land z' = \textit{stop} \\
\hline
\end{array}$$

Operations for Broken State

$$\begin{aligned}
\mathit{ControlBroken1} \;\widehat{=}\; & \quad \mathit{SBrokenContinue1} \\
& \lor \; \mathit{SBrokenNormal1} \\
& \lor \; \mathit{SBrokenControlStop1} \\
& \lor \; \mathit{SBrokenWaterStop1}
\end{aligned}$$

Complete Operation

$$\begin{array}{lcl} \mathit{Control}1 & \mathrel{\widehat{=}} & \quad \mathit{ControlInit}1 \\ & & \lor \ \mathit{ControlNormal}1 \\ & & \lor \ \mathit{ControlBroken}1 \end{array}$$