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

$OnOff ::= on \mid off$

$OpenClosed ::= open \mid closed$

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

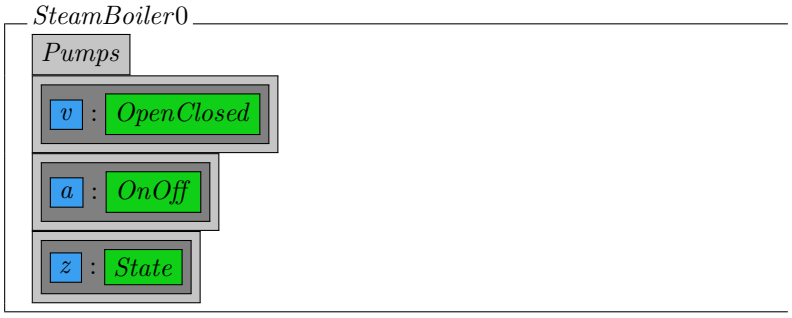
Input

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

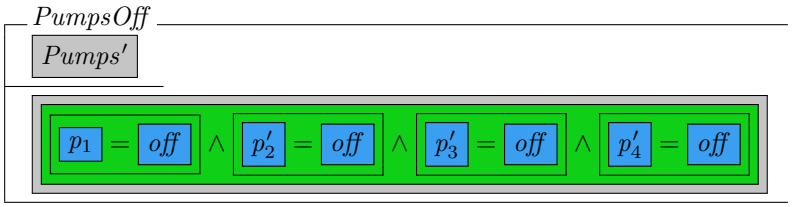
Control values

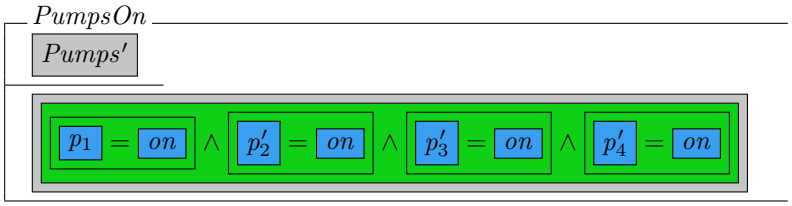
Pumps

$$p_1, p_2, p_3, p_4 : OnOff$$

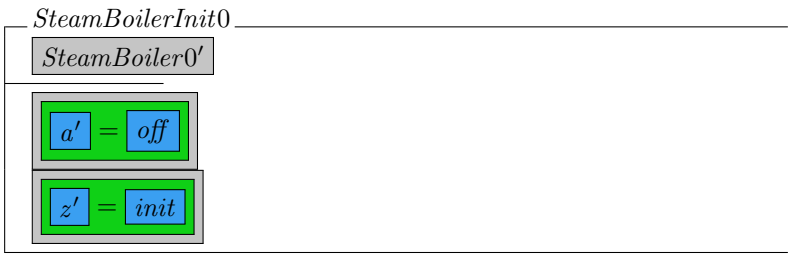


Auxiliary Schemata





Steam Boiler Initial State



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

SNormalFill0

$\Delta SteamBoiler0$

$Input$

$z = norm$

$w? \geq w_{min}$

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

$PumpsOn$

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

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

SNormalContinue0

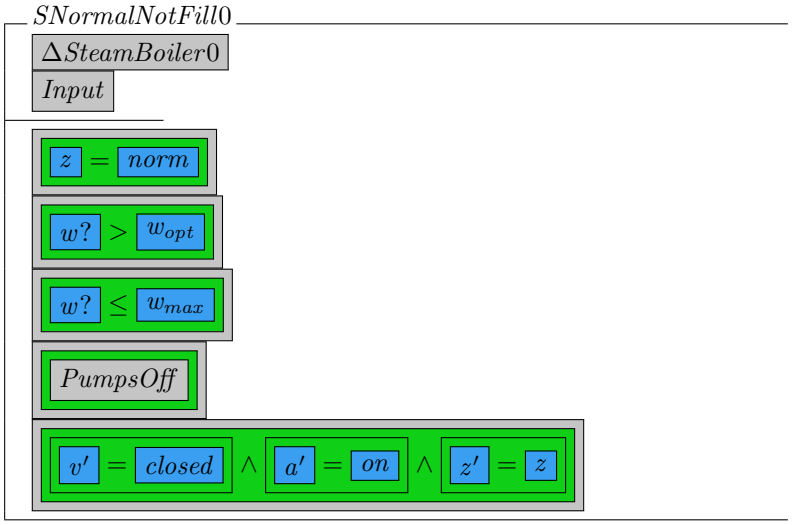
$\Xi SteamBoiler0$

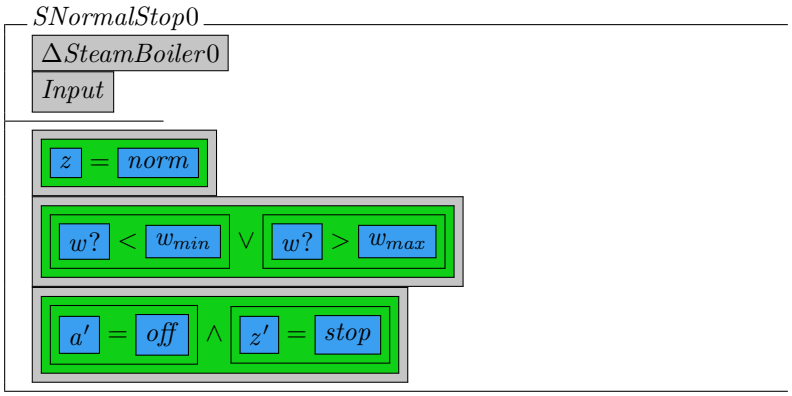
$Input$

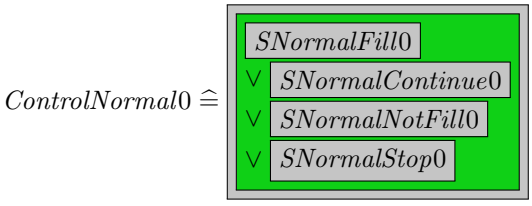
$z = norm$

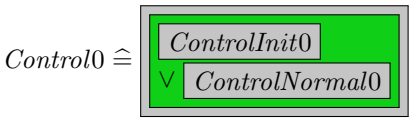
$w? > w_{opt} - 3\,l$

$w? \leq w_{opt}$









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

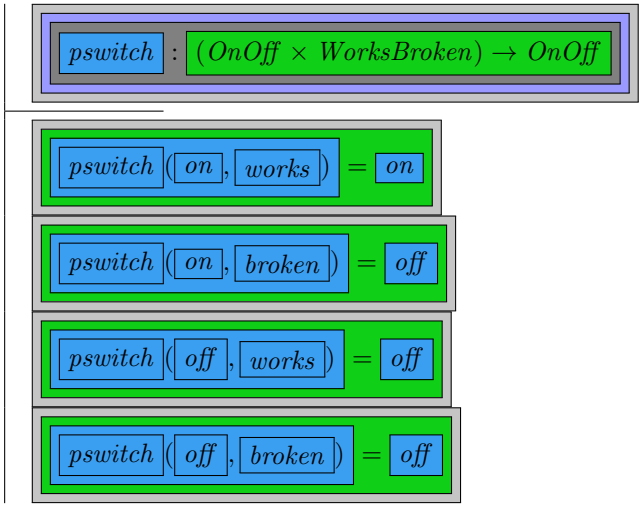
*SteamBoilerInit*1

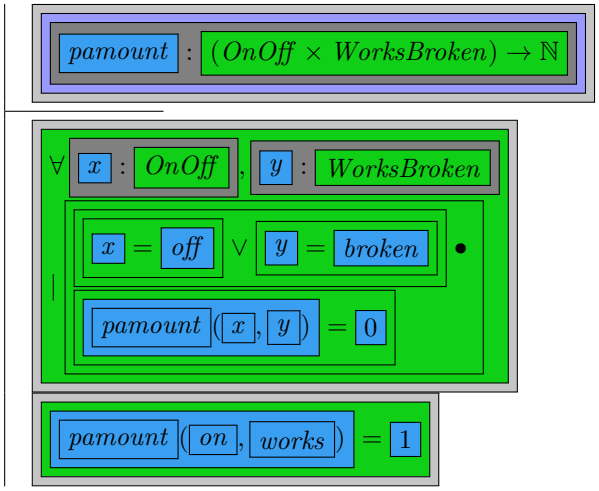
*SteamBoiler*1′

$a' = off$

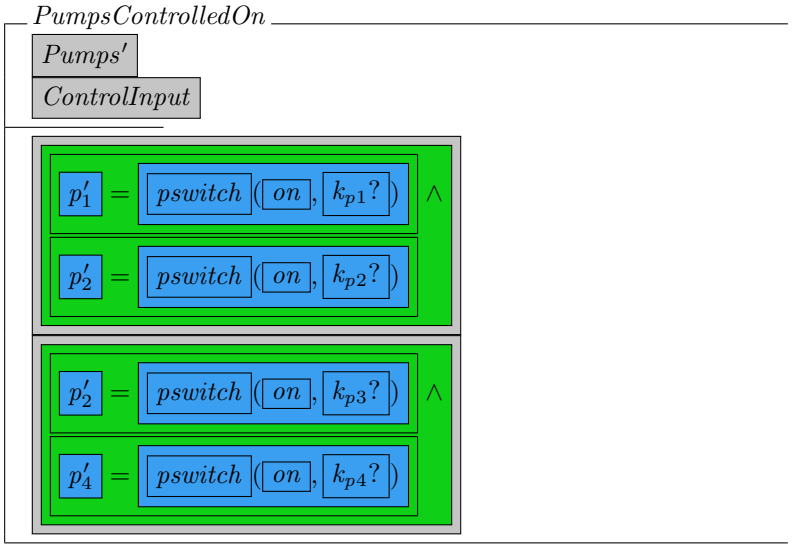
$z' = init$

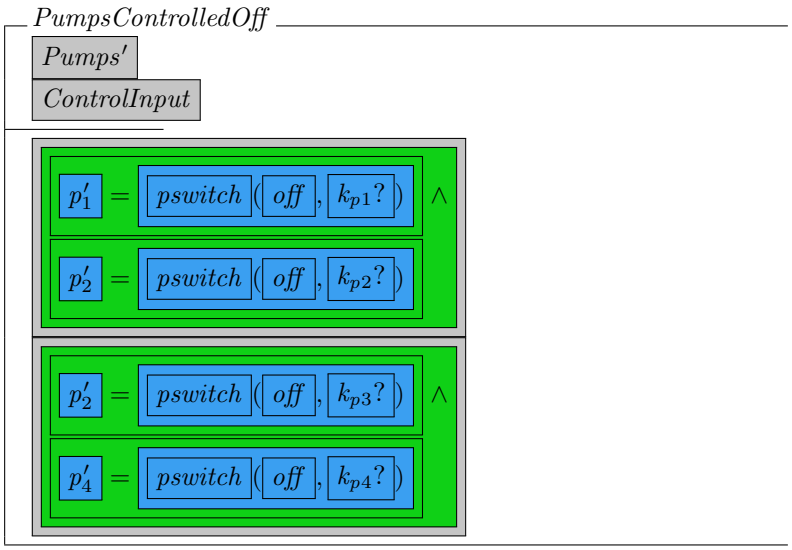
Auxiliary Functions



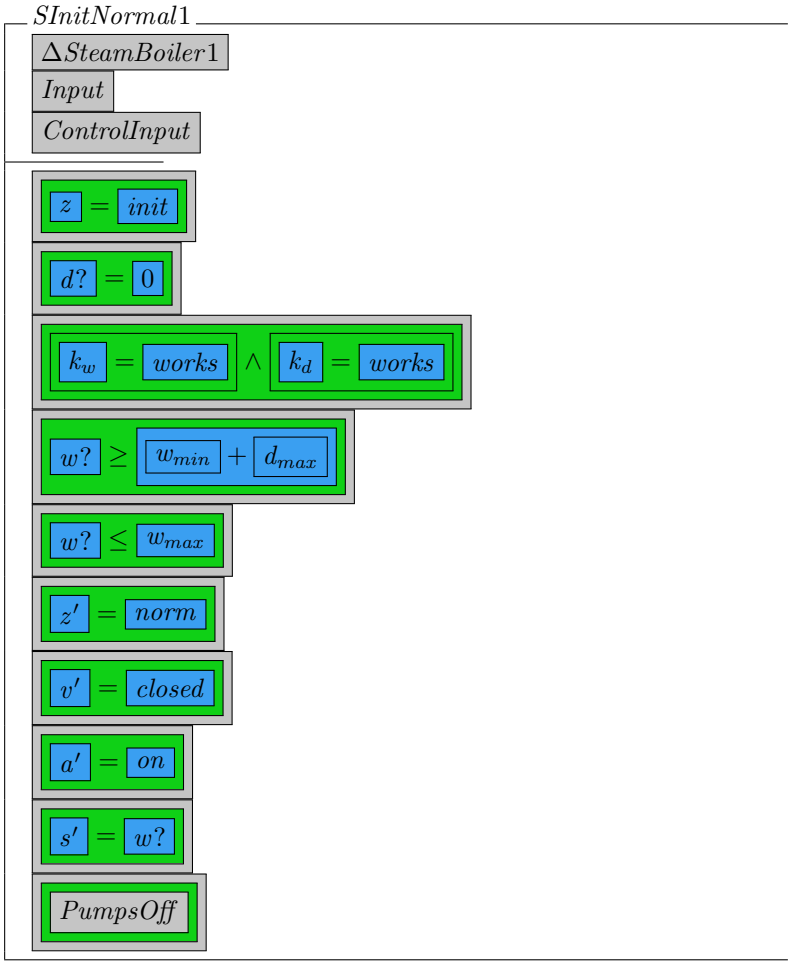


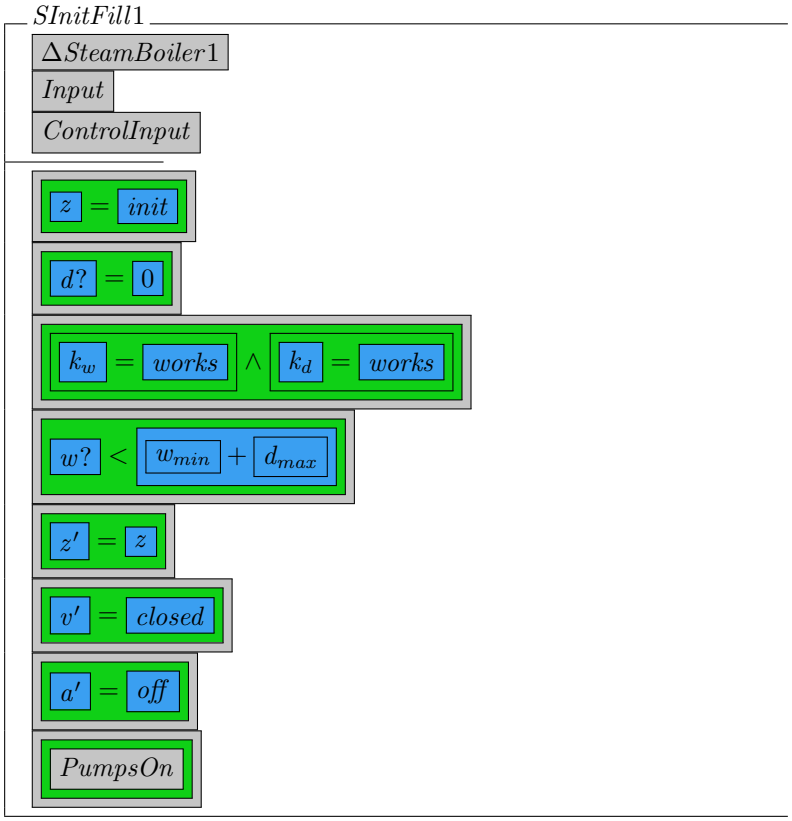
Auxilary Schemata

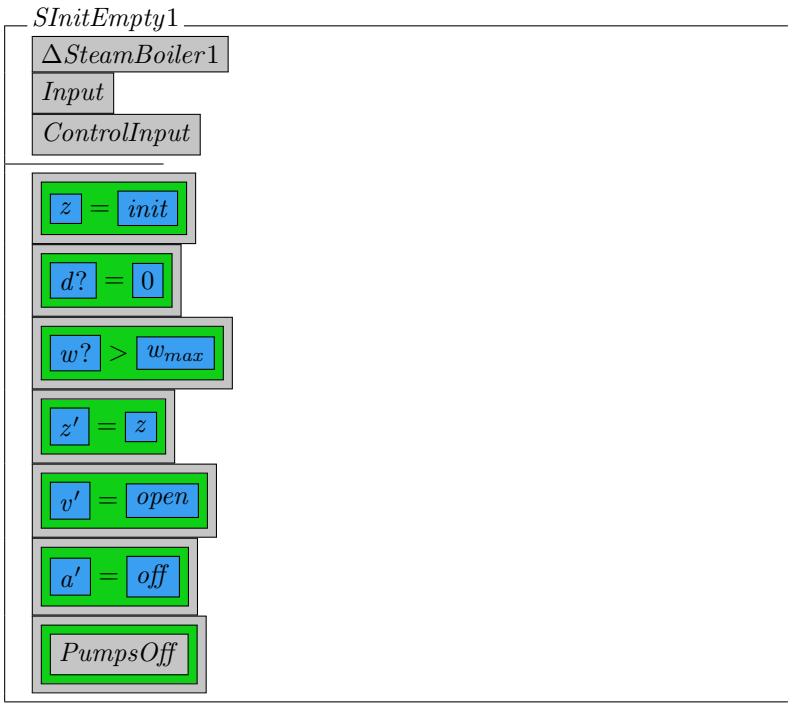


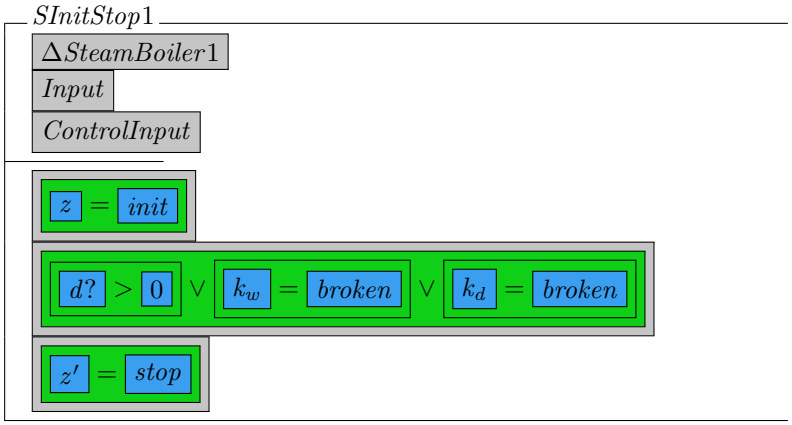


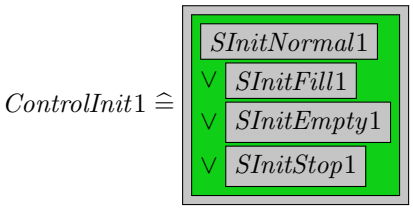
Operations for Initialisation


SInitNormal1
ΔSteamBoiler1
Input
ControlInput
z = init
d? = 0
k_w = works ∧ k_d = works
w? ≥ w_min + d_max
w? ≤ w_max
z' = norm
v' = closed
a' = on
s' = w?
PumpsOff

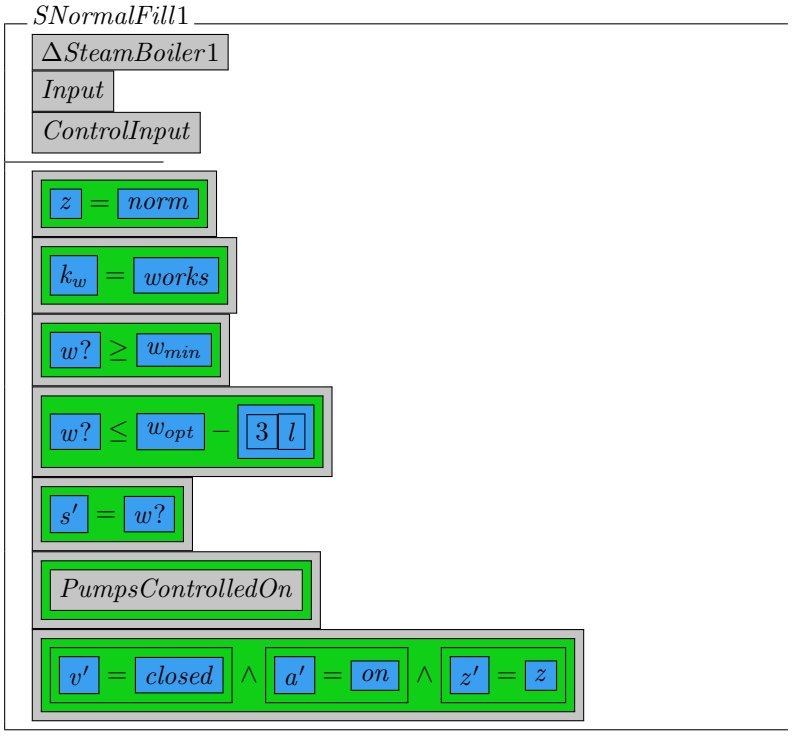

SInitFill1
ΔSteamBoiler1
Input
ControlInput
z = init
d? = 0
k_w = works ∧ k_d = works
w? < w_min + d_max
z' = z
v' = closed
a' = off
PumpsOn

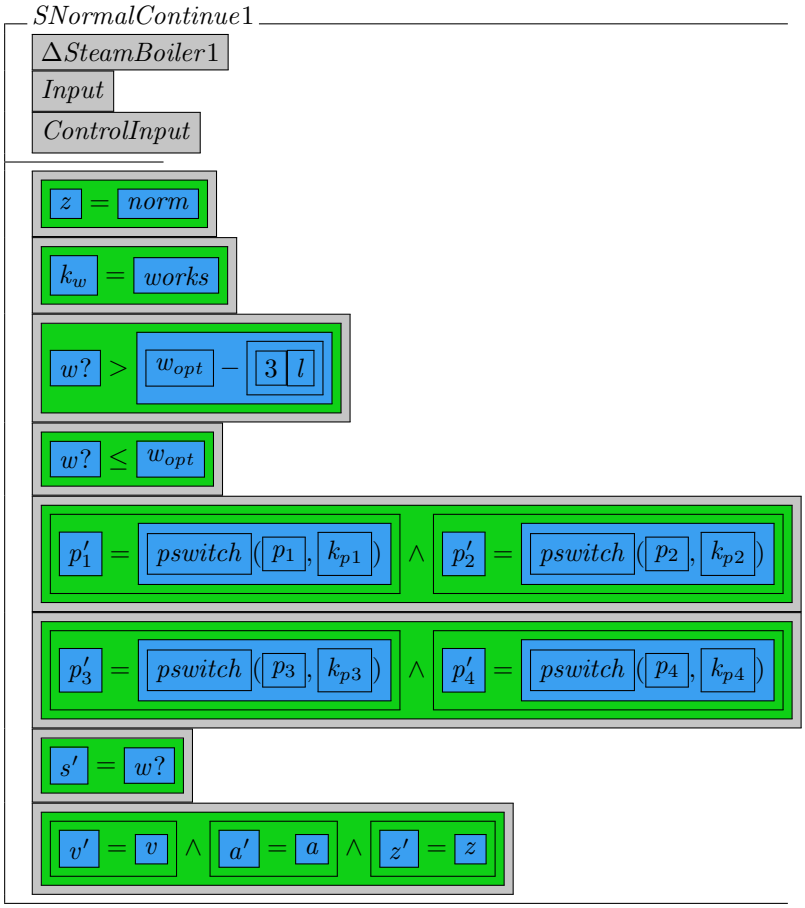






Operations for Normal State


SNormalFill1
ΔSteamBoiler1
Input
ControlInput
z = norm
k_w = works
w? ≥ w_min
w? ≤ w_opt − 3 l
s' = w?
PumpsControlledOn
v' = closed ∧ a' = on ∧ z' = z


SNormalContinue1
ΔSteamBoiler1
Input
ControlInput
z = norm
k_w = works
w? > w_opt − 3 l
w? ≤ w_opt
p'_1 = pswitch(p_1, k_p1) ∧ p'_2 = pswitch(p_2, k_p2)
p'_3 = pswitch(p_3, k_p3) ∧ p'_4 = pswitch(p_4, k_p4)
s' = w?
v' = v ∧ a' = a ∧ 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

$\Delta SteamBoiler$

$Input$

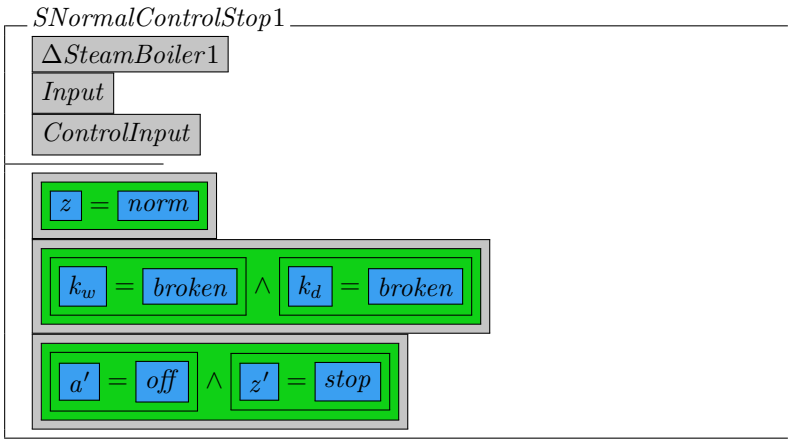
$ControlInput$

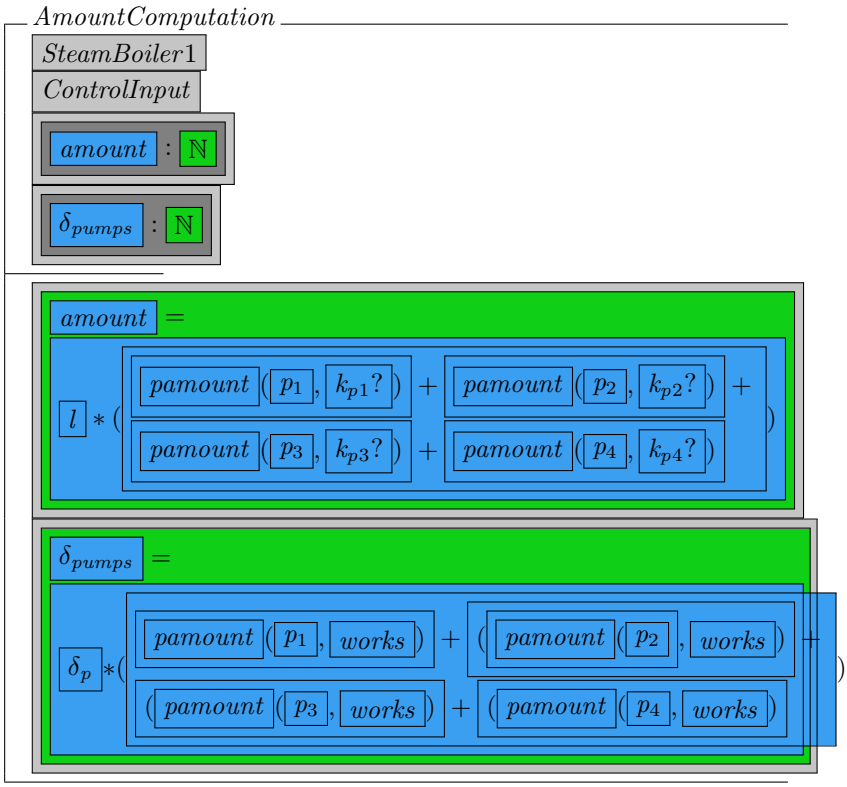
$z = norm \lor z = broken$

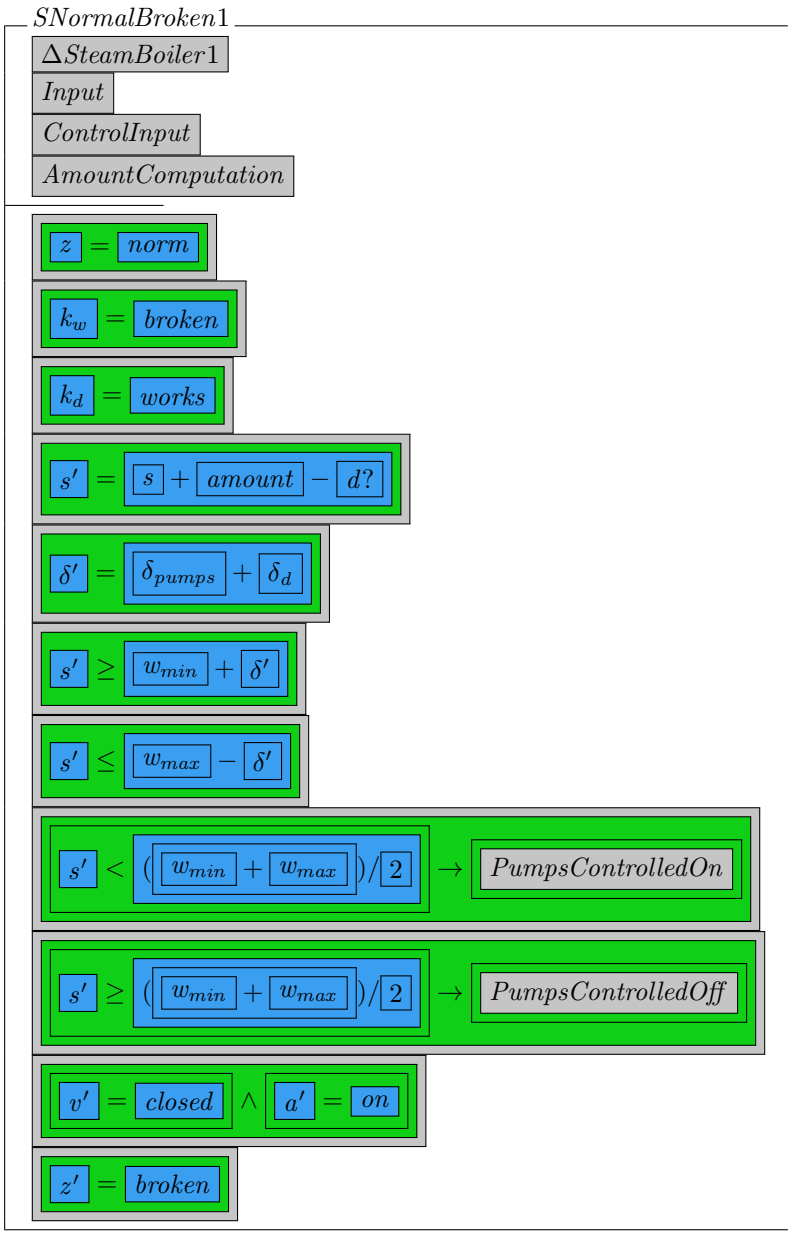
$k_w = works$

$w? < w_{min} \lor w? > w_{max}$

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


SNormalControlStop1
ΔSteamBoiler1
Input
ControlInput
z = norm
k_w = broken ∧ k_d = broken
a' = off ∧ z' = stop

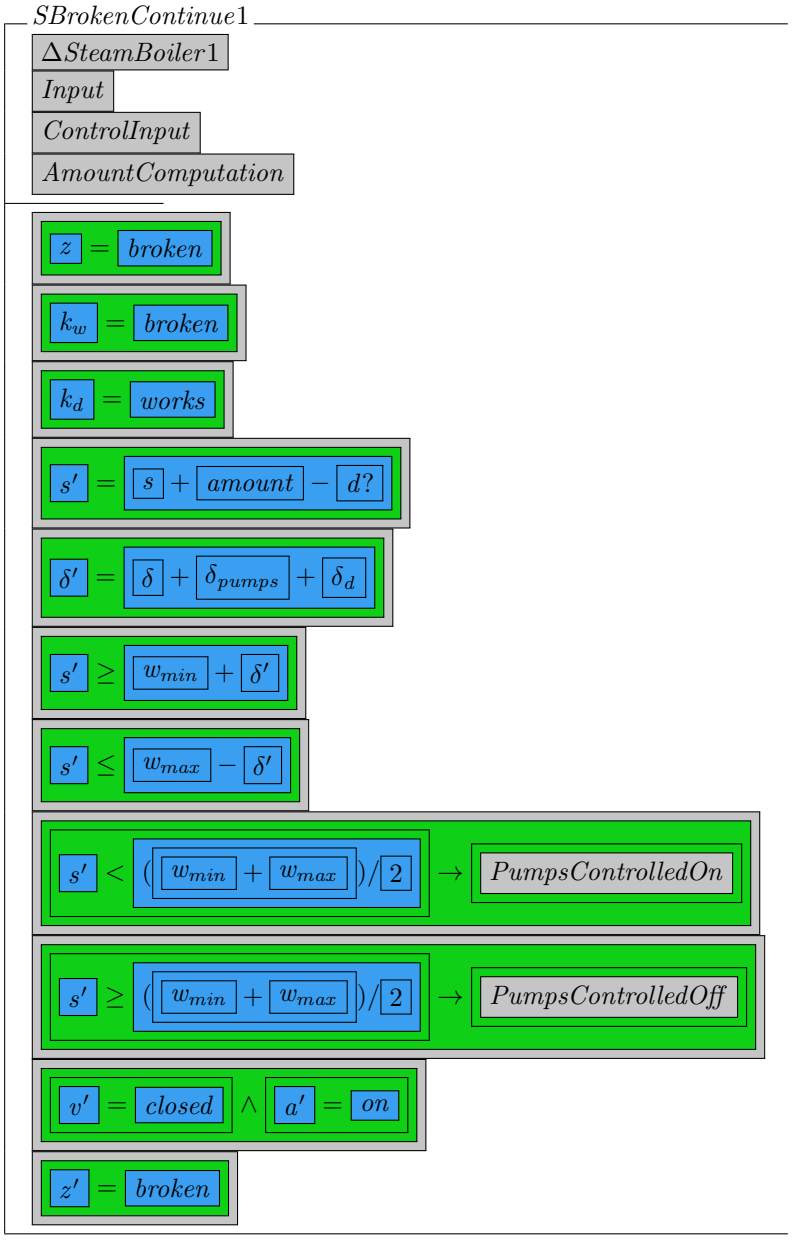

AmountComputation
SteamBoiler1
ControlInput
amount : ℕ
δ_pumps : ℕ
amount =
l * (pamount(p1, k_p1?) + pamount(p2, k_p2?) + pamount(p3, k_p3?) + pamount(p4, k_p4?))
δ_pumps =
δ_p * (pamount(p1, works) + (pamount(p2, works) + (pamount(p3, works) + (pamount(p4, works)))))

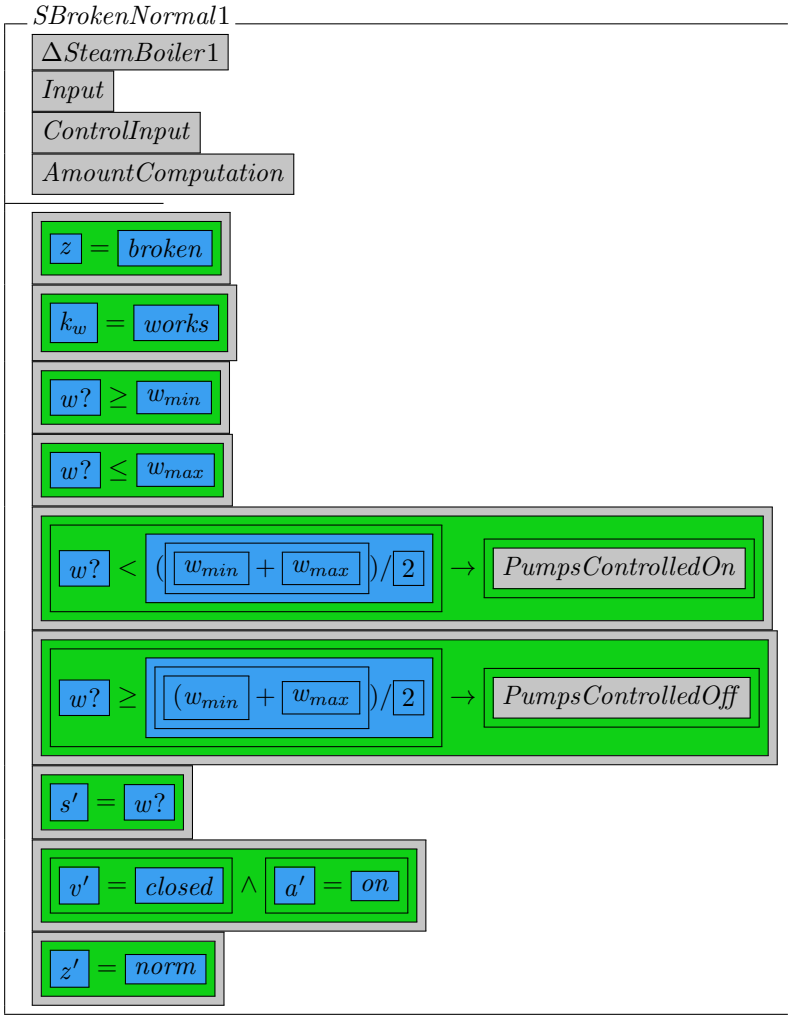


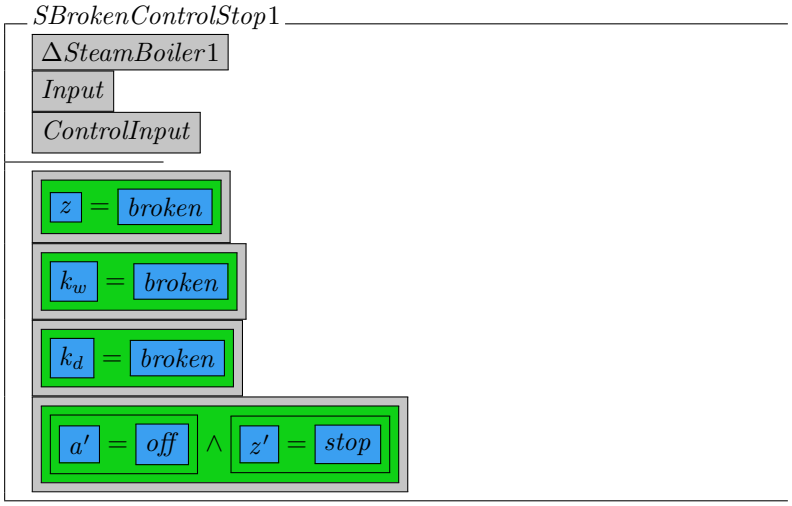
Complete Operation

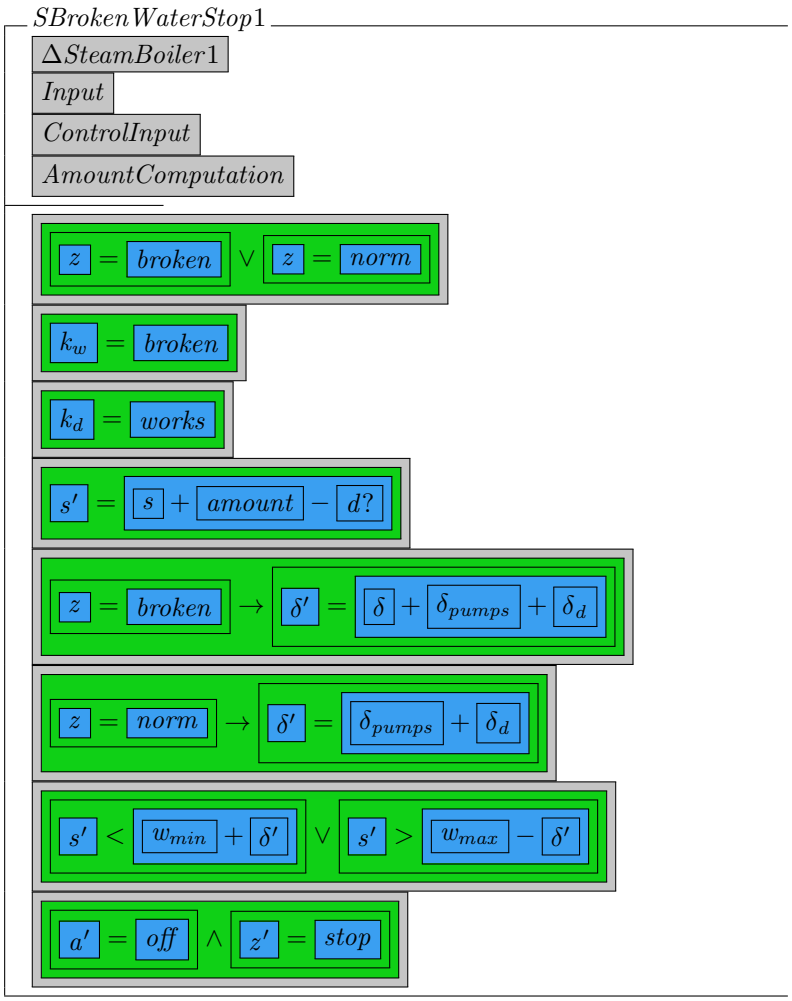
$$ControlNormal1 \mathrel{\widehat{=}} \boxed{\begin{array}{l} SNormalFill1 \\ \vee\ SNormalContinue1 \\ \vee\ SNormalNotFill1 \\ \vee\ SNormalWaterStop1 \\ \vee\ SNormalControlStop1 \\ \vee\ SNormalBroken1 \end{array}}$$

Operations for Broken State


SBrokenContinue1
ΔSteamBoiler1
Input
ControlInput
AmountComputation
z = broken
k_w = broken
k_d = works
s' = s + amount − d?
δ' = δ + δ_pumps + δ_d
s' ≥ w_min + δ'
s' ≤ w_max − δ'
s' < (w_min + w_max)/2 → PumpsControlledOn
s' ≥ (w_min + w_max)/2 → PumpsControlledOff
v' = closed ∧ a' = on
z' = broken


SBrokenNormal1
ΔSteamBoiler1
Input
ControlInput
AmountComputation
z = broken
k_w = works
w? ≥ w_min
w? ≤ w_max
w? < (w_min + w_max)/2 → PumpsControlledOn
w? ≥ (w_min + w_max)/2 → PumpsControlledOff
s' = w?
v' = closed ∧ a' = on
z' = norm


SBrokenControlStop1
ΔSteamBoiler1
Input
ControlInput
z = broken
k_w = broken
k_d = broken
a' = off ∧ z' = stop



$ControlBroken1 \mathrel{\widehat{=}}$