Correction Sheet

After our paper "Proving Safety Properties of the Steam Boiler Controller" went already to print, Myla Archer and Constance Heitmeyer verified the lengthy lemmas and theorems with the theorem prover PVS. Unfortunately, several errors were found in the proofs. These pages summarize the corrections to the paper. No major changes were done to the model. An updated version of both papers is available under the WWW address http://theory.lcs.mit.edu/tds/boiler.html.

Following are the corrections to these errors and some typing errors for the full version of the paper (on the LNCS CD-ROM):

1. p. 7: Lemma 1.2 is incorrect. It should be:

$$\delta_{LOW}(a, b, u) \geq \begin{cases} a^2/(2*\mathbf{U_2}) & \text{if } a < \mathbf{U_2} * u \\ a * u - \mathbf{U_2}*u^2/2 & \text{otherwise} \end{cases}$$

   Consequent changes in the proofs which use this information are straight forward. This information is used only in Lemma 13 and Theorem 2 which are described below.

2. p. 7: Lemma 1.3 is imprecise. It should be:

$$\delta_{LOW}(a, b, u) \geq \begin{cases} b^2/(2*\mathbf{U_1}) & \text{if } b < \mathbf{U_1} * u \\ b * u - \mathbf{U_1}*u^2/2 & \text{otherwise} \end{cases}$$

   Consequent changes in the proofs which use this information are straight forward. Only slight modifications to the simulation proof are necessary.

3. p. 7: Disregard Lemma 1.7: $\delta_{HIGH}(\mathbf{W}\text{-}\mathbf{U_1}, \mathbf{W}, \mathbf{I}) = \mathbf{W}*\mathbf{I} - \mathbf{U_1}*\mathbf{I}^2/2$ should be $\delta_{HIGH}(\mathbf{W}\text{-}\mathbf{U_1}*\mathbf{I}, \mathbf{W}, \mathbf{I}) = \mathbf{W}*\mathbf{I} - \mathbf{U_1}*\mathbf{I}^2/2$ and requires $\mathbf{W} \geq \mathbf{U_1}*\mathbf{I}$ but it is never used by any of the proofs.
4. p. 7, Some basic relations are missing between constants:
   a. $0 \leq \mathbf{M_1} < \mathbf{M_2} \leq \mathbf{C}$
   b. $\mathbf{S} < \mathbf{I}$
5. p. 8, *error* should be cleaner defined: *error* in the range *[0 … **#pumps**]* instead *[0 … pr_new]*
6. p.12: *min_steam_water(sr)* is wrong defined:

$$min\_steam\_water(sr) = \begin{cases} sr^2/(2*\mathbf{U_2}) & \text{if } sr < \mathbf{U_2}*\mathbf{I} \\ (sr*\mathbf{I} - \mathbf{U_2}*\mathbf{I}^2/2) & \text{otherwise} \end{cases}$$

6. p.12, We introduce *min_steam_water_est(sr)* used in the fault-tolerant controller:

$$min\_steam\_water\_est(sr) = \begin{cases} sr^2/(2*\mathbf{U_1}) & \text{if } sr < \mathbf{U_1}*\mathbf{I} \\ (sr*\mathbf{I} - \mathbf{U_1}*\mathbf{I}^2/2) & \text{otherwise} \end{cases}$$

7. p.13, The initial state of *stopmode* is ***true*** so that Lemma 3 is correct in the initial state.
8. p.13 & p.15, In the sensor action *if* $sr' \leq \mathbf{W} - \mathbf{U_1} * \mathbf{I}$ *or …* should be *if* $sr' \geq \mathbf{W} - \mathbf{U_1} * \mathbf{I}$ *or …*

9. p.15, In the activate action *error* should be *error’*

10. p.16, Lemma 3.1 is consequentially:

   $\boldsymbol{M_2} > wl + \boldsymbol{P} * (pumps * \boldsymbol{S} + \boldsymbol{\#pumps} * (\boldsymbol{I} - \boldsymbol{S})) - min\_steam\_water(sr)$ *or stopmode =* ***true***

11. p.19: Lemma 12 should be:

   if do_output = ***false*** *then*

   if $set = read - \boldsymbol{I} + \boldsymbol{S}$ *then*

   $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*(set\text{-}now) - (v * (read\text{-}now) + \boldsymbol{U_1}*(read\text{-}now)^2/2)$ *or stop =* ***true***

   else $\boldsymbol{M_1} < q - (v * (read\text{-}now) + \boldsymbol{U_1}*(read\text{-}now)^2/2)$ *or stop =* ***true***

   The detailed proof can be found below.

12. p.20: Lemma 13 should be:

   if do_output = ***false*** *then*

   if $set = read - \boldsymbol{I} + \boldsymbol{S}$ *then*

   $\boldsymbol{M_2} > q + \boldsymbol{P}*(pumps*(set\text{-}now) + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - steam$ *or stop =* ***true***

   else $\boldsymbol{M_2} > q + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now) - steam$ *or stop =* ***true***

   $$\text{with } steam = \begin{cases} v^2/2*\boldsymbol{U_2} & \text{if } v < \boldsymbol{U_2}(read\text{-}now) \\ (read\text{-}now) - \boldsymbol{U_2}*(read\text{-}now)^2/2) & \text{otherwise} \end{cases}$$

   The detailed proof can be found below.

13. p.21, Consequentially, the proof to Theorem 2 changes. Its detail can be found below. Moreover, Theorem 2 needs following additional information which, we prove also below.

   $d(u) \geq min(0, d(S))$ for $S \geq u \geq 0$, $d(u) = A*u - B*u^2$ with A real and B positive real

14. p.24, The estimated water level in the sensor action should be more precise:

   Use *min_water_level_est(srl’)* instead $(max(0, srl' - \boldsymbol{U_1}*\boldsymbol{I}/2))*\boldsymbol{I}$.

15. p.24, In the sensor action *wl_ok’* and *sr_ok’* should be *wl_ok* and *sr_ok* since they are not changed.

16. p.26ff. There are slight modifications to the simulation proof necessary to accommodate changes in Lemma 1.3 and the introduction of *min_water_level_est*.

We want to excuse for these errors and to thank Myla Archer and Constance Heitmayer for their help in identifying most of them.

The following lemma describes the amount of water remaining above the lower limit depending on the current steam rate and minimum pump rate.

Lemma 12: In all reachable states of the combined steam boiler system,
if do_output = ***false*** *then*

if set = *read* - $\boldsymbol{I}$ +$\boldsymbol{S}$ *then*

$\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*(set\text{-}now) - (v * (read\text{-}now) + \boldsymbol{U_1}*(read\text{-}now)^2/2)$ *or stop* = ***true***

else $\boldsymbol{M_1} < q - (v * (read\text{-}now) + \boldsymbol{U_1}*(read\text{-}now)^2/2)$ *or stop* = ***true***

Proof. In the initial state this Lemma is true. We distinguish on the cases for the action *a*: For the sensor action this lemma is trivially true.

A) *a* = actuator (*set*, *q*, *v*, *pumps* and *now* are unchanged):
We know $\boldsymbol{M_1} < wl + \boldsymbol{P}*pumps*\boldsymbol{S} - (sr * \boldsymbol{I} + \boldsymbol{U_1}*\boldsymbol{I}^2/2)$ *or stopmode* = ***true*** (Lemma 3.2) and Lemma 4: *if do_output then now = read and sr = v and wl = q*. Since *do_output* = ***true*** in the precondition, we know *now* = *read*, *sr* = *v* and *wl* = *q*. Since $now \le read - \boldsymbol{I} + \boldsymbol{S}$ *or set* = *read* + $\boldsymbol{S}$ (Lemma 6), $now \le read$ (Lemma 2), we know *set* = *read* + $\boldsymbol{S}$ and, since *read'* = *now* + $\boldsymbol{I}$ from the effect, *set* = *read'* - $\boldsymbol{I}$ +$\boldsymbol{S}$. Moreover, we know *stop'* = *e_stop* = *stopmode* from the effect and thus, $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*(set\text{-}now) - (v * (read'\text{-} now) + \boldsymbol{U_1}*(read'\text{-}now)^2/2)$ *or stop'* = ***true***. Actuator sets *do_output'* = ***false*** and this lemma is true for the actuator action.

B) *a* = time-passage (*do_output*, *set*, *read*, *stop* and *pumps* are unchanged):
We know *do_output* = ***false*** from *if now < read then do_output* = ***false*** (Lemma 7), from the precondition ($now + \Delta t \le read$) and $\Delta t > 0$.

Based on *set* = *read* + $\boldsymbol{S}$ *or set* = *read* - $\boldsymbol{I}$ + $\boldsymbol{S}$ (Lemma 5), we can distinguish two cases:

1. Case *set* = *read* - $\boldsymbol{I}$ + $\boldsymbol{S}$:

   We know from the assumption $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*(set\text{-}now\text{-}\Delta t+\Delta t) - (v * (read\text{-}now\text{-}\Delta t+\Delta t) + \boldsymbol{U_1}*(read\text{-}now\text{-}\Delta t+\Delta t)^2/2)$ *or stop* = ***true***. This is equivalent to $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*\Delta t - (v*\Delta t + \boldsymbol{U_1}*\Delta t^2/2)+ \boldsymbol{P}*pumps*(set\text{-}now\text{-}\Delta t) - (v * (read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*\Delta t *(read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*(read\text{-}now\text{-}\Delta t)^2/2)$ *or stopmode* = ***true***. Since $v * (read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*\Delta t *(read\text{-}now\text{-}\Delta t) = (v + \boldsymbol{U_1}*\Delta t)*(read\text{-}now\text{-}\Delta t)$ and $now' = now +\Delta t$, $v' \le v + \boldsymbol{U_1} * \Delta t$ from the effect, we get $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*\Delta t - (v*\Delta t + \boldsymbol{U_1}*\Delta t^2/2)+ \boldsymbol{P}*pumps*(set\text{-}now') - (v' * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2)$ *or stop* = ***true***. Since $\delta_{HIGH}(a, b, u) \le (a*u + \boldsymbol{U_1}*u^2/2)$ from Lemma 1.10, *pumps* = *pr* from Lemma 10: *if set* = *read* + $\boldsymbol{S}$ *and do_output* = ***false*** *then pr* = *pr_new* - *error else pr* = *pumps* and $q + pr * \boldsymbol{P} * \Delta t - \delta_{HIGH}(v, v', \Delta t) \le q'$ from the effect, we get $\boldsymbol{M_1} < q' + \boldsymbol{P}*pumps*(set\text{-}now') - (v * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2)$ *or stop* = ***true*** and this case true.

2. Case *set* = *read* + $\boldsymbol{S}$:

We know from the assumption $\boldsymbol{M_1} < q - (v * (read\text{-}now\text{-}\Delta t+\Delta t) + \boldsymbol{U_1}*(read\text{-}now\text{-}\Delta t+\Delta t)^2/2)$ *or stop* = ***true***. This is equivalent to $\boldsymbol{M_1} < q - (v*\Delta t + \boldsymbol{U_1}*\Delta t^2/2) - (v * (read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*\Delta t *(read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*(read\text{-}now\text{-}\Delta t)^2/2)$ *or stop* = ***true***. Since $v * (read\text{-}now\text{-}\Delta t) + \boldsymbol{U_1}*\Delta t *(read\text{-}now\text{-}\Delta t) = (v + \boldsymbol{U_1}*\Delta t)*(read\text{-}now\text{-}\Delta t)$ and $now' = now +\Delta t$, $v' \le v + \boldsymbol{U_1} * \Delta t$ from the effect, we get $\boldsymbol{M_1} < q - (v*\Delta t + \boldsymbol{U_1}*\Delta t^2/2) - (v' * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2)$ *or stop* = ***true***. Since $\delta_{HIGH}(a, b, u) \le (a*u + \boldsymbol{U_1}*u^2/2)$ from Lemma 1.10, $0 \le pr * \boldsymbol{P} * \Delta t$ and $q + pr * \boldsymbol{P} * \Delta t - \delta_{HIGH}(v, v', \Delta t) \le q'$ from the effect, we get $\boldsymbol{M_1} < q' - (v * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2)$ *or stop* = ***true*** and this case true.

C) *a* = activate (only *set* is changed):

If *do_output* = ***true*** this lemma is trivially true. Since we get *set* = *now* from the precondition, $now \le read$ (Lemma 2) and *set* = *read* + ***S*** *or set* = *read* - ***I*** + ***S*** (Lemma 5), we know *set* = *read* - ***I*** + ***S*** and we get from the assumption $\boldsymbol{M_1} < q - (v * (read\text{-}now) + \boldsymbol{U_1}*(read\text{-}now)^2/2)$ *or stop* = ***true***. Since the effect sets *set'* = *read* + ***S*** this lemma is true.

■

The following lemma describes the amount of water remaining to the upper water level limit depending on the current steam rate and the maximum pump rate.

Lemma 13: In all reachable states of the combined steam boiler system

if do_output = ***false*** *then*

if set = *read* - ***I*** + ***S*** *then*

$\boldsymbol{M_2} > q + \boldsymbol{P}*(pumps*(set\text{-}now) + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - steam$ *or stop* = ***true***

else $\boldsymbol{M_2} > q + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now) - steam$ *or stop* = ***true***

with $steam = \begin{cases} v^2/2*\boldsymbol{U_2} & \text{if } v < \boldsymbol{U_2}(read\text{-}now) \\ (v*(read\text{-}now) - \boldsymbol{U_2}*(read\text{-}now)^2/2) & \text{otherwise} \end{cases}$

Proof. In the initial state this Lemma is true. We distinguish on the cases for the action *a*: For *a* = sensor this lemma is trivially true.

A. *a* = actuator (*set*, *q*, *v*, *pumps* and *now* are unchanged):

We know $\boldsymbol{M_2} > wl + \boldsymbol{P}*(pumps*\boldsymbol{S} + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - min\_steam\_water(sr)$ *or stopmode* = ***true*** with

$$min\_steam\_water(sr) = \begin{cases} sr^2/(2*\boldsymbol{U_2}) & \text{if } sr < \boldsymbol{U_2}*\boldsymbol{I} \\ (sr*\boldsymbol{I} - \boldsymbol{U_2}*\boldsymbol{I}^2/2) & \text{otherwise} \end{cases}$$

(Lemma 3.1) and Lemma 4: *if do_output then now = read and sr = v and wl = q*. Since *output* = ***true*** in the precondition, we know *now* = *read*, *sr* = *v* and *wl* = *q*. Since $now \le read$ - ***I*** + ***S*** *or set* = *read* + ***S*** (Lemma 6), $now \le read$ (Lemma 2), we know *set* = *read* + ***S*** and, since *read'* = *now* + ***I*** from the effect, *set* = *read'* - ***I*** +***S***. Since *stop'* = *e_stop* = *stopmode* from the effect, we know $\boldsymbol{M_2} > q + \boldsymbol{P}*(pumps*(set - now) + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - min\_steam\_water(v)$ *or stop'* = ***true*** with

$$min\_steam\_water(sr) = \begin{cases} v^2/2*\boldsymbol{U_2} & \text{if } v < \boldsymbol{U_2}*(read'\text{-}now) \\ \end{cases}$$

$(v*(read'-now) - \mathbf{U_2}*(read'-now)^2/2)$ *otherwise*

The actuator action sets *do_output'* = ***false*** and this lemma is true for the actuator action.

2. *a*= time-passage (*do_output*, *set*, *read*, *stop* and *pumps* are unchanged):
We know *do_output* = ***false*** from (Lemma 7) *if now < read then do_output* = ***false***, from the precondition ($now + \Delta t \leq read$) and $\Delta t > 0$. Since we know $set = read + \mathbf{S}$ *or* $set = read - \mathbf{I} + \mathbf{S}$ (Lemma 5), we can distinguish two cases:

   a. Case $set = read - \mathbf{I} + \mathbf{S}$:

   We know from the assumption $\mathbf{M_2} > q + \mathbf{P}*(pumps*(set\text{-}now\text{-}\Delta t+\Delta t) + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - steam$ *or stop* = ***true*** which is equivalent to $\mathbf{M_2} > q + \mathbf{P} * pumps*\Delta t - \delta_{LOW}(v, v', \Delta t) + \mathbf{P}*(pumps*(set\text{-}now\text{-}\Delta t) + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - steam + \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true***. Moreover, we know from the effect that $now' = now + \Delta t$, $q + \mathbf{P} * pr * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$, and *pumps* = *pr* from Lemma 10: *if set* = *read* + ***S*** *and do_output* = ***false*** *then pr* = *pr_new - error else pr* = *pumps*. Thus, we get $\mathbf{M_2} > q' + \mathbf{P}*(pumps*(set\text{-}now') + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - steam + \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true*** with

$$steam = \begin{cases} v^2/2*\mathbf{U_2} & \text{if } v < \mathbf{U_2}*(read\text{-}now) \\ v(read\text{-}now' + \Delta t) - \mathbf{U_2}*(read\text{-}now' + \Delta t)^2/2) & \text{otherwise} \end{cases}$$

   Based on the steam rate condition and Lemma 1.2:

$$\delta_{LOW}(a, b, u) \geq \begin{cases} a^2/(2*\mathbf{U_2}) & \text{if } a < \mathbf{U_2} * u \\ a * u - \mathbf{U_2}*u^2/2 & \text{otherwise} \end{cases}$$

   we distinguish following cases:

   i. Sub-case $v < \mathbf{U_2}(read\text{-}now)$ and $v < \mathbf{U_2} * \Delta t$:

   Since $\delta_{LOW}(v, v', \Delta t) \geq v^2/(2*\mathbf{U_2})$ and $v'^2/2*\mathbf{U_2} > 0$, we get $\mathbf{M_2} > q' + \mathbf{P}*(pumps*(set\text{-}now') + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - v'^2/(2*\mathbf{U_2})$ *or stop* = ***true*** and this case true.

   ii. Sub-case $v < \mathbf{U_2}(read\text{-}now)$ and $v \geq \mathbf{U_2} * \Delta t$:

   Here, we know $\mathbf{M_2} > q' + \mathbf{P}*(pumps*(set\text{-}now') + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - v^2/(2*\mathbf{U_2}) + (v * \Delta t - \mathbf{U_2}*\Delta t^2/2)$ *or stop* = ***true*** and since $v^2/(2*\mathbf{U_2}) - (v * \Delta t - \mathbf{U_2}*\Delta t^2/2) = (v - \mathbf{U_2}*\Delta t)^2/2*\mathbf{U_2}$ and $v - \mathbf{U_2}*\Delta t \leq v'$, we get $\mathbf{M_2} > q' + \mathbf{P}*(pumps*(set\text{-}now') + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - v'^2/2*\mathbf{U_2}$ *or stop* = ***true*** and this case true.

   iii. Sub-case $v \geq \mathbf{U_2}(read\text{-}now)$:

   Since $now + \Delta t \leq read$ from the precondition, we know $v \geq \mathbf{U_2}*\Delta t$ and using Lemma 1.2, we get $\mathbf{M_2} > q' + \mathbf{P}*(pumps*(set\text{-}now') + \mathbf{\#pumps}*(\mathbf{I}\text{-}\mathbf{S})) - v*\Delta t - (v*(read\text{-}now') - \mathbf{U_2}*\Delta t*(read\text{-}now') - \mathbf{U_2}*(read\text{-}now')^2/2) + \mathbf{U_2}*\Delta t^2/2 + (v * \Delta t - \mathbf{U_2}*\Delta t^2/2)$ *or stop* = ***true***. Since $v*(read\text{-}now') - \mathbf{U_2}*\Delta t*(read\text{-}now') = (v -$

$\boldsymbol{U_2}*\Delta t)*(read\text{-}now') - \boldsymbol{U_2}*\Delta t*(read\text{-}now')$ and $v - \boldsymbol{U_2}*\Delta t \leq v'$ from the effect, we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*(pumps*(set\text{-}now') + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - (v'*(read\text{-}now') - \boldsymbol{U_2}*(read\text{-}now')^2/2)$ *or stop* = ***true***.

This case is obviously true.

b. Case $set = read + \boldsymbol{S}$:

Since $\boldsymbol{\#pumps} \geq pr$ per definition, we know from the assumption $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*\Delta t - \delta_{LOW}(v, v', \Delta t) + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now - \Delta t) - steam + \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true*** with

$$steam = \begin{cases} v^2/2*\boldsymbol{U_2} & \text{if } v < \boldsymbol{U_2}*(read\text{-}now) \\ (read\text{-}now\text{-}\Delta t + \Delta t) - \boldsymbol{U_2}*(read\text{-}now\text{-}\Delta t + \Delta t)^2/2) & \text{otherwise} \end{cases}$$

Moreover, we know from the effect that $now' = now + \Delta t$, $q + \boldsymbol{P} * pr * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$. Thus, we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - steam + \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true***. Based on the steam rate condition and Lemma 1.2:

$$\delta_{LOW}(a, b, u) \geq \begin{cases} a^2/(2*\boldsymbol{U_2}) & \text{if } a < \boldsymbol{U_2} * u \\ a * u - \boldsymbol{U_2}*u^2/2 & \text{otherwise} \end{cases}$$

we distinguish in following cases:

i. Sub-case $v < \boldsymbol{U_2}(read\text{-}now)$ and $v < \boldsymbol{U_2} * \Delta t$:

Since $\delta_{LOW}(v, v', \Delta t) \geq v^2/(2*\boldsymbol{U_2})$ and $v'^2/(2*\boldsymbol{U_2}) > 0$, we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - v'^2/(2*\boldsymbol{U_2})$ and this case true.

ii. Sub-case $v < \boldsymbol{U_2}(read\text{-}now)$ and $v \geq \boldsymbol{U_2} * \Delta t$:

Here, we know $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - v^2/2*\boldsymbol{U_2} + (v * \Delta t - \boldsymbol{U_2}*\Delta t^2/2)$ and since $v^2/(2*\boldsymbol{U_2}) - (v * \Delta t - \boldsymbol{U_2}*\Delta t^2/2) = (v - \boldsymbol{U_2}*\Delta t)^2/(2*\boldsymbol{U_2})$ and $v - \boldsymbol{U_2}*\Delta t \leq v'$, we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - v'^2/2*\boldsymbol{U_2}$ and this case true.

iii. Sub-case $v \geq \boldsymbol{U_2}(read\text{-}now)$:

Since $now + \Delta t \leq read$ from the precondition, we know $v \geq \boldsymbol{U_2}*\Delta t$ and we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - v*\Delta t - (v*(read\text{-}now') - \boldsymbol{U_2}*\Delta t*(read\text{-}now') - \boldsymbol{U_2}*(read\text{-}now')^2/2) + \boldsymbol{U_2}*\Delta t^2/2 + (v * \Delta t - \boldsymbol{U_2}*\Delta t^2/2)$ *or stop* = ***true***. Since $v*(read\text{-}now') - \boldsymbol{U_2}*\Delta t*(read\text{-}now') = (v - \boldsymbol{U_2}*\Delta t)*(read\text{-}now') - \boldsymbol{U_2}*\Delta t*(read\text{-}now')$ and $v - \boldsymbol{U_2}*\Delta t \leq v'$ from the effect, we get $\boldsymbol{M_2} > q' + \boldsymbol{P}*\boldsymbol{\#pumps}*(read - now') - (v'*(read\text{-}now') - \boldsymbol{U_2}*(read\text{-}now')^2/2)$ *or stop* = ***true***.

This case is obviously true.

3. *a*= activate (all but *set* are unchanged):

Since $set = now$ from the precondition, $now \leq read$ (Lemma 2) and $set = read + \boldsymbol{S}$ *or* $set = read - \boldsymbol{I} + \boldsymbol{S}$ (Lemma 5), we know $set = read - \boldsymbol{I} + \boldsymbol{S}$ and from the assumption

$\boldsymbol{M_2} > q + \boldsymbol{P} * \boldsymbol{\#pumps} *(\boldsymbol{I}\text{-}\boldsymbol{S}) - steam\ or\ stop = \textbf{true}$. Since $\boldsymbol{I} - \boldsymbol{S} = read - now$ and the effect sets $set' = read + \boldsymbol{S}$ this lemma is true for the activate action.

■

Lemma 14: $d(u)$ is convex:

$d(u) \geq min(0, d(S))$ for $S \geq u \geq 0$, $d(u) = A*u - B*u^2$ with A real and B positive real

1. Case $u \leq A/(2*B)$:

   Proof (indirect): Suppose $d(u) < 0$. From $A*u-B*u^2 < 0$, we get $u > A/B$. Since $u \geq 0$ and $A/B > A/(2*B)$, we have a contradiction to the case assumption. We know $d(u) \geq 0 \geq min(0, d(S))$ and this case is true.

2. Case $u > A/(2*B)$:

   Proof (indirect): Suppose $d(u) < d(S)$. Define $S = u + \varepsilon$ with $\varepsilon > 0$. From $A*u-B*u^2 < A(u + \varepsilon) - B(u + \varepsilon)^2$ follows $u < A/(2*B) - \varepsilon/2$. Since $u \geq 0$ and $\varepsilon \geq 0$ we have a contradiction to the case assumption. We know $d(u) \geq d(S) \geq min(0, d(S))$ and this case is true.

■

Theorem 1: In all reachable states of boiler system,

$\boldsymbol{M_1} < q < \boldsymbol{M_2}$ *or stop* = ***true***

Proof. First, we show $\boldsymbol{M_1} < q$ *or stop* = ***true*** by induction on the steps of the automaton. It is true in the initial state and trivial for the actuator action. The only remaining action is a = time passage (*stop* is unchanged):
We know *do_output* = ***false*** from (Lemma 7) *if now < read then do_output* = ***false***, from the precondition ($now + \Delta t \leq read$) and $\Delta t > 0$. Since we know $set = read + \boldsymbol{S}$ *or* $set = read - \boldsymbol{I} + \boldsymbol{S}$ (Lemma 5), we can distinguish two cases:

1. Case $set = read - \boldsymbol{I} + \boldsymbol{S}$:

   From Lemma 12, we get $\boldsymbol{M_1} < q + \boldsymbol{P}*pumps*(set-now) - (v * (read-now) + \boldsymbol{U_1}*(read-now)^2/2)$ *or stop* = ***true***. Using $(v * (read-now) + \boldsymbol{U_1}*(read-now)^2/2) > (v * (set-now) + \boldsymbol{U_1}*(set-now)^2/2)$ (since $set < read$), $pumps = pr$ from Lemma 10: *if* $set = read + \boldsymbol{S}$ *and do_output* = ***false*** *then pr = pr_new - error else pr = pumps* and $d(u) = A*u - B*u^2$ as defined in Lemma 14 with $A = \boldsymbol{P}*pr - v$ and $B = \boldsymbol{U_1}/2$, we get: $\boldsymbol{M_1} < q + d(set-now)$ *or stop* = ***true***.

   From Lemma 14 follows that $d(\Delta t) \geq min(0, d(set-now))$ for $\Delta t \leq set-now$.

   a. Sub-case $d(\Delta t) \geq d(set-now)$:

      Here, we know $\boldsymbol{M_1} < q + d(\Delta t)$ *or stop* = ***true***. Since $q + pr * \boldsymbol{P} * \Delta t - \delta_{HIGH}(v, v', \Delta t) \leq q'$ from the effect which is equivalent to $q + d(\Delta t) \leq q'$ because $\delta_{HIGH}(a, b, u) \leq (a*u + \boldsymbol{U_1}*u^2/2)$ from Lemma 1.10, we know $\boldsymbol{M_1} < q'$ *or stop* = ***true*** and this sub-case true.

   b. Sub-case $d(\Delta t) \geq 0$:

      We assume $\boldsymbol{M_1} < q$ *or stop* = ***true***. Since $d(\Delta t) \geq 0$ and $q + pr * \boldsymbol{P} * \Delta t - \delta_{HIGH}(v, v', \Delta t) \leq q'$ from the effect which is equivalent to $q + d(\Delta t) \leq q'$ because $\delta_{HIGH}(a, b, u)$

$\leq (a*u + \boldsymbol{U_1}*u^2/2)$ from Lemma 1.10, we know $\boldsymbol{M_1} < q'$ *or stop* = ***true*** and this sub-case true.

2. Case *set* = *read* + ***S***:

   From Lemma 12, we get $\boldsymbol{M_1} < q' - (v' * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2)$ *or stop* = ***true***. Since $v' * (read\text{-}now') + \boldsymbol{U_1}*(read\text{-}now')^2/2 \geq 0$ this lemma is true.

Second, we show $\boldsymbol{M_2} > q$ *or stop* = ***true*** trough induction on the steps of the automaton. It is true in the initial state and trivial for the actuator action. The only remaining action is *a* = time passage (*stop* is unchanged):
We know *output* = ***false*** from (Lemma 7) *if now < read then do_output* = ***false***, from the precondition ($now + \Delta t \leq read$) and $\Delta t > 0$. Since we know *set* = *read* + ***S*** *or set* = *read* - ***I*** + ***S*** (Lemma 5), we can distinguish following cases:

1. Case *set* = *read* - ***I*** + ***S***:

   From Lemma 13, we get $\boldsymbol{M_2} > q + \boldsymbol{P}*(pumps*(read - \boldsymbol{I} + \boldsymbol{S} - now) + \boldsymbol{\#pumps}*(\boldsymbol{I}\text{-}\boldsymbol{S})) - steam$ *or stop* = ***true***.

   Using $\boldsymbol{\#pumps} \geq pumps$ per definition, $pumps = pr$ from Lemma 10: *if set* = *read* + ***S*** *and do_output* = ***false*** *then pr = pr_new - error else pr = pumps*, we get $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - (v*(read\text{-}now) - \boldsymbol{U_2}*(read\text{-}now)^2/2) + \boldsymbol{P}*(pumps*(\boldsymbol{S}\text{-}\boldsymbol{I}) + pumps*(\boldsymbol{I}\text{-}\boldsymbol{S}))$ *or stop* = ***true***. The rest of the proof for this case is analog to the case *set* = *read* + ***S***.

2. Case *set* = *read* + ***S*** and $v \geq \boldsymbol{U_2}(read\text{-}now)$:

   From Lemma 13 and using $\boldsymbol{\#pumps} \geq pr$ per definition, we get $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - (v*(read\text{-}now) - \boldsymbol{U_2}*(read\text{-}now)^2/2)$ *or stop* = ***true***.

   Since $d(u) = A*u - B*u^2$ as defined in Lemma 14 with $A = v - \boldsymbol{P}*pr$ and $B = \boldsymbol{U_2}/2$, we get: $\boldsymbol{M_2} > q - d(read - now)$ *or stop* = ***true***.

   From Lemma 14 follows that $d(\Delta t) \geq min(0, d(read\text{-}now))$ for $\Delta t \leq read\text{-}now$.

   a. Sub-case $d(\Delta t) \geq d(read\text{-}now)$:

      Here, we know $\boldsymbol{M_2} > q - d(\Delta t)$ *or stop* = ***true***.

      Since $q + pr * \boldsymbol{P} * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$ from the effect which is equivalent to $q - d(\Delta t) \geq q'$ because $v \geq \boldsymbol{U_2}(read\text{-}now)$, $read\text{-}now \geq \Delta t$ from the precondition and Lemma 1.2:

      $$\delta_{LOW}(a, b, u) \geq \begin{cases} a^2/(2*\boldsymbol{U_2}) & \text{if } a < \boldsymbol{U_2} * u \\ a * u - \boldsymbol{U_2}*u^2/2 & \text{otherwise} \end{cases}$$

      we know $\boldsymbol{M_2} > q'$ *or stop* = ***true*** and this sub-case true.

   b. Sub-case $d(\Delta t) \geq 0$:

      Here, we assume $\boldsymbol{M_2} > q$ *or stop* = ***true***. Since $d(\Delta t) \geq 0$ and $q + pr * \boldsymbol{P} * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$ from the effect which is equivalent to $q - d(\Delta t) \geq q'$ because $v \geq$

$\boldsymbol{U_2}(read\text{-}now)$, $read\text{-}now \geq \Delta t$ from the precondition and Lemma 1.2, we know $\boldsymbol{M_2} > q \geq q - d(\Delta t) \geq q'$ *or stop* = ***true*** and this sub-case true.

3. Case $set = read + \boldsymbol{S}$ and $v < \boldsymbol{U_2}(read\text{-}now)$:

   From Lemma 13 and using ***#pumps*** $\geq pr$ per definition, we get $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - v^2/2*\boldsymbol{U_2}$ *or stop* = ***true***. From Lemma 1.2, we get two sub-cases:

   a. Sub-case $v < \boldsymbol{U_2} * \Delta t$:

      We get $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true***. Since $read - now \geq \Delta t$ from the precondition, we know $\boldsymbol{M_2} > q + \boldsymbol{P} * pr*\Delta t - \delta_{LOW}(v, v', \Delta t)$ *or stop* = ***true***. Since $q + \boldsymbol{P} * pr*\Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$, this case is true.

   b. Sub-case $v \geq \boldsymbol{U_2} * \Delta t$:

      We get $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - v^2/(2*\boldsymbol{U_2})$ *or stop* = ***true***. Since $v^2/(2*\boldsymbol{U_2}) = v*(v/\boldsymbol{U_2}) - \boldsymbol{U_2}*(v/\boldsymbol{U_2})^2/2$, we know $\boldsymbol{M_2} > q + \boldsymbol{P}*pr*(read - now) - (v*(v/\boldsymbol{U_2}) - \boldsymbol{U_2}*(v/\boldsymbol{U_2})^2/2)$ *or stop* = ***true***. Using $d(u) = A*u - B*u^2$ as defined in Lemma 14 with $A = v - \boldsymbol{P}*pr$ and $B = \boldsymbol{U_2}/2$, we get: $\boldsymbol{M_2} > q - d(v/\boldsymbol{U_2}) + \boldsymbol{P}*pr*(read - now - v/\boldsymbol{U_2})$ *or stop* = ***true***. Since $pr \geq 0$ per definition and from the case statement we know $v < \boldsymbol{U_2}(read\text{-}now)$, we get $\boldsymbol{M_2} > q - d(v/\boldsymbol{U_2})$ *or stop* = ***true***.

      From Lemma 14 follows that $d(\Delta t) \geq min(0, d(v/\boldsymbol{U_2}))$ for $\Delta t \leq v/\boldsymbol{U_2}$.

      i. Sub-sub-case $d(\Delta t) \geq d(v/\boldsymbol{U_2})$:

         Here, we know, using Lemma 14, $\boldsymbol{M_2} > q - d(\Delta t)$ *or stop* = ***true***.

         Since $q + pr * \boldsymbol{P} * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$ from the effect which is equivalent to $q - d(\Delta t) \geq q'$ because $v \geq \boldsymbol{U_2} * \Delta t$ and Lemma 1.2, we know $\boldsymbol{M_2} > q'$ *or stop* = ***true*** and this sub-case true.

      ii. Sub-sub-case $d(\Delta t) \geq 0$:

         Here, we assume $\boldsymbol{M_2} > q$ *or stop* = ***true***. Since $d(\Delta t) \geq 0$ and $q + pr * \boldsymbol{P} * \Delta t - \delta_{LOW}(v, v', \Delta t) \geq q'$ from the effect which is equivalent to $q - d(\Delta t) \geq q'$ because $v \geq \boldsymbol{U_2} * \Delta t$ and Lemma 1.2, we know $\boldsymbol{M_2} > q \geq q - d(\Delta t) \geq q'$ *or stop* = ***true*** and this sub-case true.

■