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 short version of the paper (published in the LNCS book):

1. p. 6: 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.

2. p. 6: 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. 6: 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 relations are missing between constants:

   a) $0 \leq \mathbf{M_1} < \mathbf{M_2} \leq \mathbf{C}$

   b) $\mathbf{S} < \mathbf{I}$

5. p. 7, *error* should be cleaner defined: *error* in the range *[0 … **#pumps**]* instead *[0 … pr_new]*

6. p.10: *min_steam_water(sr)* is wrong defined:

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

   Lemma 3.1 is consequentially (whenever used in the described proofs):

   $\mathbf{M_2} > wl + \mathbf{P} * (pumps * \mathbf{S} + \mathbf{\#pumps} * (\mathbf{I} - \mathbf{S})) - min\_steam\_water(sr)$ *or stopmode =* ***true***
6. p.10, 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.11, The initial state of *stopmode* is ***true*** so that Lemma 3 is correct in the initial state.

8. p.11, 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.14: Lemma 12 should be:

```
if do_output = false then
  if $set = read - \mathbf{I} + \mathbf{S}$ then
    $\mathbf{M_1} < q + \mathbf{P}*pumps*(set-now) - (v * (read-now) + \mathbf{U_1}*(read-now)^2/2)$ or stop = true
  else   $\mathbf{M_1} < q - (v * (read-now) + \mathbf{U_1}*(read-now)^2/2)$ or stop = true
```

10.p.14: Lemma 13 should be:

```
if do_output = false then
  if $set = read - \mathbf{I} + \mathbf{S}$ then
    $\mathbf{M_2} > q + \mathbf{P}*(pumps*(set-now) + \mathbf{\#pumps}*(\mathbf{I}-\mathbf{S})) - steam$ or stop = true
  else   $\mathbf{M_2} > q + \mathbf{P}*\mathbf{\#pumps}*(read - now) - steam$ or stop = true
```

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

13. p.14, Consequentially, the proof to Theorem 2 changes. Its detail can be found in the full version of this paper. Moreover, Theorem 2 needs following additional information:

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

14. p.16, The estimated water level in the sensor action should be more precise:

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

15. p.16, In the sensor action *wl_ok’* and *sr_ok’* should be *wl_ok* and *sr_ok* since they are not changed.

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